**Terms and Conditions of Use of Digitised Theses from Trinity College Library Dublin**

**Copyright statement**

All material supplied by Trinity College Library is protected by copyright (under the Copyright and Related Rights Act, 2000 as amended) and other relevant Intellectual Property Rights. By accessing and using a Digitised Thesis from Trinity College Library you acknowledge that all Intellectual Property Rights in any Works supplied are the sole and exclusive property of the copyright and/or other IPR holder. Specific copyright holders may not be explicitly identified. Use of materials from other sources within a thesis should not be construed as a claim over them.

A non-exclusive, non-transferable licence is hereby granted to those using or reproducing, in whole or in part, the material for valid purposes, providing the copyright owners are acknowledged using the normal conventions. Where specific permission to use material is required, this is identified and such permission must be sought from the copyright holder or agency cited.

**Liability statement**

By using a Digitised Thesis, I accept that Trinity College Dublin bears no legal responsibility for the accuracy, legality or comprehensiveness of materials contained within the thesis, and that Trinity College Dublin accepts no liability for indirect, consequential, or incidental, damages or losses arising from use of the thesis for whatever reason. Information located in a thesis may be subject to specific use constraints, details of which may not be explicitly described. It is the responsibility of potential and actual users to be aware of such constraints and to abide by them. By making use of material from a digitised thesis, you accept these copyright and disclaimer provisions. Where it is brought to the attention of Trinity College Library that there may be a breach of copyright or other restraint, it is the policy to withdraw or take down access to a thesis while the issue is being resolved.

**Access Agreement**

By using a Digitised Thesis from Trinity College Library you are bound by the following Terms & Conditions. Please read them carefully.

I have read and I understand the following statement: All material supplied via a Digitised Thesis from Trinity College Library is protected by copyright and other intellectual property rights, and duplication or sale of all or part of any of a thesis is not permitted, except that material may be duplicated by you for your research use or for educational purposes in electronic or print form providing the copyright owners are acknowledged using the normal conventions. You must obtain permission for any other use. Electronic or print copies may not be offered, whether for sale or otherwise to anyone. This copy has been supplied on the understanding that it is copyright material and that no quotation from the thesis may be published without proper acknowledgement.

# A Domain Knowledge Driven Information Uplift Approach for Network Monitoring

A thesis submitted to the
University of Dublin, Trinity College,
for the degree of
Doctor of Philosophy

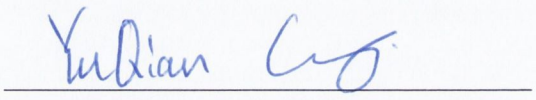
**Yuqian Song**

Knowledge and Data Engineering Group
School of Computer Science and Statistics
Trinity College, University of Dublin

2014

# Declaration

I, the undersigned, declare that this work has not previously been submitted as an exercise for a degree at this or any other University, and that, unless otherwise stated, it is entirely my own work.



Yuqian Song

May 2014

# Permission to Lend or Copy

I, the undersigned, agree that Trinity College Library may lend or copy this thesis upon request.

Yuqian Song

May 2014

# ACKNOWLEDGEMENTS

I would like to thank my supervisors Prof. Dr. Owen Conlan, Dr. David Lewis and Dr. John Keeney for their unflagging support, insightful contributions and the many revisions of this thesis. I appreciate the collaboration work from Dr. Rob Brennan and other researchers for sharing innovative ideas and offering great opportunities for my research. I also would like to thank Prof. Dr. Declan O'Sullivan for chairing the SFI FAME project, which sponsored my whole Ph.D. study. My thanks to all in the KDEG research group for their knowledge sharing, lively discussions, their participation in my experiments, and also the proof reading/feedback. I truly appreciate for the high quality of education and research in Trinity College Dublin.

I would like to especially thank my parents and all family members for their constant encouragement, support and the many sacrifices.

# ABSTRACT

With the advance of modern network technologies, people now enjoy increased convenience whilst occasionally suffering annoyance from network issues by lacking domain expertise. In the Home Area Network (HAN), these issues bring extra support costs for network providers and also reduce the user's satisfaction. Network providers also face a number of systemic challenges to delivery services and ensuring the Quality of Experience (QoE) for the end-user. A key challenge is how to support non-expert users to understand and monitor complex network systems by leveraging domain expert knowledge. This thesis proposes a knowledge-driven information uplift approach to support non-expert users in understanding and monitoring network systems. This research combines the research in areas of semantic uplift, knowledge modelling, network monitoring, and information visualization to face the addressed challenge. Specifically, this approach helps users to uplift semantically meaningful information across separate data sources gathered from network resources. These heterogeneous sources can be in various data formats, and are uplifted and presented to non-expert users in a consolidated fashion, which is derived from captured and modelled domain expert knowledge. A Semantic Information Uplift Engine (CASIU) and its monitoring framework (CasiuVis) with corresponding information representations based on this approach have been designed and are implemented. How to capture and model the domain expertise and represent meaningful information to non-expert users is another key

challenge in this research. Importantly, the design and implementation of CASIU and CasiuVis can be used in a broad range of real-world network systems. Furthermore, the validation of these systems and their underlying approach is performed through a series of iterative evaluations. Based on four evolving experiments, these evaluations incorporate a variety of techniques, including user trials, performance tests, feasibility tests and functionality tests.

As a summary, this thesis presents research of a domain knowledge-driven information uplift approach -- the design and implementation of this approach with its monitoring framework and comprehensive information representations has been validated and evaluated to enable the support of non-expert users in understanding and monitoring network systems.

# TABLE OF CONTENTS

# TABLE OF FIGURES

# TABLE of TABLES

# ABBREVIATIONS

| | |
|---|---|
| ADSL | Asymmetric Digital Subscriber Line |
| CP | Change Point |
| CPU | Central Processing Unit |
| CSV | Comma-separated values |
| DB | Database |
| DSLAM | Digital Subscriber Line Access Multiplexer |
| GW | Gateway |
| HAN | Home Area Network |
| HD Video | High-definition Video |
| IPTV | Internet Protocol Television |
| KB | Knowledge Base |
| LOS | Port Loss of Signal Seconds |
| MOS | Video Mean Opinion Score |
| NM | Network Management |
| OS | Operating System |

| | |
|---|---|
| OWL | Web Ontology Language |
| PLR | Packet Loss Ratio |
| QoE | Quality of Experience |
| QoS | Quality of Service |
| RDF | Resource Description Framework |
| RDFS | RDF Schema |
| SD Video | Standard-definition Video |
| SES | Port Severely Errored Seconds |
| SPARQL | Simple Protocol and RDF Query Language |
| SUS | System Usability Scale |
| SWRL | Semantic Web Rule Language |
| UAS | Port Unavailable Seconds |
| UI | User Interface |
| XML | eXtensible Markup Language |
| XSLT | XML Stylesheet Transformation |

# Chapter 1
# Introduction

## 1.1 *Motivation*

In recent years, the rapid development of network infrastructures provides increasing connectivity and advanced communication services for network consumers. More and more households are connected to the Internet through broadband access services. In 2013 there are around 2.7 billion fixed internet users worldwide and around 25% of these will have access to fixed broadband [Wansink 2013]. The growing broadband connectivity allows a large variety of home devices to connect to the Internet, and high bandwidth ensures advanced Internet applications and services such as video and audio streaming, high quality video conferencing, and file sharing and backup are now becoming commonplace. Home Area Networks (HAN) is defined as a network which could control many devices, all of them working together to keep home comfortable, entertaining, and safe [Saif et al. 2002]. A strategic analysis research report [King 2009] indicated the global sales of home network devices would reach 409 million units in 2009, representing 35% of the total market for digital home devices and forecasted the annual sales will reach 1.2 billion units by the end of 2014. Despite huge investments in broadband, and over a decade of experience with advanced network technologies, HAN still face a number of systemic challenges:

Hard to monitor: This evolving of HAN brings increasing complexity for HAN users to diagnose, analyse and resolve the network-related issues in their daily usage [Tolmie et al. 2007]. As the HAN become a normal part of people's daily lives [Pediaditakis et al. 2012a], a growing percentage of these households [King 2009] has been motivated to adopt a variety of modern networking technologies. They interconnect devices within the home to enable networking services for different purposes, such as media sharing, communication, gaming and

other applications, working together thus resulting in a more comfortable, entertaining, and safe home [Saif et al. 2002]. The heterogeneity of network resources and monitoring purposes also brings increasing complexity to most of HAN users also considered as non-expert users, whom have neither sophisticated technical knowledge nor motivation to learn complex tools [Chetty et al. 2007] [Crabtree et al. 2012]. They lack the technical know-how (or the desire) to monitor their home network. Networks typically operate with the default settings shipped by device or service provider. Compared to large enterprise-wide networks, HANs are also coupling with a variety of devices to deliver heterogeneous advanced communication services, but most current monitor/management tools are designed for commercial networks that lack usability for HAN users. Researchers have noted that a large number of users run into difficulties as they try to monitor/manage their home network [Bly et al. 2006] [Grinter and Edwards 2005] [Shehan and Edwards 2007]. A large number of devices are returned because users could not get them to function. A business report revealed 25% of networking equipment was returned (of which 90% is fully functional)—one of the highest return rates among consumer electronics [Accenture 2008]. According to a user research [Brown et al. 2007] [Kiesler et al. 2000], over 70% of home users needed technical support to set up their device and connect it to the Internet for the first time, and 90% of the households called the help desk for technical support during the first year of network usage. Worse, many inexperienced home users do not call the help desk, especially if they feel they do not have the necessary vocabulary or background knowledge to discuss an issue with a technical person [Yang et al. 2010]. This difficulty for users to monitor their HANs brings a large number of extra support costs for network devices or service providers.

Lack of visibility: Along with its complexity, the invisibility of the HAN makes home network monitoring even more difficult [Grinter et al. 2005] [Chetty et al. 2012]. Such invisibility gives users an incomplete view of the HAN, which consequently makes understanding it difficult [Brown et al. 2013] [Sundaresan et al. 2013]. This highlights the importance of the visibility of the home network components, which contain the status of network infrastructures, services, and the high-level meanings of these components. If users are to monitor their home networks successfully, they should be given an accurate, complete conceptual model of their HAN. Researchers agree that one of the best ways to make a network more "visible" to the home user is by presenting it as a diagram [Tolmie et al. 2007]. Because of the usability problems of home network monitoring, researchers have called for network

monitoring tools for general home network users [Chetty et al. 2007] [Edwards and Grinter 2001]. They suggested more interactive tool for home network users who have neither the sophisticated technical knowledge nor the motivation to learn complex network systems currently designed for network administrators.

Prone to failure: Networks in the home often suffer unpredictable failures (e.g high packet-loss and disconnection). Although HAN users are often troubled with a very small set of common problems [Wallin et al. 2009], reasons for failures are numerous [Nakamura et al 2013], ranging from poor AP placement, to interference with neighboring WiFi APs, to misconfigured APs and network settings. Non-expert users have difficulties dealing with these network failures, which are also reckoned as the type of issues usually happening but hard to diagnosis the root-reason without domain expertise [Bly et al. 2006] [Grinter et al. 2005] [Shehan et al. 2007]: (1) an IPTV service suddenly suffers a degradation of the quality, perhaps caused by some WiFi activities in the same channel – causing interference, (2) or a signal weakens when the antenna of the wireless device is obstructed, (3) or the laptop user may upload a large file which causes network congestion for other devices. Such trivial issues seem unremarkable but will impact on the end-user's perception of the network quality and increase the support cost of vendors [Teger et al. 2002]. They require the user to have a working knowledge of low-level networking concepts such as network protocols and packets that are unfamiliar to general home users. The user normally concerns only the high-level objectives, like the status of connection, the root-cause of current problem, or how to protect the network [Teger et al. 2002]. Presumably a service provider with access to more expert resources and technical know-how can better diagnose these failures and manage the network to deliver predictable and good performance. But in most cases, the assistance from network vendors is not timely or is unavailable, which affects the user satisfaction and increases the support cost of network vendors. In spite of the strong incentives (e.g. IPTV service providers would be motivated to carefully manage the home network to deliver good streaming quality), current home networks still lack the affordable mechanisms for the service provider to innovate and improve the behaviour of the home network to increase the quality of the product they deliver.

Because of these challenges, many firms [Savoia et al. 2006] have realized, as their marketplaces have become more global and service oriented, that customer support is critical to their competitiveness. A survey of 350 information systems executives [Savoia et al. 2006]

revealed that connecting to customers and suppliers is their top priority. Among this same group, 60% of the respondents indicated that developing applications to support their customers was the most important focus for their system development efforts. It has become a $1.9 billion global market for supporting customers in managing and monitoring networks [McGillicuddy et al. 2009]. However, the goal of making network meaningful and easily accessible to non-expert users is still presenting a series of research/technical challenges in the network monitoring area [Pras et al. 2007]. The monitoring data from heterogeneous network resources exhibit bewildering complexity and are often beyond the cognitive capability of non-expert users. A non-expert user may be defined as "typical network consumer" whom is assumed neither a real "techie" nor a "Luddite" [Teger et al. 2002]. This complexity is further increased by a lack of visibility to non-expert users. It is not reasonable to expect non-expert users to acquire the professional network domain knowledge and understand technical details, and a clear conceptual view should be delivered by monitoring. This complexity and invisibility also lead to perplexed users, when they face unpredictable failures of their HANs, which is also a major concern for this fast-growing market of Home Area Network (HAN) [McGillicuddy et al. 2009]. Domain experts from ISP, device, or service venders could identify particular problems with their own products but these issues always involve the understanding of the interaction between all the different network devices and services. This also leads to a large amount of extra support costs for vendors to deal with many classes of HAN problems and increasing risk of no fault returns.

Such inherent difficulties make the role of a more meaningful network monitoring approach critical for both non-expert users and network vendors. A meaningful monitoring approach could assist in their understanding of what happens in the HAN, what causes the problem and how to attain a solution, whilst determining what domain knowledge is required. On one hand, as revealed in the State of the Art section there are a variety of available tools for network monitoring and control, they are usually a poor fit for modern HANs. On the other hand, a combination of visualisation and information extraction technologies are proven effective for non-expert users [Keller et al. 2005], but the challenge still exists of how to extract and present meaningful monitoring information to support non-expert users to understand the status of their HAN and overcome unpredictable failures.

The complexity, invisibility and unclear failure for HAN monitoring also affect the service provider to ensure the quality of their service delivery. One of the most significant factors

driving the growth in HAN is the increased transport of video over IP networks including IPTV (Internet Protocol Television) services [Asghar et al. 2009]. It is reported that nearly 40% issues relating to IPTV delivery occur in the HAN [Gupta et al. 2011], which trouble non-expert HAN users. Another significant research challenge for IPTV delivery network administrators is to assure good delivery, particular if such monitoring can be used for Customer Experience Management (CEM) to understand network status, diagnose problems, and analyse from two different but related viewpoints, Quality of Service (QoS) and Quality of Experience (QoE) to improve the user experience and control the operation cost. To maximize return-on-investment and to be competitive, operators will need to meet customer expectations to ensure that there is demand for their IPTV service. Recent work has explored strategies for coordinating the allocation of resources for multiple virtual IPTV providers to maximize revenue [Balasubramaniam et al. 2011a] and routing strategies to manage network resources when multiple IPTV services are overlaid on the same network [Balasubramaniam et al. 2011b]; however, the fundamental problem –indeed an integral part of satisfying customer expectation– lies in monitoring the quality of the IPTV service being provided and then giving guidance on how delivery can be improved. The IPTV delivery network is usually a combination of heterogeneous servers, routers, and even sub-networks systems. Its complex nature requires cross-domain knowledge from both QoS and QoE aspects to ensure the delivery of IPTV services to HANs. A meaningful monitoring approach of this IPTV delivery network is also desired by both HAN users and service providers to reduce the support cost and increase user satisfaction.

A common strategy to guarantee monitoring is to extract structured information from unstructured and/or semi-structured data and present them in a meaningful way [Andersen et al. 1992]. As a formal structured representation of information, semantic web techniques are capable of extracting the rich semantics from growing amount of information available in unstructured form [Berners-Lee et al. 2001]. As presented in a large body of work [Madden et al. 2002] [Demers et al. 2003] [Barford et al. 2002], Information Extraction is widely applied to extract the meaningful information from real-time network log data and then aggregate and analyse them for different network monitoring purposes. Meaningful information is defined as the efficient information gathering from the captured characteristics of log data set for purposes such as monitoring, fault diagnosis, and performance evaluation [Liotta et al. 2002]. A number of stream data analysis techniques, e.g. stream data mining [Chu et al. 2004], data trend

analysis [Brutlag, 2000], stream data aggregation [Rajagopalan et al. 2006], change point detection [Karagiannis et al. 2008], etc., specialize to capture one or several particular types of characteristics from network log data stream. Moreover, the highly heterogeneous nature of current network works always requires a combination of several analysis approaches which desire a structured format to maintain the extracted meaningful information. However, simultaneously monitoring all time-series of interesting meaningful information is an impossible task even for the accomplished network technician. This requires a further aggregation process for the overload of meaningful information from low-level to high-level according to specific monitoring purposes. Due to its standard format and reasoning capability, Semantic Web technology promises a well-defined structure to represent meaningful information so that both monitoring agent and human users can understand the meaning of information and know "how to deal" with it. This semantically structured information also supports formal semantic reasoning which benefits the knowledge-driven problem analysis in the network monitoring scenario. As well-developed semantic techniques, Semantic Annotation, Semantic Modelling, and Semantic Reasoning are effective approaches for information extraction, collaboration and translation from heterogeneous data and information structures into Semantic Web metadata with formal semantic meanings [Handschuh et al. 2007]. The semantic information extraction could be executed as either a manual or an automatic process [Uren et al. 2006]. The automatic process is traditionally driven by pre-defined rules or policies. In order to perform the intelligent and automatic monitoring for heterogeneous network scenarios, the context for network components and services [Huebscher et al. 2008] [Toutain et al. 2011] is foundational to determine how to adapt the automatic semantic information extraction approach which requires modelling of network components based on the reasoning results from domain knowledge models rather than manually created rules. The concerns and goals of the end-user are rarely incorporated into this process and the extracted information sometimes still contains too many details of underlying data. In this research, we defined the information about underlying data as low-level information for end-users and information about monitoring objectives as high-level information. The information uplift is defined as a way to extract meaningful information from low-level to high-level and represent them in a formal, explicit and sharable format. Many other current approaches only partially provide the solution that end users needed to find pertinent information hidden within dynamic large data sets. The ability to elicit, represent and analyse the tacit knowledge of domain expertise is crucial to show the promise of generating the meaningful information

[Jennings et al. 2007]. Some authoring tools [Hampson et al. 2011] are developed for network experts who lack semantic coding skills to express their insights in an expressive and compatible way.

Another effective strategy for presenting and coping with high complexity is visualization [Latham 1995], which is the process of representing information as a visual image which can facilitate problem-solving and discovery by providing a structure for expressing and communicating the meaning of highly complex information. In order to investigate the combination of research in information visualization and network monitoring, a large number of systems have already been implemented to dynamically represent the topology structure, device connection and situation of domestic networks with well-designed dashboards. However, only a few of them focus on network information representation for non-expert users [Yang et al. 2010] [Chetty et al. 2010]. Information visualization is also an effective approach to show the value of information uplift by representing semantically uplifted meaningful information to improve understanding for non-expert users.

As discussed, the network monitoring challenges for both vendors and non-expert users are:

- Hard to monitor with increasing complexity of HAN and lack of domain knowledge for non-export users.
- Lack of visibility for the information contained in heterogeneous monitoring data to the non-expert users.
- Difficult to diagnose, analyse and resolve unpredictable failures without directly support from network and service vendors.
- Hard to ensure the quality of experience for the non-expert user through service delivery.

According to these challenges, there is a clear need for techniques to support non-expert users in understanding and monitoring their network systems. The high complexity of current network systems and their large amount of log data raise difficulties for non-expert users without the appropriate domain knowledge. Information uplift is widely used to extract information by capturing the characteristics of network log data stream. For HAN monitoring,

it needs common representation for aggregated information from network logs, and also more investigation about how to leverage domain expertise to uplift meaningful information from low-level to high-level. It is also a challenge to capture and represent domain knowledge in complex network environments. Furthermore, an investigation is required to demonstrate that uplifted information could support the better understanding of complex network systems for non-expert users. By achieving these challenges, this research aims to reduce the cost of custom support and increase the user satisfaction. Hence, the focus of this thesis is to support non-expert users in understanding and monitoring network systems by leveraging domain knowledge driven information uplift. This research also investigates a general framework for network monitoring and comprehensive representations for network information and domain knowledge.

## 1.2 *Research Question and Objectives*

This thesis addresses the question of:

"How and to what extent domain expert knowledge may be leveraged to enable the real time uplift of meaningful information from raw data to support non-expert users in understanding and monitoring network systems?"

This thesis describes an information uplift approach with accompanying domain knowledge models and framework to support non-expert users in understanding and monitoring network systems. In this research, we defined the information about underlying network log data as low-level information for end-users and information about monitoring objectives or network activities as high-level information. The information uplift is defined as an approach to extract meaningful information from low-level to high-level and represent them in a formal, explicit and sharable format.

Network systems generally have heterogeneous types of interconnected nodes that allow a variety of services transferring and sharing of resources and information. These network components may also cause failures to reduce the Quality of Service (QoS) and Quality of Experience (QoE). Specifically this research considers providing a meaningful monitoring approach for Home Area Network (HAN) and ensuring the quality of IPTV delivery network, in which non-expert users lack the appropriate expertise in such a highly heterogeneous,

dynamic and data rich environment.

Non-expert users in this thesis are common network users who only have basic computing skills, and have no formal knowledge background in network monitoring and lack problem solving capability. In HAN, non-expert users indicate most of normal home network users. In IPTV delivery network, ordinary network administrators are also considered as non-expert users who are trained for several particular types of network issues but not qualified for cross-domain network problems. To the contrary, domain expert is differed through their degree of expertise in one or several network domains.

Knowledge is information, which has been cognitively processed and integrated into an existing human knowledge structure [Rumelhart & Ortony, 1977]. Domain refers to the knowledge domain which is adapted to the affordances in coping with network task situations, e.g. IPTV network monitoring domain, HAN monitoring domain, QoE anomaly diagnosis domain, etc. In this thesis, the expert knowledge means the accumulated experience and knowledge of network domain experts for diagnosis, analysis and solving network problems.

Five objectives are derived:

- **Objective 1**: survey the state of the art of network monitoring and identify related approaches and techniques to support non-expert users and categorize them. Find out the existing similar approaches, analyze and compare them to indicate the research challenges.

- **Objective 2**: design and implement representations for domain expertise to support the knowledge-driven network monitoring.

- **Objective 3**: design and implement a knowledge-driven approach to uplift meaningful information from real time log data to support non-expert users.

- **Objective 4**: design and implement a general framework to support non-expert user to perform monitoring tasks in different network scenarios.

- **Objective 5**: follow an iterative approach to prototype, evaluate, and validate the design and implementation in different network monitoring use cases.

By achieving Objective 1, a study is established as a foundation for the other research

carried out in this thesis. This study describes a state of art research of *Network Monitoring Tools for Non-expert Users* and *Information Representation and Uplift Approaches.* The surveys of existing network monitoring tools for non-expert users expose the motivation of our research. The review of current information representation and uplift approaches provides this research with a general grounding. It helps the study of what the research challenges of existing approaches are and review what techniques could assist in fulfilling the requirements of network monitoring scenarios. Furthermore during categorization of related research, similar approaches and tools are compared to indicate the research challenges. This study provides a basis for objective 2 - 5 where our research is carried out.

By combining Objective 2 and 3 together, this research examines ***how domain expert knowledge may assist to enable the real time uplift of meaningful information from raw data***. According to the addressed research challenges, the research for Objective 2 aims to design a comprehensive information representation for network information and domain expertise to support network monitoring. This research further displays how the captured and modelled domain expertise could drive the information uplift approach to represent the network information in a meaningful way. The research for Objective 3 aims to design and implement an approach to extract the information from raw data and uplift the meaning from low-level to high-level to support network monitoring for non-expert users. This research displays a further development of existing information representation and uplift techniques learned from previous research.

Addressed by Objective 4 and 5, another half of the research question, ***to what extent the information uplift approach may support non-expert users in understanding and monitoring network systems,*** is answered to illustrate the effectiveness in real world problem and examine the boundary of our information uplift approach performed in objective 3. According to the addressed research challenges in existing network monitoring approaches and techniques, a framework is designed to support network monitoring tasks in different network systems for non-expert users. This design and implementation are in an iterative process distributed in four experiments and also evaluated in separate network scenario with different monitoring task and domain expertise. Objective 5 focuses on the evaluation of the research in this thesis and also intends to address ***what extent***, the limitation and boundary of this research. The evaluation is performed in an iterative way to refine, prototype and validate the design from the perspectives of functionality, effectiveness, performance and usability. These evaluations are enforced in a

series of experiments.

## 1.3 *Research Process and Approach*

As shown in Figure 1-1, the research in this thesis breaks the research question into five research objective (**Obj1-5**) and these objectives are fulfilled with corresponding designs, implementations, and evaluations.

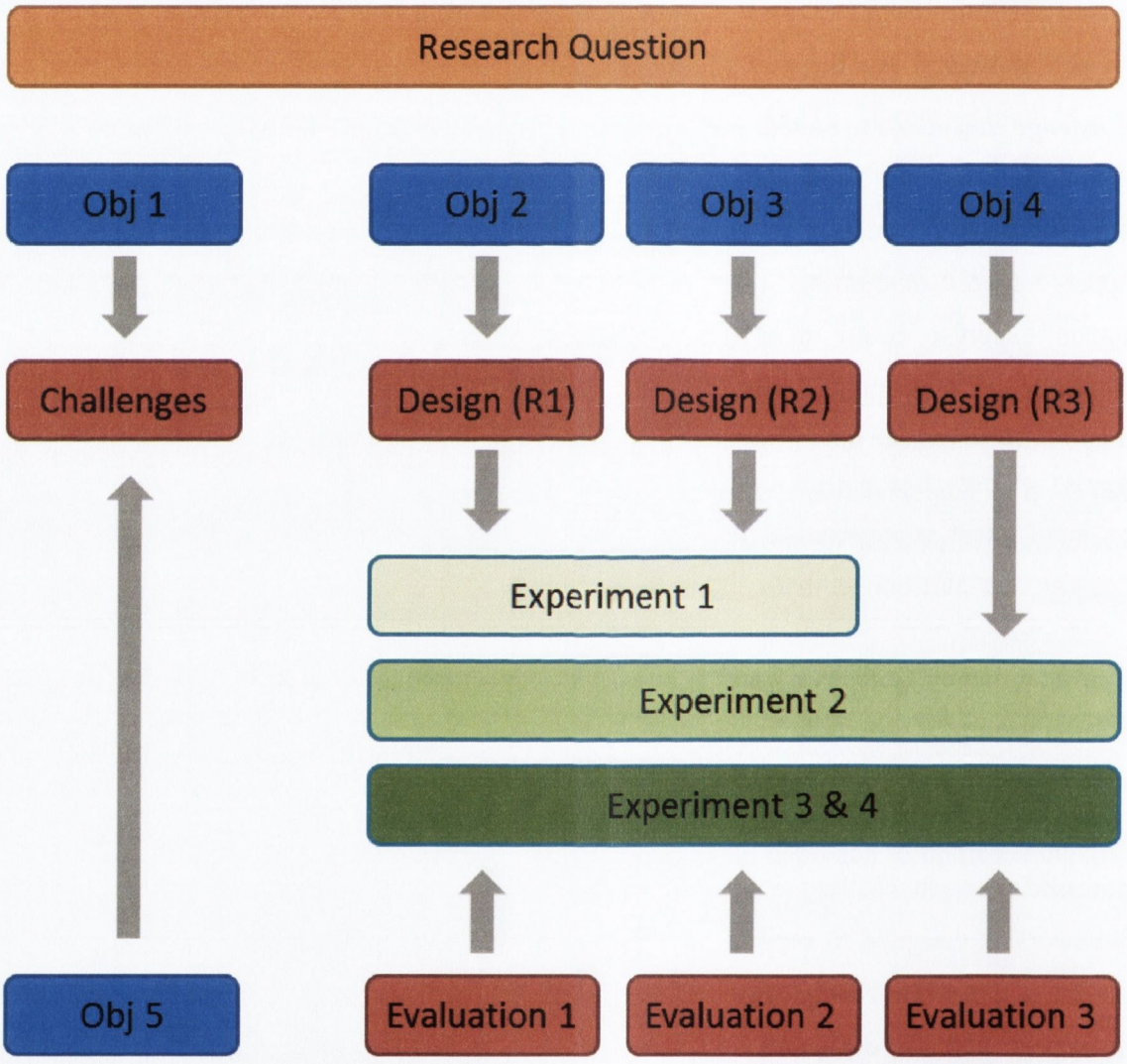



Figure 1-1 Research Process in this Thesis

An initial state of the art was concluded on general network monitoring approaches and

their challenges for non-expert users. According to addressed challenges, three more focusedsurveys were undertaken in the areas of information extraction on network stream data, knowledge-driven network monitoring and visual representation for network information to benefit non-expert network users. Each of these areas is classified by semantic and non-semantic approaches, and then further categorized based on their characteristics. The classifications are compared to state the benefits/shortcomings in order to pick up the suitable approaches for our research. Moreover, several existing network monitoring systems/tools were selected and most of them covered one or two stated research areas. A functional comparison was performed among them. The literature review helped in providing an understanding of the major challenges in these areas and in identifying the strengths and weaknesses of these approaches. This process was important in identifying what niche this research fitted into, and was also vital when deriving the requirements that the proposed approach had to satisfy.

Based on addressed challenges in the state of the art, our knowledge-driven information uplift approach with its network monitoring framework was designed and implemented in an iterative implementation and test process. Focusing on one or several research objectives, new/improved factors are proposed in each iteration with a prototype implementation. Followed by a well-performed evaluation of each iteration, the implementation prototype will be examined against initial objectives. Each iteration process could be considered as an experiment. The deployment and evaluation result of each iteration will also provide feedbacks to adjust and improve the initial design. Each iteration will be documented and published in order to get external feedback and review, which will also benefit the current research. All of these iterations are based on the log data from research partner's test bed, which means the evaluation result could truly reflect the real world problem. During the experiment iteration process, the information uplift approach and its framework is continually improving until they fulfil all research objectives.

The evaluation in this research was performed in three major aspects: usability, effectiveness, and performance. The usability is mainly based on user-based evaluation, which was performed through questionnaires and feedback from both non-expert and expert users. The effectiveness is evaluated by functional comparison with existing similar systems and also the user performance through a series of functional tests. The performance evaluation was combined by tests from both performance and accuracy aspects. Our approach and its framework were tested based on different network scenarios. In other words, our approach was

finally measured by different performance and accuracy level to fulfil the different requirements of network monitoring from non-expert users. And the experiment results also exposed the potential for further research and development.

## 1.4 *Contributions*

Two contributions are identified.

Major contribution: an information uplift approach driven by domain expert knowledge.

Minor contribution: the design and implementation of an information uplift framework and a prototypical implementation to support non-expert users in understanding and monitoring different network systems, termed the *Semantic Information Uplift engine (CASIU) and* its *network monitoring framework (CasiuVis)*.

This thesis proposes an innovative approach that uplifts semantic meaningful information by leveraging domain expert knowledge to support non-expert users in understanding and monitoring network systems. The major contribution that distinguishes this research from the state of the art is a domain expert knowledge driven information uplift approach which contains a set of semantic encodings for domain expert's insights, a domain knowledge model, and an information uplift process. Importantly, this approach specifies a novel and general information uplift engine, which serves as a useful intermediary to extract, aggregate and uplift the meaningful information from the real-time network log data. Specifically it contributes to the state of the art through its approach to establishing the logical relationship between captured domain expert's insights and existing domain knowledge model. This formal knowledge representation also enables an information uplift process, which could automatically invoke related knowledge model to uplift semantic meanings from low-level to high-level and maintain them structurally based on the network component and service.

By extending Hampson's research [Hampson et al. 2011], we further develop his semantic attribute encoding into three types: basic semantic attribute, semantic segment, and temporal semantic attribute. Differentiated with his definition, these new encodings could combine atom semantic concepts with temporal attributes, which enable a structure to describe captured domain knowledge and also endow the temporal reasoning capability to better fit the dynamic nature of network scenario. Comparing to most existing semantic extraction approaches, our knowledge-driven approach has a high compatibility for heterogeneous network environments.

The uplift approach invented in this thesis could extract information from low-level to high-level and perform flexibly on different data set input by dynamically invoking corresponding domain knowledge model. By using standard semantic techniques, our knowledge model could interoperate with other semantic knowledge models on the web and the flexibility of our information uplift approach promises the potential to address different network scenario and improve the understanding of non-expert users.

The minor contribution of this thesis is the network monitoring framework to support our knowledge-driven information uplift approach to fit into different network scenarios and promise the visual representation for non-expert users. The implementation of our Semantic Information Uplift engine (CASIU) is the instrument of this framework which was used to showcase its features. And the framework (CasiuVis) has been implemented into four iterative experiments and its details have appeared in several peer-reviewed publications. CasiuVis was deployed in the Science Foundation Ireland funded FAME project, Scenario E, as the novel HAN monitoring tool and our framework is recently deployed in FAME-IBM Tivoli work plan as central technologies, which is aiming to investigate a novel IPTV delivery network monitoring solution. In summary, the successful deployment and evaluation of CasiuVis validates the framework designed, and reinforces the value of our knowledge-driven information uplift approach.

Six papers have been submitted/published in relation to research carried out in this thesis:

"Integration of QoS Metrics, Rules and Semantic Uplift for Advanced IPTV monitoring", Ruairı de Frein, **Yuqian Song**, Rob Brennan, Patrick McDonagh, Cristian Olariu, Adriana Hava, Christina Thorpe, John Murphy, Liam Murphy, Paul French, Journal of Network and Systems Management, 2014

This paper describes the CasiuVis framework with extended semantic encoding and knowledge model to show how it fits into IBM Tivoli IPTV delivery network monitoring scenario.

"Secure Federated Monitoring of Heterogeneous Networks", Rob Brennan, Kevin Feeney, **Yuqian Song**, Declan O'Sullivan, IEEE Communications Magazine, 2013

This paper proposes a novel approach by combining CASIU and federated network monitoring to give the flexibility to deal with the dynamism and diversity of realistic multi-

domain monitoring deployments.

"A framework to leverage domain expertise to support novice users in the visual exploration of Home Area Networks", **Yuqian Song**, John Keeney, Owen Conlan, in Proceeding of the IEEE Network Operations and Management Symposium (NOMS 2012), Maui, HI, USA, April 16-20, 2012.

This paper concentrates on the design, implementation and evaluation of CasiuVis framework. The design of information uplift approach and the knowledge model is given in detail. The implementation of them in CasiuVis as well as the evaluation are also described and discussed in this paper.

"An ontology-driven approach to support wireless network monitoring for home area networks", **Yuqian Song**, John Keeney, Owen Conlan, Philip Perry, Adriana Hava, in Proceedings of International Conference on Network and Service Management (CNSM 2011) Paris, France, October 24-28, 2011.

This paper designs, implements and evaluates the CASIU engine with functionality and usability evaluation in the HAN environment.

"Towards a framework to support novice users in understanding and monitoring of Home Area Networks", **Yuqian Song**, Rob Brennan, Dave Lewis, Owen Conlan, in Proceedings of the IEEE Workshop on Managing Ubiquitous Communications and Services (PerCom 2012 workshop), March 19-23, 2012, Lugano, Switzerland

This paper describes the CasiuVis framework and how it fits into SFI FAME HAN monitoring scenario.

"A Novel Approach to Support the Visual Exploration and Management of Heterogeneous Home Area Network Devices and Services", **Yuqian Song**, John Keeney, Owen Conlan, in Proceedings of International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2011) Nancy, France, June 13-17, 2011

This paper investigates a potential use of information uplift approach and a visual interface to perform HAN monitoring with usability evaluation.

## 1.5 *Thesis Overview*

This thesis is comprised of six chapters.

Chapter Two provides related work of this thesis. This chapter includes a survey of state of the art approaches, a discussion for revealed challenges, and finally a study of cutting-edge research about semantic web, information uplift and visualisation techniques referred in the thesis with conclusion at the end.

Chapter Three describes the design of a semantic information uplift approach with corresponding information representations and network monitoring framework.

Chapter Four describes an evolving implementation process of CASIU engine and its monitoring framework CasiuVis with some code snippets and screen shots attached in two real-world network scenarios.

Chapter Five presents the goals, settings and results of evaluations performed for this thesis.

Chapter Six concludes this thesis. Contributions and future work of this work are also discussed.

# Chapter 2
# State of the Art

## 2.1 *Introduction*

This chapter describes a state of art study of *Network Monitoring Tools for Non-expert Users* and *Information Representation and Uplift Approaches*. The surveys and reviews in this study give special attention to features of approaches, which are relevant to this thesis. After each survey and review, an analysis is approached to discuss and conclude the key findings related to the research in this thesis. The study of existing network monitoring approaches/tools for non-expert users exposes the motivation of this research, which aims to find out what approaches/tools are currently employed, as well as to investigate the paradigm and challenges of network monitoring and what deficiencies approaches/tools suffer from, especially for non-expert users. This study concludes key approaches to face these challenges to uplift and represent meaningful information from the network data. The study of current approaches and related technologies provides this research with a general grounding. It helps the analysis of the research challenges in existing approaches to fulfil the challenges of network monitoring for non-expert users. Key findings from this chapter motivate and influence the design of the novel approach with corresponding models and framework discussed in following chapters. And a functional comparison of five high-impact tools further investigates current attempts to partly overcome these challenges. This comparison also reflects the effectiveness of information extraction approach to simplify network monitoring for non-expert users. The study in this chapter also benefits the iterative approach endowed in this thesis to prototype, validate, and evaluate the design.

## 2.2 *Network Monitoring Tools for Non-expert Users*

### 2.2.1 Introduction

As exposed in the motivation in Section 1.1, the increasing evolving of modern network systems is often accompanying with large amount of monitoring and measurement log data sets which exhibit bewildering complexity and are often beyond the cognitive capability of non-expert users. It is not reasonable to expect non-expert users to acquire appropriate domain knowledge, and in most cases, the assistance from domain experts is expensive or unavailable. This phenomenon happens in many common network scenarios, such as Home Area Networks (HAN) and IPTV delivery networks. As a result, this section firstly reviews traditional network monitoring approaches/tools and analyse these approaches/tools with a series of key findings. By further investigating these key findings, it then presents empirical studies about the information representation and information visualization applied for network monitoring. Followed by an analysis, this section indicates challenges of network monitoring systems for non-expert users. At the end, this section overviews the current network monitoring approaches/tools and concludes key findings and challenges for non-expert users, which also motivates the study of *Information Representation and Uplift Approaches*.

### 2.2.2 Traditional Network Monitoring Approaches and Tools

Network monitoring has a long history in the network community. With tremendous growth in network deployment in the 1980s and 1990s, network monitoring issue became crucial for the network evolving in size and complexity. Monitoring connections across a network can include such diverse activities as supporting network optimization, network planning, security concerns, and troubleshooting [Wilson 2000], which are also fundamental to support modern network management [Comer 2007]. These activities inspect network traffic across a series of network protocols introduced by international standardization bodies and organizations in order to maximize performance, reduce congestion, plan for growth, and identify intrusions effectively. Among the well-known internet and network standards are Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite, Hypertext Transfer Protocol (HTTP), Cisco's NetFlow Protocol [CISCO 1990], IETF's Simple Network Management Protocol (SNMP) [Rose 1996], and OSI's Common Management Information Service (CMIS) [ISO DIS 9595] coupled with Common Management Information Protocol (CMIP) [ISO DIS 9596]. Consequently, a number of common network monitoring

approaches/tools have been introduced to reduce the maintain cost and improve satisfaction for network users:

#### *2.2.2.1 Network Traffic Analysis*

Network traffic analysis helps with network performance assessment and optimization. A number of tools for network traffic analysis (also called network sniffers, packet sniffers, or IP sniffers) capture all incoming and outgoing packets passing through the network entities, such as individual links, network elements, network services, and applications [Comer 2007] and measure them according to the latency, throughput, packet loss, jitter, availability and transmission protocols. Then they provide comprehensive visualized reports and charts to help users analyze network behaviors. These tools demonstrate the range of possible ways flow analysis could be applied, such as Traffic Characterization, Throughput Estimation, Accounting and Billing, Ingress/Egress Traffic Comparison, Confirming Quality of Service, Anomaly Detection, Security Analysis, Real-time Troubleshooting, After-The-Facet Forensics, Capacity Planning, Application Measurement and Planning, etc. These flow analyses are applied into numerous proprietaries and free traffic analyzers based on current network protocols. Focusing on basic IP flow, these include naturally tcpdump [tcpdump 1999] , and specialized tools as FlowMon [FlowMon 2008], which is a monitoring solution by providing wire speed processing with no packet loss, for all types of networks from 10Mbps to 10 Gbps. By extending the protocol compatibility, Netflow Analyzer [Netflow Analyzer 2011] is a product which has partnership with Cisco and 3COM and specifically meant for Traffic Analysis and Network Forensics, therefore, gives an in-depth visibility into the network traffic, bandwidth utilization, top-talkers in the network from various flows. NetQoS [NetQoS 2005] inspects NetFlow whith pre-defined thresholds to identify when and where problems are occurring or occurred, identify viruses using real time reporting, remove unwanted traffic instead of unnecessarily upgrading links, view and plan the impact of applications on the network over time. OpenFlow [OpenFlow 2008] is an open interface for remotely controlling the forwarding tables in network switches, routers, and access points. It is gaining considerable attention as the technology moves from research labs into mainstream products with providing a library [Liboftrace 2012] for monitoring and debugging OpenFlow control traffic and an extensible foundation [ENVI 2012] for OpenFlow-related networking visualizations. AURORA [AURORA 2007] is an IBM Research project targeted at investigating further analysis based on flow-based network traffic monitoring and visualization for very large networks on anomaly and virus

detection/mitigation, network forensics, distributed flow processing, BGP/OSPF/RIP monitoring, traffic network maps and indexing of very large flow repositories. Network traffic analysis is a fundamental approach for a range of other network monitoring activities.

#### *2.2.2.2 Network Security Monitoring*

Network security monitoring is a well-developed area and network security itself is a process of continually improvement instead of a goal—although no network can be absolutely secured. A large amount of tools has been developed and kept evolving to perform the monitoring for the security concerns of identity, authentication, authorization, data integrity, privacy and confidentiality. Nsauditor [Nsauditor 2006] is a network security scanner that allows to audit and monitor network for possible vulnerabilities, checks methods that a hacker might use to attack it. Lan-Secure [Lan-Secure 2011] provides real-time intrusion detection and prevention by enforcing network policy organization rules and online network users activity management. Wormholes (IVoW) [Wang and Lu 2007] is an interactive network intrusion detecting visual tool, which uses an automatic detection algorithm to help detect intrusion in large-scale wireless networks in real time. It adopts various visual forms to assist in the understanding and analysis of wireless network topology and to improve detection accuracy. Although network security monitoring is not the focus in this thesis, the approaches and techniques used in this area, e.g. behavior modeling, real-time processing, anomaly representation, can still inspire and benefit the research in this thesis.

#### *2.2.2.3 Network Troubleshooting*

Network troubleshooting is adapted to refer to process of finding the cause of a network problem by capturing and inspecting the characteristics of incomplete data, high rate of events, and simultaneous presence of several problems, which is usually benefited by the expert knowledge [Mathonet et al. 1987]. By inspecting network infrastructures, Etherpeek [Etherpeek 2002] is an Ethernet network traffic and protocol analyzer designed to assist in troubleshooting and debugging mixed-platform, multi-protocol networks. AlertFox [AlertFox 2011] supports transaction monitoring of web applications that use complex HTML, AJAX, Flash, Flex, and Silverlight, by providing in-depth root cause analysis for trouble-shooting sporadic issues. There are also diagnostic tools that help check the availability, reachability, and health of the network or the host in a network using ICMP and SNMP [NetPrefect 2009] [GNetWatch 2008]. The network troubleshooting is also widely applied for a range of network services. NetQoS

VoIP Monitor [NetQoS 2005] tracks the call quality user experience, provides alerts on call performance problems, and isolates performance issues to speed troubleshooting and MTTR. Netrounds [Netrounds 2011] is a novel cloud-based solution using distributed active measurement probes deployed on PC hardware to support concurrent monitoring of SIP signalling performance and ongoing call quality, as well as live IPTV MPEG monitoring in combination of flexible TCP/UDP traffic. In most cases, network troubleshooting always accompanies with other network monitoring purposes, which requires a more structural approach to support the troubleshooting across a number of different network components and services.

#### *2.2.2.4 Network Monitoring Platform*

As the network complexity grows, the market demands for more flexible monitoring systems rather than specialized tools (like most tools listed above). These specialised tools are designed to collect information required for some particular analysis. They often depend on a particular version of a protocol, or a particular configuration of the underlying infrastructure. For example, NetQoS [NetQoS 2005] only works with Netflow protocol to identify network problems, remove unwanted traffic instead of unnecessarily upgrading links, view and plan the impact of applications on the network. Such dependences make most existing tools hard to adapt the change of network infrastructures or configurations. These require a platform should permit to ensure functional performance with the heterogeneous rapid evolving network structures, protocols, and services. Some more general and flexible monitoring approaches have been developed. OpenNMS [OpenNMS 1999] was announced as the world's first enterprise-grade network monitoring/management integrated platform developed under the open source model. It is designed to scale to tens or hundreds of thousands of managed nodes from a single instance. OpenNMS provides service availability management, performance data collection via most common protocols, such as SNMP, JMX, HTTP, WMI, XMP, etc., event management by supporting internal events, custom events via an XML/TCP interface, and external events via SNMP traps and TL1, event de-duplication, and flexible notifications (via SMTP, XMPP, and many other protocols). Another research focused system, Pandora Monitoring Platform [Patarin et al. 1999], is designed as a flexible network monitoring platform to monitor and detect network systems using remote tests (ICMP, TCP Sweep, Network scan, and SNMP monitoring), or using local agents to grab application/system data (has agents for Linux, AIX, HP-UX, Solaris and Windows XP,2000/2003). Pandora is able to fire alarms, draw graphs and

keeps event history for each element using a SQL backend. Lemon [Lemon 2012] is a new server/client based monitoring system with monitoring agents on every monitored node using a push/pull protocol to communicate with sensors, which are responsible for retrieving monitoring information. The extracted samples are stored on a local cache and forwarded to a central Measurement Repository using UDP or TCP transport protocol with or without authentication/encryption of data samples. Sensors can collect information on behalf of remote entities like switches or power supplies. The Measurement Repository can interface to a relational database or a flat-file backend for storing the received samples. Web based interface is provided for visualizing the data. A semantic framework [Viswanathan et al. 2011] is designed is to enable semantic analysis at a level closer to the user's understanding for the network security monitoring. The key to their approach is the introduction of a logic-based formulation of high-level behavior abstractions as a sequence or a group of related facts, which allows treating behavior representations as fundamental analysis primitives, elevating analysis to a higher semantic-level of abstraction. This framework demonstrates emphasizes reuse, composibility of higher-level models and extensibility of abstractions by applying it to security analyses tasks. Netcool [Netcool 2006] suite offers five product families that support domain-specific IT management, end-to-end consolidated operations and business service network management by enabling to identify and resolve the most critical problems with automated event correlation, isolation and resolution capabilities. Netcool has been deployed successfully focusing on heteronomous network environments over the world. Current network monitoring platforms and structures can effectively support diverse monitoring purposes through a range of network standards and protocols over large-scale commercial networks.

#### *2.2.2.5 Key Findings*

According to above empirical studies, a variety of common network monitoring approaches are introduced with representative tools for diverse specified purposes. Network traffic analysis is a fundamental approach to address network performance assessment and optimization. This approach is applied on specified current network protocols and interfaces (TCP/IP, Netflow, OpenFlow, etc.) and inspects the measurements through network entities. Most current tools use a set of pre-defined thresholds adapted on measurements of network log data. The triggered thresholds are reported via visual widgets to display data trend, historical review, network status, etc. Network security monitoring usually inspects network activities, diagnosis threaten with algorithms and rules and then visually report problems. Based on traffic

analysis approaches, network troubleshooting is a process of finding the cause of a network problem by capturing and inspecting the characteristics of incomplete data, high rate of events, and simultaneous presence of several problems, which is usually benefited by the expert knowledge. A set of specialized approaches is aggregated on platforms to ensure a more general and flexible network monitoring with the heterogeneous rapid evolving network structures, protocols, and services.

By reviewing these approaches/tools, the following points have been analysed and identified as critical findings to motivate the following state of the area research and influence the design in next chapter:

- **Disparity of Monitoring Resources:** Current network monitoring tools are experiencing increasing difficulties caused by the disparity of the monitoring resources. Modern network systems are built on a number of highly heterogonous network elements and services. Most network elements (e.g. laptop, mobile device, router, DSLAM, server, etc.) are from different vendors and domains and interconnect to each other via different network standards and protocols (TCP/IP, HTTP, NetFlow, SNMP, CMIS, CMIP, OpenFlow and others). Rapid increasing and evolving network services (e.g. IPTV, VoIP, On-line Gaming, etc) also lead to growing monitoring complexity. This disparity nature of the monitoring resources increases challenges with a large of amount heterogeneous log data. A large amount of tools was developed focusing on one or several sorts of network protocols [tcpdump 1999] [NetQoS 2005] [Liboftrace 2012], network elements [Network Magic 2012] [Etherpeek 2002] [PRTG 2004], and network services [NetQoS 2005] [Netrounds 2011]. Such dependences make most existing tools hard to adapt increasing monitoring requirements. As a solution, an integration approach was developed to aggregate monitoring log data from diverse network resources to enable a more general and flexible network monitoring. Existing solutions [OpenNMS 1999] [Lemon 2012] [Netcool 2006] usually adapt a common model to represent the information from diverse network resources. Especially, a framework [Viswanathan et al. 2011] demonstrates the capability of semantic web techniques to model not only the information directly from network resources, but also high-level behaviour abstractions.

- **Complexity of Monitoring Purposes:** Current network monitoring is no longer satisfied with onefold purpose. The increasing complexity of network normally leads to

compose monitoring purposes to directly express user demands, which are referred as high-level monitoring objectives. Comparing to onefold purpose monitoring tools as tcdump, [tcpdump 1999] FlowMon, [FlowMon 2008] and Liboftrace [Liboftrace 2012] for flow-based analysis; PRTG [PRTG 2004] and Network Probe [Network Probe 2003] for network status monitoring; Etherpeek [Etherpeek 2002] and AlertFox [AlertFox 2011] for single purpose troubleshooting; and Telchemy [Telchemy 2003] and SevOne VoIP [SevOne VoIP 2010] for VoIP service quality monitoring, composed monitoring purpose requires an one-stop solution for disparity of monitoring resources and fickle monitoring requirements for network users/administrators to support higher level network monitoring/management objectives. Thus, some solutions [OpenNMS 1999] [Patarin et al. 1999] [Netcool 2006] provide an open interface to integrate diverse monitoring/management components and models across a range of network resources to support domain-specific IT management, end-to-end consolidated operations and business service network management by enabling to identify and resolve the most critical problems with automated event correlation, isolation and resolution capabilities. These solutions mostly focus on the large-scale commercial network systems, and also require certain understanding and knowledge of the network system for using and configuring, which require well-trained network administrators.

- **Requirement of Expert Knowledge**: The disparity of monitoring resources and the complexity of monitoring purposes require invoking expert knowledge to ensure the function and improve the intelligence of monitoring systems. The way to adapt the expert knowledge depends on the purposes of network monitoring. For the specialised flow-based analysis, Netflow Analyzer [Netflow Analyzer 2011] and NetQoS [NetQoS 2005] adapt a simple utilisation of expert knowledge with pre-defined thresholds and some other approaches in HomeMaestro [Athanasopoulos et al. 2008], OneClick [Chen et al. 2009] and EmNet [Miller et al. 2009] apply monitoring algorithms with expert adjusted parameters. In order to support more complex monitoring purposes, expert knowledge is usually captured and modelled into knowledge representations for network optimisation, security, troubleshooting, and integration with network management. In a range of cut-edge systems [Yang et al. 2010] [Sventek et al. 2011] [Lemon 2012], policies are well developed [Strassner 2004] and widely adapted to capture the domain expert knowledge and enforce logical computation on the network

log data to support network control and troubleshooting. However, as Strassner [Strassner 2004] stated, policies are challenged to encode and update for domain experts. Some other frameworks [Viswanathan et al. 2011] [Vergara et al. 2008] semantically represents expert knowledge in a more explicit, formal, and shareable way [Vergara et al. 2009].

- **Visual Representation of Monitoring Information**: The complexity and real-time nature of network determine the monitoring information is always overladen for the human network users. The current approaches/tools are approaching this challenge from two ways: optimise the monitoring information and improve the visual representation. tcpdump [tcpdump 1999] presents network traffic information by command lines in the system console, which is easy to invoke but restricts the knowledge requirements for understanding. FlowMon [FlowMon 2008] and Netflow Analyzer [Netflow Analyzer 2011] analyses the monitoring information and highlight the information with visual widgets for network traffic comparison, historical review and network topology. Focusing on the overload information from large-scale commercial network, some systems [Netcool 2006] [Patarin et al. 1999] contain a set of visual views to represent the monitoring information for different monitoring purposes. The visual widgets also keep evolving by adapting the information visualisation techniques. As a common way, a set of charts, like pie chart, line chart, bar chart, geo-map, graph chart, is widely used in existing monitoring tools [NetQoS 2005] [Netflow Analyzer 2011] [Etherpeek 2002] [Netcool 2006]. However, these visual widgets still require a certain degree of network knowledge to understand the network status for diagnosis, analysis, and identification of network problems. Some novel projects [Viswanathan et al. 2011] [Yang et al. 2010] [Sventek et al. 2011] propose new visual representations to provide better understanding for high-level monitoring objectives, but it still needs further investigation in this area to reduce the understanding barrier.

Concluded from the review and analysis of current approaches and tools, a system that intends to perform heterogeneous network monitoring tasks must obtain data values that correspond to conditions in the network. Thus, a typical network monitoring system follows a basic paradigm [Comer 2007]:

- Import network information from the underlying resources, and then maintain the

information in storage.

- Utilize the imported information to perform the necessary computation based on domain knowledge.

- Display information after the computation for a user/administrator.

As reviewed, network information is imported from network resources and maintained in different ways: some tools [FlowMon 2008] [NetQoS 2005] [Etherpeek 2002] load information about network traffic flow from real-time stream data into memory and trigger thresholds embedded into system logic; some systems [Lemon 2012] maintain captured information in a database with SQL access; and other approaches [Viswanathan et al. 2011] [Sventek et al. 2011] capture the information from different network sources and model them with domain knowledge models. The imported information is then performed necessary computations for different monitoring purpose based on expert knowledge: Netflow Analyzer [Netflow Analyzer 2011] and NetQoS [NetQoS 2005] apply comparison with expert-defined thresholds and focusing on more complex monitoring purpose, some tools Netcool [Netcool 2006] [Viswanathan et al. 2011] [Sventek et al. 2011] use modeled expert knowledge to perform necessary computations to achieve higher level meanings. The computed information is displayed to human user/administrator via a range of visual representations. Thus, the scope, functionality and limitation of a monitoring system are inherently linked to the available information exchanged with network resources. In another word, the way to deal with information determines to what extent a monitoring system can monitor. Hence, the representation of information is tight coupling to the challenges of **Disparity of Monitoring Resources, Complexity of Monitoring Purposes** and **Requirement of Expert Knowledge** of all sorts of network monitoring systems. A study of ***Representation of Information in Network Monitoring Systems*** is performed in next section. The final consumer of a network monitoring system is human users/administrators. A study of ***Information Visualisation in Network Monitoring Systems*** is also performed in another section to discuss the challenges addressed in **Visual Representation of Monitoring Information**.

### 2.2.3 Representation of Information in Network Monitoring Systems

This section aims to review existing information representation approaches in network monitoring systems and exposes the challenges in **Disparity of Monitoring Resources**,

**Complexity of Monitoring Purposes** and **Requirement of Expert Knowledge** of all sorts of network monitoring systems, which influence the design and evaluation in this thesis. As discussed in Section 2.2.2.5, in order to achieve a functional network monitoring system, two types of information must be imported:

- Information obtained from network resources that give the current state of the network.
- Information inputted from domain knowledge, such as a set of rules to govern decisions about network troubleshooting.

Due to the difference in origin, the representations of two types of information usually differ. For example, information imported from domain knowledge is always in a representative description (e.g. policy) which allows computation and logical reasoning, but the information from network resources is mostly stored in pre-defined metrics, which are usually restricted to the manufacturer or underlying protocol. Moreover, the challenges of **Disparity of Monitoring Resources, Complexity of Monitoring Purposes** perform a need for representations of heterogeneous network elements and the information representation for domain knowledge is discussed to fulfil the **Requirement of Expert Knowledge**, which are further discussed in following two sections. And the key findings are presented in the last section.

#### *2.2.3.1 Representation of Information from Network Resources*

This section presents a study of information representation for network resources. In both industrial and academic field, people are always trying to find a consistent, uniform, internal information representation for network resources. An information model [Strassner 2004] is a common abstraction and representation to accommodate the features and functions of heterogeneous network components in policy-based network monitoring/management systems. A range of information models are developed such as the Common Information Model (CIM) [CIM 2004], the TMF Shared Information/Data Model (SID) [SID 2005], and DEN-ng [Strassner 2002], which facilitate a unified and consistent representation of polices across a wide spectrum of network domains. By focusing on the subset of relevant information model, Barrett et al. [Barrett et al. 2007] proposed a novel method to tag and extract only relevant aspects and leverage existing models in defining ontologies to facilitate enhanced representation, exchange, integration and querying of information by annotating data with

formal semantics and thus allow for automated reasoning. Model-driven architectures enable automatic monitoring/management to some degree and to control the allocation and use of network resources according to the monitoring/management purpose. The problem to be solved is the mapping of high-level monitoring objectives in the information model to low-level information from diverse network components. In an early investigation of Sloman [Sloman, 1994], an architecture was developed to make use of a common set of underlying management services for monitoring and manipulating domains and policies in order to express management objects to meet the requirements of particular applications. To operate, maintain, and secure a communication network, network operators must grapple with low-level vendor-specific configuration to implement complex high-level network policies [Kim et al., 2013]. The model-driven architecture was then well developed and widely used in a board range of applications. Kosiour [Kosiour, 1999] implemented a "mainstream" model-driven system with IETF model and they proved their system was better than some other contemporary management systems at that time. IBM developed an architecture to support self-management by using policy-based management for autonomic computing [Agrawal, etal. 2005]. Another trend of this research focuses on Service Level Agreement (SLA) monitoring with Quality of Service (QoS) and also the perceived Quality of Experience (QoE) for the user. Focusing on the Quality of Experience which offers guidance to present the deeper understanding of user's purpose and needs, Sheridan-Smith [Sheridan-Smith et al. 2003] proposed a system with a service-oriented architecture to ensure the scale of millions of users. Kharbili et al. [Kharbili et al. 2008a] [Kharbili et al. 2008b] presented a semantic policy-based approach to apply compliance management of business processes in a semantically-enabled environment and discuss why leveraging compliance checking to a semantic level enhances compliance management. However, most current systems still lack appropriate representations for harmonizing the cross-domain information from network resources in diverse monitoring aspects and the underlying information models are hardly in coping with high-level monitoring goals.

#### *2.2.3.2 Representation of Information from Domain Knowledge*

The information from domain knowledge in network monitoring systems is used to enable translation/code generation and logical reasoning processes that automatically focus network elements in response to monitoring goals and/or the environmental context. As a common representation of domain knowledge, Sloman and Lupu [Sloman& Lupu 2002] defined polices as "rules governing the choices in the behavior of a system". Since work of Damianou et al

[Damianou et al. 2000], polices are used to capture high-level business-driven behaviours by applying different policies to change the behaviour of the system. They defined a policy language, Ponder, and codified four types of basic polices, authorization policies, refrain policies, obligation polices and delegation polices, to develop a translation from high-level business-oriented specifications of behaviour to lower levels of specification. All basic polices can be specified as parameterized types to correspond to classes defined in an information model. As Sheridan-Sminth [Soliman et al. 2008] analyzed, policies could benefit the network monitoring/management system from a series of aspects: enable automatic management, support higher level goals, consistent end-to-end behaviour, etc. Currently, there are three main policy models in the industry: DEN model [Strassner 1999], IETF model [Moore et al. 2001], and the DMTF model [DMTF 1992]. According the policy models, policy languages provides the ability to translate the information model with formal and concise syntax. PAX-PDL [PAX-PDL 2002], SRL [Brownlee 1999], and PPL [Stone et al. 2001] were first proposed for pattern matching in the selection of the network traffic on which a policy can be applied. These are relatively low-level policy languages with limited efficiency since they do not provide a view of how the overall policy managed network system will work. Within high-level policy language, policies are generally viewed as using event-condition-action (ECA) rules. Policy Description Language (PDL) [Lobo et al. 1999] is a declarative policy definition language for system management formulates policies using the ECA rule paradigm of active databases and extends it by providing a rich event sub-language allowing only uninterrupted concurrent actions. Some of the languages are based on formal logic grounds such as PDL which is flexible to represent a wide range of policies and at the same time formal enough to support automatic translation to logic [Stone et al. 2001]. Meantime, the policy could also be encoded into XML and other semantic format such as RuleML [Boley et al. 2001]. These policy languages we mentioned have been compared and analyzed by Aib et al. [Aib et al. 2003] from several aspects. At present, policy languages still lack consistency, especially for highly heterogeneous network components, and even supported by a range of authoring tools, it is not convenient to encode and update by domain experts. Furthermore, it is also hard to interpret with information inputted from different domain knowledge to overall high-level monitoring goals.

The autonomic monitoring/management are designed as a further solution. Autonomic Computing was first proposed by IBM in 2001 [IBM 2001]. The research space of autonomic

computing was divided into three basic parts by Kephart [Kephart 2005]: autonomic elements, autonomic systems and human-computer interactions. Any type of computing resource could be considered as an autonomic element, which is the basic block of autonomic systems and produce the self-managing behaviour by mutual interactions. Autonomic systems entail "interactions among multiple autonomic elements to achieve system-level goals, including problem determination and remediation, automated provisioning, work-load management, automated installation and configuration, integrity management, etc" [Kephart 2005]. Kephart also indicated one challenge for individual autonomic elements is the standard interface, which could be capable of requesting and generating information from other elements. One notable solution is Common Base Event Format [IBM 2004], which defined a consistent and common format for monitored events and log files. Rule engines and correlation engines (like Drools [Drools 2007]) are also successful for analyzing the monitored data and log files to identify trends or situations of autonomic elements. Advances in OWL [Dean et al. 2004] to develop semantically modelled resources also enable autonomic elements to discover and interact with each other more effectively by expressing their needs, capabilities and properties. Ontology-based information representation has recently evolved from a theoretical proposal to a more mature technology for network monitoring, which is considered as a novel and effective strategy to overcome network complexity by involving ontology-based modeling and reasoning; Hoag [Hoag et al. 2006] presents an approach to apply semantic reasoning techniques for network management and resource allocation to avoid overbuilding and improve quality. FOCALE [Strassner et al. 2006] is a semantically rich architecture for orchestrating the behavior of heterogeneous and distributed computing resources. Vergara [Vergara et al. 2009] described and summarized several ontology-driven network management and monitoring projects, detailing the most important facets of how semantic technologies were applied and explaining the advantages and drawbacks. In his paper, he found semantic technologies are explicit, formal, and shareable, which means the ontology-based modelling and reasoning could be composed with other semantic techniques to express the formal network monitoring and management logic and improve current approaches. A project [Guerrero et al. 2006] proposed an ontology-based formal definition of the different management behaviour specifications integrated with the management information definitions, in which SWRL rules are defined directly over the ontology elements and allow for logical reasoning. Another ontology-based approach could dynamically evoke the internal and external ontology models, which remedies the shortcomings of some policy-based approaches. Moreover, the measurements provided by

different network monitoring tools and platforms could be modelled and integrated with a syntactic ontology-based solution [Vergara et al. 2008]. However, this success is associated with a challenge of how the domain knowledge could be applied to define a good set of rules to describe the conditions of events in an automatic detection process with service-level goals. Some initial efforts have been implemented including in the work of Hewlett-Packard Labs [Zhang et al. 2005] and IBM research [Breitgand et al. 2005] to automatically correlate low-level system measurements up and drill down high-level objectives. Up to this paint, a main problem is to populate the correlated knowledge and to develop methods for searching and adopting it effectively. A research team of IBM's Almaden Research Center [Barrett et al. 2004] has been conducting graphical studies of system administrators, observing their behaviour as they plan and rehearse complex system upgrades and diagnose problems. Although this work is still in a preliminary stage, it has led to some important insights about the nature of information models that suggest more flexible representation of information enabling humans to specify their goals in a nature manner to monitor, visualise and even control autonomic systems with sufficiently expression of cost and performance. The further investigation is still desired in this area.

#### *2.2.3.3 Key Findings*

This study reviews the representations of information in network monitoring systems. A series of key finding in current information representations are exposed in coping with the challenges of **Disparity of Monitoring Resources, Complexity of Monitoring Purposes** and **Requirement of Expert Knowledge** derived from key findings in Section 2.2.2.5.

1) **Representation Challenges for Monitoring Resources:** Aiming to the disparity nature of monitoring resources, a serious of common information models [CIM 2004] [SID 2005] [Strassner 2002] is developed and some other approaches [Barrett et al. 2007] adapt semantic models to facilitate enhanced representation, exchange, integration and querying of information by annotating data with formal semantics and thus allow for automated reasoning. A list of challenges still remain in this area:

   - **Insufficient Representation for Heterogeneous Monitoring Resources:** Although current information models [CIM 2004] [SID 2005] [Strassner 2002] provides unified and consistent representations for monitoring resources, the disparity nature of network require a more flexible and extensible approach to model the resources from different

aspects, such as QoS and QoE, and the higher level abstraction objects like the behaviour, business objective, and anomaly. Current semantic approaches [Barrett et al. 2007] partly solve this problem, but still need explicit representation to describe the logical relationship of diverse monitoring resources in different domains and abstraction levels.

- **Difficulties for Creating and Updating Information Representations:** The information models [CIM 2004] [SID 2005] [Strassner 2002] (including semantic models [Barrett et al. 2007]) lack standards or an incomplete analysis of the domain, which might have a ripple effect when the domain data model changes.

2) **Representation Challenges for Monitoring Purposes:** In order to achieve complex monitoring purposes, model-driven architectures [Sloman, 1994] [Kosiour, 1999] [Agrawal, etal. 2005] enable automatic monitoring/management to some degree and to aggregate the information about allocation and use of network resources according to the monitoring/management purpose. A list of challenges still remain in this area:

- **Challenges for High-level Monitoring Information Representation:** Current model-driven architectures [Sloman, 1994] [Kosiour, 1999] [Agrawal, etal. 2005] are built on the underlying data model and to achieve the monitoring goals by encoded policies/rules, which are only enforced when the monitoring goal is triggered, such as troubleshooting, network optimisation, or reconfiguration. However, this approach only models the low-level information of the underlying data, like packet loss, throughtput, and signal strength in the data model, which lacks higher level understanding of the characteristics and meanings of the data. This approach sometimes may cause the understanding barrier for the network users/administrators and also the difficulties to encode policies/rules for domain experts, who have to achieve every monitoring goal by encoding policies/rules for underlying data. The rich expressive of this approach is suitable for large-scale commercial network systems, where have enough expertise support and well-trained administrators. But it is obviously too "heavy" for some small networks, like home networks.

- **Challenges for Cross-domain Monitoring Information Representation:** There is a large range of policy/rule languages to provide expressivity to derive complex monitoring purposes [Strassner 2002]. However, the higher level monitoring purposes

like troubleshooting may invoke the monitoring information from different monitoring domain, such as Service Level Agreement (SLA) monitoring with Quality of Service (QoS) and also the perceived Quality of Experience (QoE) for the user [Sheridan-Smith et al. 2003]. This presents a challenge for cross-domain information representation.

3) **Representation Challenges for Expert Knowledge:** The information from domain knowledge is used to enable necessary computation and reasoning that automatically focus network elements in response to monitoring goals and/or the environmental context. A number of models (DEN model [Strassner 1999], IETF model [Moore et al. 2001], and the DMTF model [DMTF 1992]) and languages (PAX-PDL [PAX-PDL 2002], SRL [Brownlee 1999], and PPL [Stone et al. 2001]) is used to encode and model the domain expert knowledge with event-condition-action (ECA) rules. As a further evolution, the autonomic monitoring/management are performed with three basic parts [Kephart 2005]: autonomic elements, autonomic systems and human-computer interactions. The domain knowledge here is the core component to enable the autonomy and it is represented with Common Base Event Format [IBM 2004], rules [Drools 2007] or semantic modelling [Hoag et al. 2006] [Strassner et al. 2006] [Vergara et al. 2009]. A list of challenges still remain in this area:

- **Degree of Autonomy Ensured by Expert Knowledge:** A series of existing systems promised the information from expert knowledge can ensure certain degree of autonomy. The study in autonomic network monitoring [Kephart 2005] demonstrates the representation of expert knowledge enabling interpretation across autonomic elements, autonomic systems and human-computer interactions is the key point to promise the autonomy of network monitoring. This requires an explicit, formal, and shareable representation for domain knowledge. Semantic techniques are widely applied in a range of autonomic systems [Vergara et al. 2009] [Guerrero et al. 2006] [Strassner et al. 2006] to represent the expert knowledge. However, this success is associated with a challenge of how the domain knowledge could be applied to encode a good set of knowledge representation to enable the intelligence of an automatic monitoring system with high-level goals. In addition, most semantic approaches are adapted statically, but the autonomy of a real-time network monitoring requires dynamic modeling and reasoning capabilities [Vergara et al. 2009], which is another challenge for current semantic approaches.

- **Drill-down Analysis Ensured by Expert Knowledge:** According to the model-driven architectures [Sloman, 1994] [Kosiour, 1999], the network information should be able to use for presenting high-level monitoring purposes, which normally supports the drill-down analysis back to the low-level monitoring information. The systems from Hewlett-Packard Labs [Zhang et al. 2005] and IBM research [Breitgand et al. 2005] to automatically correlate low-level system measurements up and drill down high-level objectives. For example, the high-level business goals can be enforced and monitoring based on low-level information from network resources, whilst the troubleshooting is also supported to track the failure back to the underlying resources. Up to this paint, a main problem is to populate the knowledge representation for both low-level and high-level information and to develop methods for adopting it effectively.

The study in this section investigates how the information representation is coping with its domain knowledge to support monitoring from diverse network resources and achieve complex monitoring purposes. This study also summaries the semantic approach can remedy the shortcomings of some traditional representation approaches by providing a more consistent and uniform structure, which shows the possibilities to support more comprehensive cross-domain reasoning and even establish the understanding between high-level monitoring objectives and low-level network resources. The challenges stated in key findings are discussed in coping with the challenges of **Disparity of Monitoring Resources, Complexity of Monitoring Purposes** and **Requirement of Expert Knowledge**. The study of information visualisation is addressed in next section.

### 2.2.4 Information Visualisation in Network Monitoring Systems

The information generated in network monitoring is usually awkward for human users. Traditional strategies of understanding for comprehension and retention for coping effectively with increasingly complex information are influenced by the changes in the amount and complexity of information. As Keller [Keller et al. 2005] stated, Visualizations capitalise on several characteristic features of human cognitive capabilities to represent a complex concept structure externally in a visual display, which is sometimes more effective than literal and verbal representations [Ware 2004]. This section aims to review the current information visualisation and semantic visualisation techniques and investigates how they are adapted to fulfil the challenges in **Visual Representation of Monitoring Information** to improve user

experience.

#### *2.2.4.1 Information Visualisation*

The term, "Information visualization", for visualizing abstract data structures can be tracked back to the Xerox Palo Alto Research Centre in Palo Alto (USA) at the beginning of the 1990s [Dabler et al. 1998]. Since then, Information Visualization has become an autonomous and rapidly growing research area by using computer-supported, interactive visual representation in the context of processing, comprehension, and retention of information, including objects, dynamic systems, events, processes and procedures, in a static, animated, dynamic, and interactive graphics [Card et al. 1999]. According to the research of Shneiderman [Shneiderman 2005], he defined the type of Information Visualization to depend on both the underlying data type and the demands of the users. Regarding the data type, he differentiates between one-dimensional, two-dimensional, three-dimensional, temporal, multi-dimensional, tree, and network data. Text information like documents, source code, could be classified as one-dimensional. Maps, floor plans, grids belong to two-dimensional and physical objects are three-dimensional. Multi-attribute data may be presented as a multi-dimensional type. The temporal type stands for the time-varying data. Tree and network type are used for hierarchical data and arbitrary relationships between objects. With respect to the needs of users, the tasks of Information Visualization could also be classified by overview, zoom, filter, details-on-demand, relate, history, and extract [Shneiderman 2005]. These tasks aims to get a general view, to support zoom in/out operations or to execute queries from the visualization interfaces. In addition, some complex tasks are also desired, such as showing details based on user demand, presenting related information, supporting historical review, and extracting raw information. Dashboards are used to support a broad spectrum of information visualization requirements, spanning the entire range of data that could offer an immediate overview of information. Few [Few 2006] classified dashboards by three rules, strategic, analytical, and operational. In his opinion, dashboards should provide a quick overview for the decision maker to monitor or forecast. For analytical proposals, the analytical dashboard should present the information with the situation of greater context, more extensive history and suitable performance evaluation. The characteristic of an operational dashboard is to offer an interactive interface between user and data.

In particular, Becker et al. applied the visualization techniques to network data [Becker et al. 1995] and indicated data from networks is plentiful and by visualizing this data, it is

possible to greatly improve human understanding. Information visualization also plays an important role in the network monitoring. By consuming network traffic logs, a series of successful approaches and systems has been adapted to aggregate, analysis and represent the network information for the monitoring purpose [Camden et al. 2004] [Keim et al. 2006] [Kikuchi et al. 2007]. These tools usually present network information in various visual views to effectively visualize large number of network nodes [Abello et al. 1999], network topologies [AURORA 2007] [Netflow Analyzer 2011] [Network Magic 2005], network intrusion detection [Ball et al. 2004] [Papadopoulo et al. 2004], etc. However, there are still natural boundaries in current approaches to visualizing network monitoring information. Existing information visualization techniques normally require well-structured and prepared information and the visualization of real-time heterogeneous data sets is still difficult [Herman et al. 2000]. Due to these boundaries, understanding and abstracting overload information, like information from a large amount of network resources, is a challenge in this area.

#### *2.2.4.2 Semantic Visualization*

Regarding the synergy between information visualization with semantic information processing technologies, some ideas and systems have already been designed and developed in order to efficiently abstract and present the semantically meaningful information. According to Geroimenko and Chen's book [Geroimenko et al 2006], the central idea of semantic visualization is to make the overload information associated with semantic structure to be more understandable to human by using visualization theories and methods to clearly indicate the meaning of information so that people can make more use of this gigantic asset.

One typical kind of solutions is to adopt and apply existing information visualization technologies to show the pre-processed and well-structured semantically meaningful information. Focusing on the large amount of Linked-Data from Wikipedia, "Thinkbase" [Hirsch et al. 2008] provides a highly interactive and human understandable visual interface to expose and present linked-data in a relational graph. Compared to a traditional knowledge/information repository, a contribution of this system is the ability to explore a more effective and efficient way to understand and explore linked information for normal users. Currently, there is one sort of visualization layout for semantic data presentation. "GViz" [Frasincar et al. 2003] is a project to graphically show the relationship of RDF generated by RDF/OWL editor, such as Protégé. In addition, it could provide a customized interface for users to choose different visualization methods to present data. However, no user centric operation or

exploration is available, such as querying or filtering the graph. "CCA viewer" [Wienhofen 2004] is an application designed for visually representing ontologies and for searching Semantic Content. One of the benefits of this approach is that highly interactive query operations can be translated into different query languages. This is a bridge between abstract operation and visualization presentation.

Another type of solution offers novel techniques in order to support the interactive operation to create, update, delete and search semantic information in an effective user interface. Brussell [Wagner et al. 2009] is a system that "presents a novel, structured interface for navigating among the events of a news situation by using content- specific models of news event situations to perform anticipatory information retrieval and organize extraction results". Compared to traditional systems, Brussell provides semantically meaningful visual-label-based information retrieval and organization for convenient news reading and reflects the benefit of semantic visualization technology. NITELIGHT [Russell et al. 2008], designed and developed by University of Southampton, is a web-based graphical tool for semantic query design by using a Visual Query Language (VQL) to provide graphical formalisms for traditional SPARQL query specification. It is a good example of how to facilitate complex and abstract query operations in a semantic meaningful visualization method. Hildebrand's research [Hildebrand 2009] investigates how to develop Web-based user interfaces for Semantic Web applications using commonly available, off-the-shelf widget libraries. As further investigation, his research provides an in-depth investigation of combining the Semantic Web and Visualizations and indicates the model of web widgets could make semantic data to "understand" the meaning of visual components, which significantly eases the cost of web widget reusability.

Semantic Visualisation is a novel research area, but its value has already been proven to provide better understanding on structured semantic information and an effective to interact with this information, especially for the people with not too much corresponding knowledge.

#### *2.2.4.3 Key Findings*

This section introduced theories, methods and applications of information visualisation and semantic visualisation for network monitoring. By adapting information visualisation techniques, dashboards can effectively present different types of information [Shneiderman 2005], and are widely used in network monitoring and management fields to visualise the real-time stream data. As a new concept, semantic visualization [Geroimenko et al 2006] can

efficiently associate the monitoring information with semantic structure and present them more understandable to human by using visualization theories and methods to clearly indicate the meaning of information so that people can make more use of this gigantic asset. A list of challenges still remains as the key finding of **Visual Representation of Monitoring Information** in Section 2.2.2.5:

- **Visual Representation with Common Widgets:** Shneiderman [Shneiderman 2005] defined the type of Information Visualization to depend on both the underlying data type and the demands of the users. And a set of visual widget, such as line chart, pie chart, bar chart, graph chart and others is designed to present different type of information. By consuming real-time network traffic logs, a series of successful approaches and systems [Camden et al. 2004] [Keim et al. 2006] [Kikuchi et al. 2007] has been proven useful to aggregate, analysis and represent the network information for diverse monitoring purpose. They are widely accepted by network well-trained administrators. However, these tools lacks the representation for higher-level meaningful information, e.g. the correlation of different monitoring flow, the highlight of current/potential problem, the relationship of different monitoring views (underlying infrastructure, quality of service, or experience of user), which brings the understanding and monitoring barrier for human user/administrators.

- **Visual Representation for Semantic Monitoring Information:** As studied in Section 2.2.3.3, semantic techniques are widely used to model the network information [Vergara et al. 2009] [Guerrero et al. 2006] [Strassner et al. 2006]. One typical kind of solutions is to adopt and apply existing information visualization technologies to show the pre-processed and well-structured semantically meaningful information. Thinkbase [Hirsch et al. 2008] and "GViz" [Frasincar et al. 2003] visualises Linked-Data from Wikipedia and the relationship of RDF generated by RDF/OWL editor with graph chart to expose the inherent relationship and context of semantic information. However, quite few systems adapt semantic visualization for the real-time network information, which requires further investigation.

From the study in this section, it is still challenged to apply theories and techniques of information visualization and semantic visualization into the network monitoring process to improve the experience for network users/administrators. In next section, the challenges

addressed from traditional network monitoring approaches/tools will be further discussed for non-expert users.

### 2.2.5 Key Findings

In this section, a couple of reviews and surveys are performed to categorise, compare, and analyse the *Network Monitoring Tools for Non-expert Users*. This section first reviews traditional network monitoring tools by their scope of application with a conclusion of network monitoring paradigm at the end. This paradigm shows the information representation is crucial for the network monitoring. It then presents empirical studies about the information representation and visualization in network monitoring tools. Followed by an analysis of existing tools, the monitoring challenges for non-expert users are concluded to clarify findings of how to support the network monitoring for non-expert users, which inspires the study of *Information Representation and Uplift Approaches.*

## 2.3 *Information Representation and Uplift Approaches*

### 2.3.1 Introduction

According to previous section, the challenges for network monitoring are two-fold: extracting the information from vast amounts of data, and presenting the information for high-level monitoring objectives according to the domain knowledge. In order to achieve these monitoring challenges for non-expert users, extracting the high-level meanings from low-level information gathered from vast amounts of data is a reasonable solution. In other word, these challenges could be aggregated as how to find out a common representation for information from both domain knowledge and network elements with an approach to perform this representation process in order to achieve high-level monitoring for non-expert users. Thus, this section reviews the typical ways to extract information from stream data and investigates an appropriate approach and its challenges for representing this information and enabling the network monitoring for non-expert users.

### 2.3.2 Information Uplifting from the Data

There is a large body of work on information extraction in networking area. Numerous network support techniques [Madden et al. 2002a] [FaraDian et al. 2002] have been proposed to capture the characteristics of network stream data from different aspects and extract the information from them at the same time.

**Data Aggregation:** Recently, one of the most promising research directions has been in-network aggregation techniques. For many network applications and infrastructure, such as node in a large scale network, it is unnecessary for each node to report its entire data stream in full fidelity. Moreover, it is unrealistic to expect exact query results due to the inherent unreliability of readings by the sensor node and also due to the loss of connection links.

Indeed, several in-network aggregation approaches to managing data collected on sensor network shave been advocated, with particular attention paid to efficient query processing for aggregate queries. A straight method for in-network aggregation is to compute such aggregates as AVERAGE, SUM, and COUNT over a routing tree, minimizing both the number of messages as well as the size of the messages. The cougar [Yao et al. 2002], TinyDB, and TAG [Madden et al. 2002b] architectures propose the use of this method.

**Statistical Summarization:** Several studies have focused on providing statistical summarization. Deshpande [Deshpande et al. 2004] proposed a statistical model to enrich interactive sensor querying in sensor networks. They designed a novel architecture for integrating a database system with a correlation-aware probabilistic model, which reduces the number of expensive sensor readings and radio transmissions that the networks must perform. There had previously been other related work conducted on approximate, probabilistic querying in sensor networks, and in particular, Yao et al. [Yao et al. 2002] used Gaussian function to model the uncertainty as a continuous probability distribution function over possible measurement values.

**Time Series Analysis:** Statistical time series analysis is a well-studied and mature field [Change et al. 2005], and many commercial statistical tools capable of time series analysis are available, including SAS, SPlus, Matlab, and BMDP. A common assumption of these studies and tools, however, is that users are responsible to choose the time series to be analyzed, including the scope of the object of the time series and the level of granularity. These studies and tools (including longitudinal studies [Chu et al. 2006]) do not provide the capabilities of relating the time series to the associated multi-dimensional multi-level characteristics, and they do not provide adequate support for online analytical processing and mining of the time series. In contrast, the framework established in this paper provides efficient support to help users form, select, analyze, and mine time series in a multi-dimensional and multi-level manner. Statistical time series analysis can be used to support aberrant behaviour detection by supposing

a statistical model exists that describes the behavior of a time series (or at least the characteristics of interest). With such a model, one can define aberrant behavior as behavior that does conform to the model (or is not well described by the model). Of course, aberrant behavior with respect to a statistical model may or may not reflect a real event of interest for the technician. In the case that it does not, it is a false positive. Obviously, the ideal is to minimize the rate of false positives while identifying all events of real interest. However, this ideal can rarely be achieved. In most detection systems, there is a trade-off between selectivity (avoiding false positives; also referred to as specificity and precision) and sensitivity (ability to detect true positives; also referred to as recall). While it is important to remain cognizant of these issues, they become less important if one perceives a statistical model for aberrant behavior as a screening mechanism rather than a surrogate for the expert judgment of a network technician. To detect competing traffic flows, HomeMaestro [Athanasopoulos et al. 2008] first attempts to detect flows that are likely to either experience or cause performance problems. Candidate flows are identified by detecting Change Points (CPs), that reflect significant performance change according to some metric. They define three CP types: DOWN, UP, and NEW, to signal the direction in performance change or the arrival of a new significant flow. CPs are identified using time-series analysis applied to various monitored connection metrics.

This section briefly reviews the common data analysis approaches available for real time stream network log data. These analysis approaches are adaptable for diverse network purpose to extract meaningful information from awkward data stream, but the information is extracted with different characteristics and formats, which requires a more general information representation. As discussed in previous sections, semantic web techniques can provide this representation for information extracted from heterogeneous network components.

### 2.3.3 Semantic Information Representation

As a formal structured representation of information, semantic web techniques are capable of extracting the rich semantics from growing amount of information available in unstructured form [Berners-Lee et al. 2001]. With the advance of semantic web research, several significant concepts have been developed to encode information and knowledge in a machine-understandable way.

RDF (Resource Description Framework) [RDF 2004] is a W3C (World Wide Web Consortium) recommended metadata model for conceptual description or modeling of the

information on the web by using a variety of syntax format. The W3C published a specification of RDF's data model and XML syntax as a recommendation in 1999, with a new version published as a set of related specifications in 2004 and it is still under further improvement. RDF provides open information models about Web resources for the machine processing with following features:

- having a simple data model
- having formal semantics and provable inference
- using an extensible URI-based vocabulary
- using an XML-based syntax
- supporting use of XML schema datatypes
- allowing anyone to make statements about any resource

The underlying structure of any expression in RDF is a collection of triples, each consisting of a subject, a predicate and an object: the subject (what the data is about), the predicate (an attribute of the subject) and the object (the actual value for the attribute). With this triple structure, a relationship between two things may be represented as an RDF triple in which the predicate names the relationship, and the subject and object denote the two things. As such, comparing to XML, RDF is designed to represent knowledge, not data, and thus is much more concerned with meaning and interrelations of concepts and their attributes, thus facilitating a degree of machine interpretability and understanding. An RDF-based data model is more naturally suited to a labelled, directed multi-graph of knowledge representation than the relational model. A set of tools has been developed for RDF generation, implementation, reasoning and storage. AlchemyAPI [AlchemyAPI 2011] uses statistical natural language processing technology and machine learning algorithms to analyse the content of data, extracting semantic meta-data. AllegroGraph [AllegroGraph 2008] is a system to load, store and query RDF data with a SPARQL interface and also support RDFS reasoning. It also has Java, Prolog, and Python interfaces.

SPARQL (SPARQL Protocol and RDF Query Language) [SPARQL 2008] is a protocol and query language for RDF that became an official W3C Recommendation in 2008. SPARQL can

be used to express queries consisting of triple patterns, conjunctions, disjunctions, and optional patterns across diverse data sources, whether the data is stored natively as RDF or viewed as RDF via middleware. Results from SPARQL queries can be expressed as result sets or RDF graphs. SPARQL is supported by most popular RDF/OWL tools. Jena [Jena 2006] is a Java framework to construct Semantic Web Applications. It provides a programmatic environment for RDF, RDFS and OWL, SPARQL, and includes a rule-based inference engine.

OWL (Web Ontology Language) [OWL 2004] is a family of knowledge representation languages for authoring ontologies, which focuses on formalizing and providing the meaning of information for processing and reasoning with using formal semantics and RDF/XML-based serializations for the Semantic Web. The languages are characterized by OWL are endorsed and recommended by W3C in 2004. OWL facilitates greater machine interpretability of Web content than that supported by XML and RDF by providing additional vocabulary for classes and properties of resources along with a formal semantics supporting automatized machine reasoning and inference processes. By differentiating the levels of expressiveness, the W3C-endorsed OWL specification includes the definition of three variants of OWL: OWL Lite, OWL DL, and OWL Full with a corresponding increase in language expressivity, but with reducing decidability in reasoning. OWL also has a good applicability with other semantic techniques: SPARQL [SPARQL 2008] can be used to access data stored in any of the OWL formats; Protégé [Protégé 2004] is a suitable platform for the OWL design; and Jena enables the Java application could consume OWL ontologies. In ontology engineering, OWL is used to model human knowledge into ontologies, which include a set of ontology classes and corresponding properties and constraints to describe relations between ontologies. In the network management scenario, Lo et al [Lo et al. 2009] indicated ontologies could effectively model domain knowledge and drive the network management with ontology-based logical reasoning process.

### 2.3.4 Information Uplifting for Representing Higher Level Meanings

The briefly overview of several common information extraction approaches in 2.3.2 shows how and when to adapt which information extraction approach depends on the monitoring requirement and the network composition. That indicates several information extraction approaches can be performed at the same time in a complex monitoring scenario. A common representation for information extracted by different approaches is desired and this information aggregation also requires the domain knowledge to determine the aggregation way to fulfil the high-level monitoring objectives.

As revealed in a large body of work [Madden et al. 2002] [Demers et al. 2003] [Barford et al. 2002], Information Extraction is widely applied to extract the meaningful information from real-time network log data and then aggregate and analyse them for different network monitoring purposes. Meaningful information is defined as the efficient information gathering from the captured characteristics of log data set for purposes such as monitoring, fault diagnosis, and performance evaluation [Liotta et al. 2002]. A number of stream data analysis techniques, eg. stream data mining [Chu et al. 2004], data trend analysis [Brutlag, 2000], stream data aggregation [Rajagopalan et al. 2006], change point detection [Karagiannis et al. 2008], etc., specialize to capture one or several particular types of characteristics from network log data stream. Moreover, the highly heterogeneous nature of current network works always requires a combination of several analysis approaches which desire a structured format to maintain the extracted meaningful information. In addition, simultaneously monitoring all time-series of interest meaningful information is an impossible task even for the accomplished network technician. This requests a further aggregation process for the overload meaningful information from low-level to high-level according to specific monitoring purpose. This process is named as information uplift. Due to its standard format and reasoning capability, the Semantic Web technology promises a well-defined structure to maintain and uplift meaningful information so that both monitoring agent and human users can understand the meaning of information and know "how to deal" with it. This semantically structured information also supports formal semantic reasoning which benefits the knowledge-driven problem analysis in the network monitoring scenario. As well-developed semantic techniques, Semantic Annotation, Semantic Modelling, and Semantic Reasoning are effective information uplift approaches for information extraction, collaboration and translation from heterogeneous data and information structures into Semantic Web metadata with formal semantic meanings [Handschuh et al. 2007]. The semantic information uplift could be executed as either a manual or an automatic process [Uren et al. 2006]. With using authoring tools such as Semantic Word [Tallis 2003], manual annotation is more easily accomplished within an integrated environment for simultaneously authoring and annotating text. However, the annotation tools often require the human annotator to be familiar with the domain and complex annotation schemas whilst this annotation process is also expensive by involving human annotators. To overcome the bottleneck of manual annotation, automated annotation provides the scalability needed to annotate existing data and reduces the burden of annotating new data with the human intervention at some point in the annotation process [Maedche et al. 2001]. Semantic annotation

platforms (SAPs) focus on the information extraction, ontology and knowledge management, access APIs, storage, and user-interfaces for ontology and knowledgebase editors [Popov et al. 2003]. SAPs could be classified based on the type of annotation method: pattern-based and machine-learning-based. For the pattern-based SAPs, the most common techniques are manually created rules, where the rule-based MUSE system [Maynard 2003] has shown that rule-based systems can equal the performance of machine-learning-based system [Handschuh et al. 2002] by using conditional processing. All kinds of SAPs require some type of resources: in rule-based systems, rules currently are manual created according to domain knowledge; machine-learning-based systems also need a training corpus. Ontologies are also needed for SAPs to tag data and up-lift them to ontology classes, individuals or properties. It is still a challenge to effectively leverage domain knowledge to derive and perform the annotation process for high-level goals in a dynamic process.

In order to perform the intelligent and automatic monitoring for heterogeneous network scenarios, the context for network components and services [Huebscher et al. 2008] [Toutain et al. 2011] is foundational to determine how to adapt the automatic semantic information uplift approach which requires modelling of network components based on the reasoning results from domain knowledge models rather than manually created rules. Furthermore, the concerns and goals of the end-user is rarely incorporated into this uplift process and current approaches only partially solve the problems that end users have in finding pertinent information hidden within dynamic large data sets. The ability to elicit, represent and analyze the tacit knowledge of domain expertise is crucial to show the promise of uplifting the meaningful information [Jennings et al. 2007]. Some authoring tools [Hampson et al. 2011] are developed for network experts who lack semantic coding skills to express their insights in an expressive and compatibility way. However, further research is still required to semantically encode domain expert's insights and leverage these encodings with modelled domain expert knowledge to enable the knowledge-driven information uplift.

This section reviews semantic techniques as a common representation for information and the stated the challenge to uplift information by using automatic semantic annotation to support high-level monitoring goals. Several methods are briefly introduced about capturing domain knowledge and explained why SABer [Hampson et al. 2011] is a suitable tool to create semantic attributes to capture domain expert knowledge. In order to model the captured knowledge in a machine-understandable way, features of popular methods and techniques are

stated with existing tools and applications, which could be used for different purposes in our research. By the analysis of current approaches to semantic annotation, this section concluded it is effective to uplift appropriate information for high-level goals. However, there is still a challenge about how to effectively leverage the domain knowledge to derive and perform the annotation process for high-level goals in a dynamic process.

### 2.3.5 Key Findings

In order to achieve these monitoring challenges stated in Section 2.2 for non-expert users, this section reviews the information extraction approaches, lists the benefits to use semantic techniques as a common representation for extracted information and the also stated the challenge to enable knowledge-driven information uplift by using automatic semantic annotation to support high-level monitoring goals. In this section, these approaches, tools, and architectures reviewed can be re-used into the approach and framework and also inspire design in this thesis. For example, extraction information approaches can be applied into experiment and SABer [Hampson et al. 2011] is possible to assist in capturing domain expert knowledge. The research challenges defined in this section can also be adapted to evaluate the approach presented in following chapters.

## 2.4 *Why Not Traditional Tools for Non-export Users?*

Network monitoring have become essential to the daily activates of the enterprise and individuals. With the fast growing network infrastructure, more and more network users are non-expert users. The large amount of data sets generated from network resources exhibits bewildering complexity for network monitoring and often beyond the cognitive capability of non-expert users. This inherent complexity of networks has made network monitoring a formidable task for even the most technically advanced people, as well as general home network users [Grinter and Edwards 2005] [Chetty et al. 2007]. Thus, a non-expert user may be defined as "typical network consumer" whom is assumed not a real "techie" [Teger et al. 2002] or network administrator who has experience in certain network domain but still not sufficient to diverse network envrionments. On one hand, it is not reasonable to expect non-expert users to acquire the necessary network knowledge; on the other hand, non-expert desires some approach could help them understand and monitor their networks [Pediaditakis et al. 2012a]. This phenomenon happens in many consumer network scenarios, such as Home Area Networks (HAN) [Pediaditakis et al. 2012b]. The innate complexity of the home network and lack of

expertise for non-expert users [Gupta et al. 2004] has forced the monitoring approach either expose or hide some network information to help users achieve their goals [Horrigan 2008].

The existing network monitoring approaches and tools discussed in Section 2.2.2 mostly are not appropriate for non-expert users. First, those approaches and tools are designed for specific monitoring purpose or composed monitoring purposes on large-scale networks such as enterprise-class networks, which consist of a number of sub networks and hosts. Consequently, the main concerns of those tools focus on effective monitoring of large-scale networks such as scalability, network configuration, network optimization, network management and complex network diagnosis. Unlike these large enterprise-wide networks, the home network is usually much smaller with different monitoring concerns and non-expert users in HAN are often troubled with a very small set of common problems and the problem correlation is hardly used even if supported by some existing systems [Wallin et al. 2009]. Second, they were originally designed for use by skilled network administrators. They require the user to have a working knowledge of low-level networking concepts such as network protocols and packets that are unfamiliar to general home users. But the user normally concerns only the high-level objectives, like the status of connection, the root-cause of current problem, or how to protect the network [Teger et al. 2002]. Therefore, to use these tools, home users would have to have the same degree of networking knowledge to establish the understanding between low-level network information and high-level monitoring/management objectives, which is unrealistic. Combined, the difference in system focus and the difference in required user training make these tools inappropriate for most non-expert home users who want to monitor their relatively small but complex home network.

Researchers have taken notice a number of users were found to run into difficulties as they try to monitor their home network [Bly et al. 2006] [Grinter and Edwards 2005] [Shehan and Edwards 2007]. According to previous research [Kiesler et al. 2000], over 70% of home users needed technical support to set up their computer and connect it to the Internet for the first time, and 90% of the households called the help desk for technical support during the 1st year of Internet usage. Furthermore, many inexperienced home users do not call the help desk, especially if they feel they do not have the necessary vocabulary or background knowledge to discuss an issue with a technical person [Yang et al. 2010] [Crabtree et al. 2012]. Along with its complexity, the invisibility of the home network makes home network management even more difficult [Grinter et al. 2005]. Such invisibility gives users an incomplete view of the home

network, which consequently makes understanding of it difficult. This reminds us of the importance of the visibility of the home network components, which contain the status of network infrastructures, services, and the high-level meanings of these components. If users are to monitor their home networks successfully, they should be given an accurate, complete conceptual model of their HAN. Researchers agree that one of the best ways to make a network more "visible" to the home user is by presenting it as a diagram [Tolmie et al. 2007]. Because of the usability problems of home network monitoring, researchers have called for network monitoring/management tools for general home network users [Chetty et al. 2007] [Edwards and Grinter 2001] [Mortier et al., 2012]. They suggested more interactive tool for home network users who have neither the sophisticated technical knowledge nor the motivation to learn complex network systems currently designed for network administrators.

It is significant that nearly 40% issues relating to IPTV (Internet Protocol Television) deliveries occurred in the HAN [Gupta et al. 2011], which are always beyond the knowledge capability of non-expert HAN users. This inherent complexity of IPTV networks has made network monitoring/management a formidable task for even the most technically advanced people to assure good delivery, particular if such monitoring can be used for Customer Experience Management (CEM) to understand network status, diagnose problems, and analyse from two different but related viewpoints, Quality of Service (QoS) and Quality of Experience (QoE) to improve the user experience and control the operation cost. To maximize return-on-investment and to be competitive, operators will need to meet customer expectations to ensure that there is demand for their IPTV service. Recent work has explored strategies for coordinating the allocation of resources for multiple virtual IPTV providers to maximize revenue [Balasubramaniam et al. 2011a] and routing strategies to manage network resources when multiple IPTV services are overlaid on the same network [Balasubramaniam et al. 2011b]; however, the fundamental problem –indeed an integral part of satisfying customer expectation– lies in evaluating the quality of the IPTV service being provided and then giving guidance on how delivery can be improved. The complex natural of the IPTV delivery network requires cross-domain knowledge about heterogeneous network services and devices from both QoS and QoE aspects. This requirement is usually beyond the knowledge of normal network administrators.

Addressed by the study above, common network monitoring challenges in previous sections are analysed for non-expert users in the following table:

Table 2-1 Key Findings and Challenges for Non-expert Users

| **Key Findings for Non-expert Users** | **Challenges for Non-expert Users** |
|---|---|
| Visibility for Disparate Monitoring Resources | Complete Conceptual Model **(C1)** |
| | Difficulties for Creating and Updating Information Representations **(C2)** |
| High-level Monitoring Purposes | High-level Monitoring Information Representation **(C3)** |
| | Cross-domain Monitoring Information Representation **(C4)** |
| Requirement of Expert Knowledge | Degree of Autonomy **(C5)** |
| | Drill-down Analysis **(C6)** |
| Visual Representation of Monitoring Information | Visual Representation to Improve Usability **(C7)** |
| | Visual Representation of High-level Monitoring Information **(C8)** |

From this table, consumer network for non-expert users (e.g. HAN) inherits most of the key findings and challenges in traditional network for network monitoring. However, from the above study of network monitoring for non-expert users, the focus and challenges are partly differed, which will be analysed in following discussions:

1) **Visibility for Disparate Monitoring Resources:** There is no signification difference between consumer network (e.g. HAN, IPTV network) and other network systems in the disparity. Large volumes of log data are generated from heterogeneous network components in a real time. However, non-expert users require more visibility for these disparate monitoring resources.

   - **Complete Conceptual Model (C1):** Although current information models [CIM

2004] [SID 2005] [Strassner 2002] provides unified and consistent representations for monitoring resources, the disparity nature of network require a more flexible and extensible approach to model the resources in specific domain, such as service quality, traffic flow, security threaten, and the higher level abstraction objects like the network behaviour, user demand, and network anomaly, which are more visible for non-expert users. There are some investigations in some novel approaches such as [Barrett et al. 2007] [Viswanathan et al. 2011], which expose the effectiveness of semantic models to describe diverse monitoring resources in different domains and abstraction levels.

- **Difficulties for Creating and Updating Information Representations (C2):** The information models [CIM 2004] [SID 2005] [Strassner 2002] (including semantic models [Barrett et al. 2007]) are widely adapted for monitoring resources modelling, but they need frequently creating and updating information model, which is acceptable in commercial network. But in small network, the complexity of information representation is similar to commercial networks, but it is hard to access network expertise from different domains like network infrastructure, services quality, and measurement of experience, which are important for normal home users, so the challenge still presents difficulties for creating and updating information representations.

2) **High-level Monitoring Purposes:** Due to the high complexity, the meaningful information contained in log data sets is highly sophisticated and hard-to-reach for non-expert users. The main concerns of those traditional tools focus on effective monitoring of large-scale networks such as scalability, network configuration, network management and complex network diagnosis. Unlike these large enterprise-wide networks, the home network is usually much smaller but with diverse monitoring concerns. Most traditional tools aim to provide necessary technical details, but non-experts require the monitoring directly expressing their high-level concerns. These concerns are targeted to improve the user satisfaction and also reduce the support cost for both network provider and the user themselves [Shehan and Edwards 2007].

   - **Challenges for High-level Monitoring Information Representation (C3):** Current model-driven architectures [Sloman, 1994] [Kosiour, 1999] [Agrawal, etal.

2005] are built on the low-level information of the underlying data, like packet loss, throughtput, and signal strength in the data model, which lacks higher-level understanding of the characteristics and meanings of the data. The The low-level information is invisible for non-experts [Grinter et al. 2005]. As discussed by [Chetty et al. 2007], non-expert is not statisfied with just monitor the status of the network connection. They need more comprehensive way to understand what the problem is, where the problem occurs, and how to solve this problem. Some commercial systems [Zhang et al. 2005] [Breitgand et al. 2005] adapts policies/rules to present high-level business monitoring goals with the status of network components, which is suitable for large-scale commercial network systems, where have enough well-trained administrators to understand the underlying infrunstrures. But it is obviously still too "complicant" for non-expert users.

- **Challenges for Cross-domain Monitoring Information Representation (C4):** There is a large range of policy/rule languages to provide expressivity to derive complex monitoring purposes [Strassner 2002]. However, the higher level monitoring purposes like troubleshooting may invoke the monitoring information from underlying resources in different monitoring domain, such as Service Level Agreement (SLA) monitoring with Quality of Service (QoS) and also the perceived Quality of Experience (QoE) for the user [Sheridan-Smith et al. 2003]. In addition, the quality of service directly refers to the satisfaction of home users [Gupta et al. 2011]. Thus, the cross domain information representation presents a challenge for non-expert users.

3) **Requirement of Expert Knowledge:** Expert knowledge from different network sub-domains is still required for diagnosis, analysis, and overcoming common problems in home networks and it is especially important to improve the network visibility for non-expert users [Gupta et al. 2004].

- **Degree of Autonomy Ensured by Expert Knowledge (C5):** A series of existing systems promised the information from expert knowledge can ensure certain degree of autonomy, which is especially important for non-expert users. The study in autonomic network monitoring [Kephart 2005] demonstrates the representation of

expert knowledge is the key point to promise the autonomy of network monitoring. This requires an explicit, formal, and shareable representation for domain knowledge. Semantic techniques are widely applied in a range of autonomic systems [Vergara et al. 2009] [Guerrero et al. 2006] [Strassner et al. 2006] to represent the expert knowledge. However, this success is associated with a challenge of how the domain knowledge could be applied to encode a good set of knowledge representation to enable the intelligence of an automatic monitoring system with high-level goals. For non-expert users, troubleshooting is a trivial but typical issue to affect the user satisfaction and support cost. The normal process of troubleshooting is in three steps: identify problem, analyse problem, and solve problem [Wilson 2000]. In addition, most troubleshooting approaches are performed statically, but the autonomy of a real-time network monitoring require dynamic modelling and reasoning capabilities, which is another challenge for current troubleshooting approaches.

- **Drill-down Analysis Ensured by Expert Knowledge (C6):** According to the model-driven architectures [Sloman, 1994] [Kosiour, 1999], the network information should be able to present for the high-level monitoring purpose, which also supports the drill-down analysis back to the low-level monitoring information. The system from Hewlett-Packard Labs [Zhang et al. 2005] and IBM research [Breitgand et al. 2005] to automatically correlate low-level system measurements up and drill down high-level objectives. For example, the high-level business goals can be enforced and monitoring based on low-level information from network resources, whilst the troubleshooting is also supported to track the failure back to the underlying resources. Up to this paint, a main problem is to populate the knowledge representation for both low-level and high-level information and to develop methods for adopting it effectively.

4) **Visual Representation of Monitoring Information:** A comprehensive visual representation of meaningful information is required to improve the visibility and usability for non-expert users.

- **Visual Representation to Improve Usability (C7):** Shneiderman [Shneiderman 2005] defined the type of Information Visualization to depend on both the underlying data

type and the demands of the users. A set of visual widget, such as line chart, pie chart, bar chart, graph chart and others is designed to present different type of information. By consuming real-time network traffic logs, a series of successful approaches and systems [Camden et al. 2004] [Keim et al. 2006] [Kikuchi et al. 2007] has been proven useful to aggregate, analysis and represent the network information for diverse monitoring purpose. As most of existing tools are designed for professional network administrators, which have usability issues for non-expert users in HAN. Even for professional administrators, current tools is hard to reveal the comprehensive representation of information from different domain in the highly complexity network. The challenge is how to improve the user experience by using the existing visual widgets.

- **Visual Representation for High-level Monitoring Information (C8):** As discussed, the user normally concerns only the high-level objectives, like the status of connection, the root-cause of current problem, or how to protect the network [Teger et al. 2002]. Semantic techniques are widely used to model the network information [Vergara et al. 2009] [Guerrero et al. 2006] [Strassner et al. 2006]. Some investigations in those novel approaches such as [Barrett et al. 2007] [Viswanathan et al. 2011], expose the effectiveness of semantic models to describe high-level information with different abstraction levels. For non-expert users, this visual representation for these semantic information aims to improve the visibility of meaningful information [Tolmie et al. 2007].

Based on the previous study on current network monitoring tools and approaches, this section analyses key findings and network monitoring challenges of traditional network monitoring systems for non-expert users. And then a functional comparison of five high-impact tools further investigates current attempts to partly fulfil these challenges. The comparison also influences the design and evaluation in following chapters.

## 2.5 *Analysis of Existing Systems for Non-expert Users*

Focusing on the key findings and challenges for non-expert users summarised above, some existing tools have already been developed to propose novel approaches to partly fulfil these challenges. In this section, a review and analysis of existing monitoring systems for non-expert users to further investigate the adapted approaches to fulfil the challenges and inspire the design in the following chapter.

#### *2.5.1.1 System Selection*

The systems are typically chosen according to following two rules: have a high reputation in industry or research and adapt effective approaches or high impact innovation to improve satisfaction and reduce support cost for non-expert users. Five innovative candidate systems have been chosen:

- **Network Magic** [Network Magic 2005] is a widely applied commercial home networking solution introduced by Cisco to address the usability problem of home network monitoring/management. Network Magic is one of earliest commercial solutions cited by a number study in the area of home network monitoring and closely related to the research in this thesis. Although it is no longer supported due to some unknown reasons, its intended purpose still has value to this study and empowers users by freeing them from the hassles of technology.

- **ISI framework** is a semantic framework [Viswanathan et al. 2011] [Hussain et al. 2011] developed in Information Sciences Institute (ISI) to enable semantic analysis at a level closer to the user's understanding of the system or process. This framework with its visual interface adapts a novel research approach to introduce a logic-based formulation of high-level behaviour abstractions as semantic representation on a sequence or a group of related facts. This work is published in a leading innovation conference (NSDI) to firstly uplift the meaning of data from low-level to high-level, which is close to the research in this thesis.

- **Eden** [Yang et al. 2010] is an interactive and direct manipulation home network monitoring/management system aimed at home end users. Eden supports a range of common tasks, and provides a simple conceptual model that can help users understand key aspects of networking better. The system leverages a novel home network router that acts as a "drop-in" replacement for users' current router and it demonstrates that Eden not only improves the user experience of networking, but also aids users in forming workable conceptual models of how the network works. As the author announced, Eden is the first system focusing on the research of improving usability for non-expert home network users. This research has enough novelty and close relates to this research.

- **Homework Project** [Homework, 2011] [Sventek et al. 2011] is a world leading collaborated research project aiming to provide the next generation of domestic infrastructure that combines empirical understanding of use with a fundamental re-invention of the protocols, models and architectures of the domestic setting. The Homework contains information plane architecture by using stream database concepts to generate derived events from streams of raw events. This supports a variety of visualization and monitoring techniques, and also enables construction of a closed-loop, policy-based management system. This research adapts the latest evolving of the information plane architecture and its associated policy-based management infrastructure. Exemplar visualization and closed-loop management applications enabled by the resulting system (tuned to the skills of non-expert home users) are also discussed in this research. This research demonstrates how "traditional" policy-based information representation with user-friendly visual interface supports non-expert users in monitoring and managing their home networks.

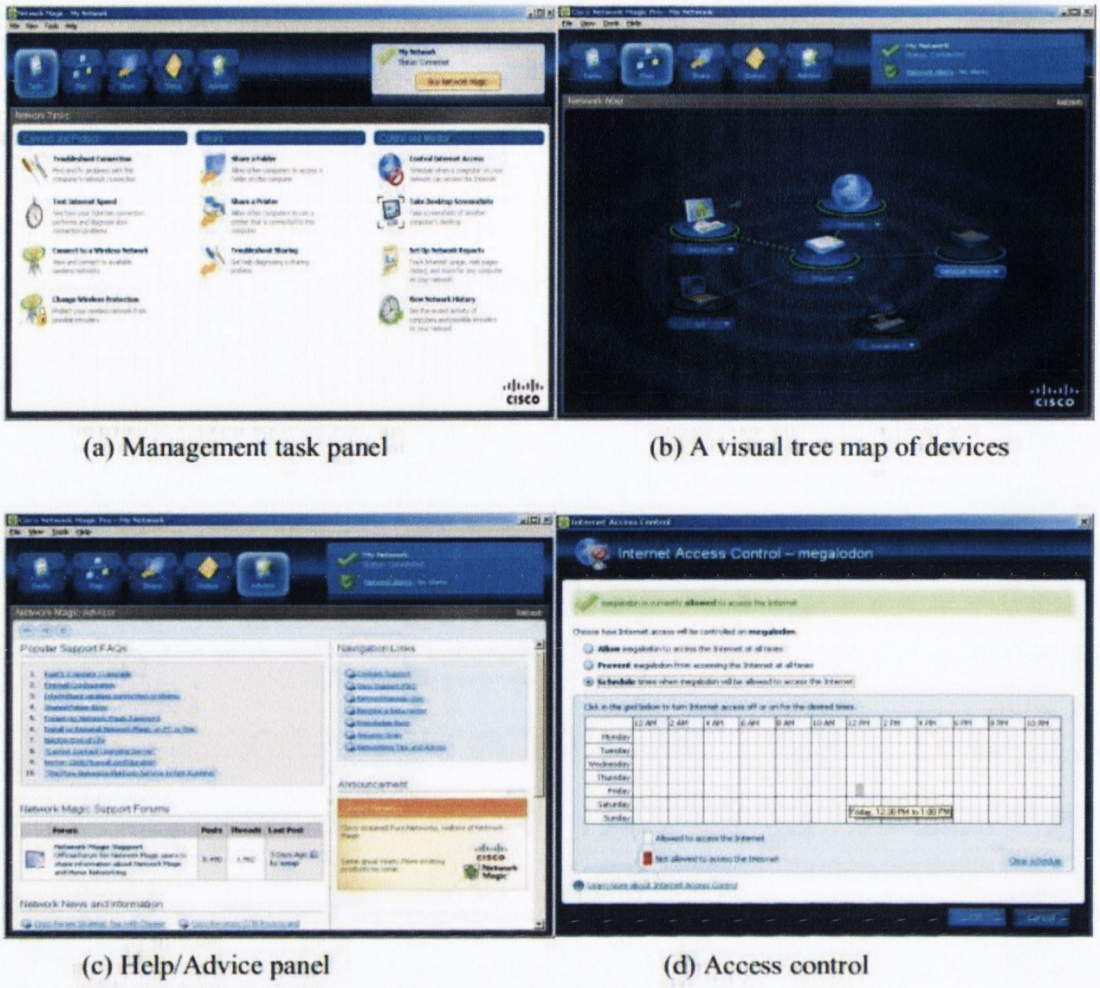
- **Netcool** [Netcool, 2006] is a mature and powerful monitoring/management tool suite for large-scale commercial networks. It offers product families that support domain-specific IT management, end-to-end consolidated operations and business service management by enabling to identify and resolve the most critical problems with automated event correlation, isolation and resolution capabilities. Although Netcool is a cut-edge solution for large-scale commercial networks, it is still aiming to simplify the monitoring/management process for network administrators, which could be a good comparison to expose the monitoring challenges in different network environment.

In following sections, these five systems will be introduced and analysed to indicate their advantages and disadvantages, and then a comparison is addressed on them according to the challenges to highlight the research challenges and inspire the available solutions to influence the design chapter.

#### *2.5.1.2 Network Magic*

Recently, Cisco introduced a home networking solution, Network Magic (Figure 1), to address the usability problem of home network management. Its intended purpose is to

empower users by freeing them from the hassles of technology. Network Magic provides a comprehensive set of household-oriented tasks including device configuration, wireless security, network speed, network status monitoring, folder sharing, troubleshooting, and network advising with a much more user-friendly user interface. It also provides a much more user-friendly view, (a visual tree map of devices on the home network) compared to the existing management tools described above. The user interaction model of Network Magic is, however, not much different from those of existing management tools. Although it provides a visual representation for some part of the home network components, it does not fully support the interaction features of direct manipulation. Network Magic provides visual representations for only a subset of home network components – at most, a router and individual computing devices. What users can do with those devices is change a device name or an icon type and see the configuration and status information of the device, including its name, connectivity status, IP address, subnet mask, MAC address, operation system, and connection speed. However, for these devices, management tasks including configuration, security, and status monitoring must be done on separate task panels through menu- and dialog-based user interactions. In other words, objects and actions are not closely coupled with each other. Furthermore, it still requires users to have some technical knowledge of networking to use it. For instance, users need to manually build and maintain a secure wireless home network just as they need to do with traditional network management tools. They first need to make a wireless home network secure by using the wireless security technology and then add a device to the secure wireless home network through the wireless security technology.




(a) Management task panel (b) A visual tree map of devices

(c) Help/Advice panel (d) Access control

Figure 2-1 Cisco's Network Magic

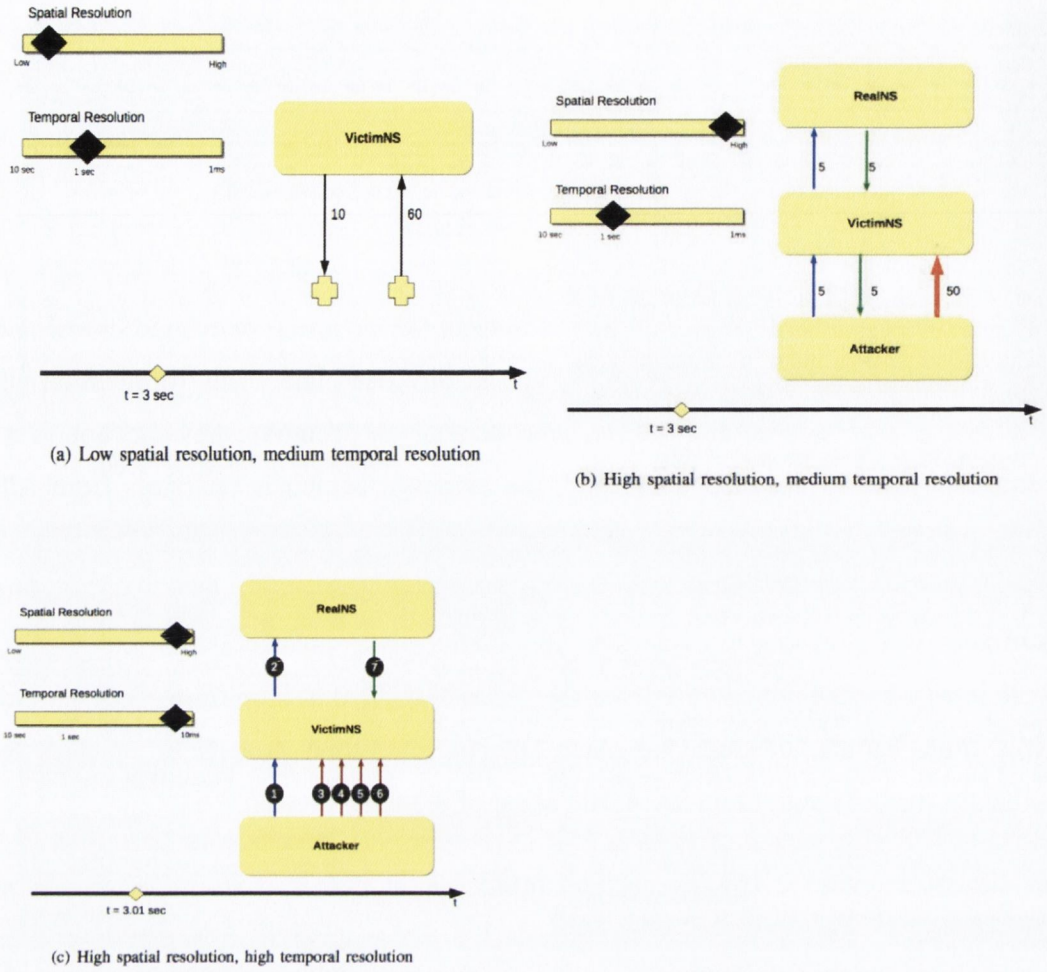
### *2.5.1.3 ISI Framework*

Effective analysis of raw data from networked systems requires bridging the semantic gap between the data and the user's high-level understanding of the system. The raw data represents facts about the system state and analysis involves identifying a set of semantically relevant behaviours, which represent "interesting" relationships between these facts. Current analysis tools restrict analysis to the low-level of individual facts and provide limited constructs to aid users in bridging the semantic gap. The objective of ISI framework is to enable semantic analysis at a level closer to the user's understanding of the system or process. The key to this approach is the introduction of a logic-based formulation of high-level behaviour abstractions as a sequence or a group of related facts. This allows treating behaviour representations as fundamental analysis primitives, elevating analysis to a higher semantic-level of abstraction.

Thus, the behaviour-based semantic analysis framework provides: (a) a formal language for modelling high-level assertions over networked systems data as behaviour models, (b) an analysis engine for extracting instances of user-specified behaviour models from raw data. This approach emphasizes reuse, composibility and extensibility of abstractions.

The framework is designed with four steps. First, the framework provides logic-based support to formulate behaviour abstractions as a sequence or group of related events, where events are uniform representation of system facts as discussed later. This formulation allows treating this behaviour representation as fundamental analysis primitive, elevating analyses to a higher semantic-level of abstraction. Second, the language combines operators from Allen's interval-temporal logic [Allen 1983], Lamport's Temporal Logic of Actions [Lamport 1994] and Boolean logic. Third, the framework enables specifying dependency relationships between event attributes while leaving the values to be dynamically populated at runtime. Lastly, the framework introduces the notion of a domain-independent event as a uniform representation of multi-type, multi-variate, timestamped data. This normalization process of data to events ensures that the analysis algorithms are independent of the input domain.

This design ensures developing abstract behaviour models as first-order primitives for capturing, storing, and reusing domain expertise for the analysis of networked systems. It demonstrates the effectiveness by applying it to diverse analyses tasks; modelling a hypothesis on traffic traces, modelling experiment behaviour, modelling a security threat, modelling dynamic change and composing higher-level models. Extending the framework that allows users to define semantics as abstract models, these models are defined to construct multiresolution visualizations of network traffic data. The methodology for visual exploration allows the user to rapidly analyse and understand network traces, by providing intuitive and interactive representations of the network (Figure).




(a) Low spatial resolution, medium temporal resolution

(b) High spatial resolution, medium temporal resolution

(c) High spatial resolution, high temporal resolution

Figure 2-2 Visual Interface of ISI Framework

#### *2.5.1.4 Eden*

Eden (Figure 3) presents a direct manipulation approach to help normal home network users to address a wide range of home network tasks. Eden is focusing on uncovering users' needs, and developing a coherent set of interface concepts that are approachable and understandable by users. Eden eliminates the need for users to deal with the technical minutia of the network with a simple drag-and-drop interface visually represented networking devices and network settings. The contributions of Eden are threefold. First, as they announced, Eden is the first fully direct manipulation system designed specifically for home network management, along with the design process that informed this system. Second, Eden presents an approach to actually implementing network policy controls in response to user interface actions, while maintaining compatibility with the diverse, deeply heterogeneous environment in the home network.

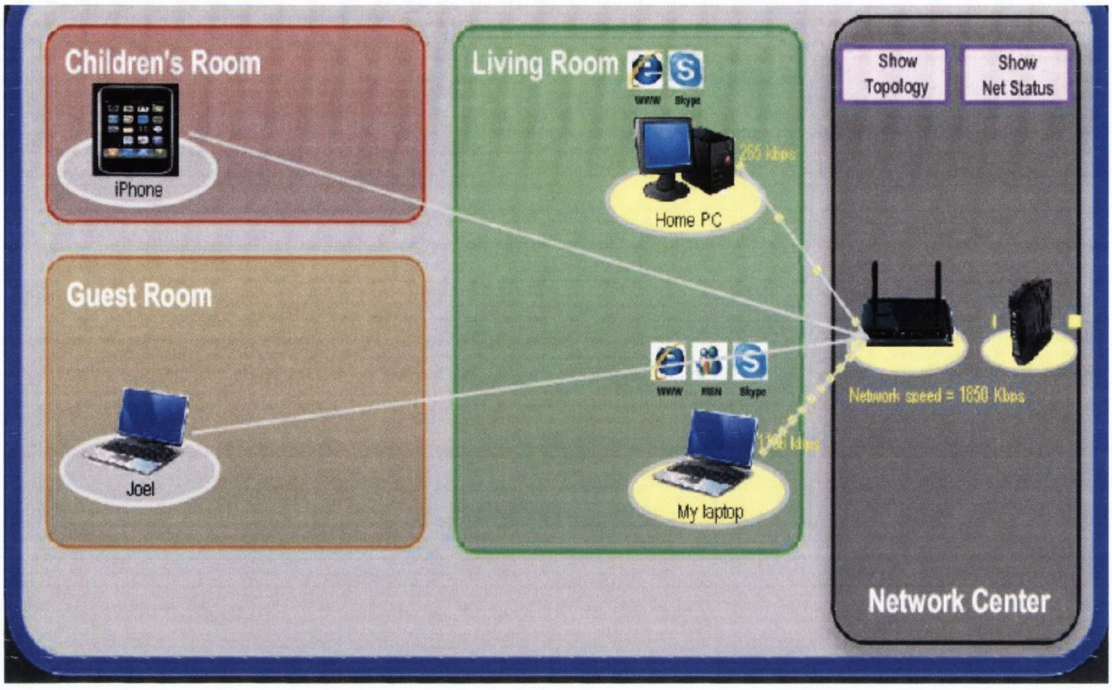



Figure 2-3 Eden prototype user interface

In its default view, Eden only shows the spatial representation of devices within Rooms. However, network topology and traffic information in a highly simplified form intended for use in common troubleshooting tasks, can be overlaid atop this representation. Enabling the topology and network status views overlays a series of visible links over the spatial representation. These links are animated flows of dots that indicate the traffic among devices in the network, and make visible the logical topology of the network. They also provide a means to get an at-a-glance view of connectivity and performance; they allow users to tell which devices are communicating, how much they are communicating, and whether or not the home is experiencing connectivity problems with the ISP. The "Show Net Status" enhances this view by showing which specific applications on each device (as determined by standard Internet Protocol port numbers) are generating or receiving traffic; these applications are depicted as icons above the originating devices.

#### *2.5.1.5 Homework Project*

The research challenge for the Homework Project is to take a radical approach to future networking in the home by considering the needs of the user. By studying the use of computer networks in the home, it is intended to create the next generation of domestic infrastructure that combines empirical understanding of use with a fundamental re-invention of the protocols,

models and architectures of the domestic setting. The challenge is to develop techniques and tools that inform users of the implications of network changes in terms that they readily understand, aiming to develop an infrastructure that can configure and repair by itself.

This project brings together a number of currently disparate research traditions to develop approaches to the domestic infrastructure that enables a much more user-centered approach to its management and use at all levels. It supports user-oriented manifestations that convey the nature of the infrastructure in terms of its internal architecture, its configuration in the home and that present key features of management, measurement and modeling that is developed in partnership with household inhabitants. These allow users to both make sense of the infrastructure and to interact with key elements of it. They exploit a range of alternative interactive technologies including personal mobile devices carried by inhabitants and shared situated screens and physical artifacts built into the environment. The user driven management approaches adopted in this system allow inhabitants to express their intent to the surrounding digital infrastructure through the expression of policies. This work explores the development of both implicit policy setting based on understanding the sensed actions of users and explicit policy setting approaches where the inhabitant directly conveys intent to the infrastructure. Based on defined policies, user motivated measurement and monitoring is deployed and provides one of the key resources to drive the project. This work focus on dynamic approaches to capturing and describing the nature of the infrastructure based on the establishment of a network measurement plane for the domestic network that captures information and statistics of use to inhabitants and external experts. User focused computational models of the infrastructure is elaborated that allow reasoning about key features of the infrastructure (e.g. the extent to which they are preserved), exploration of the consequences of users actions and the relationship to their intentions, and presentation of models of user behaviour and infrastructure to the people modelled.

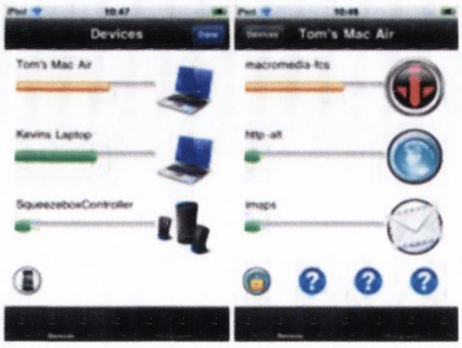



**Figure 1: Per-device bandwidth consumption.**

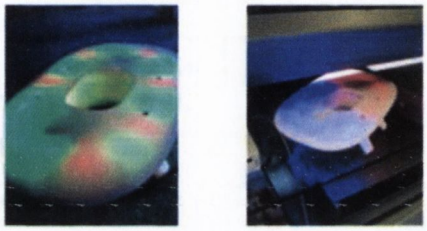


**Figure 2: Network artefact as physical interface.**

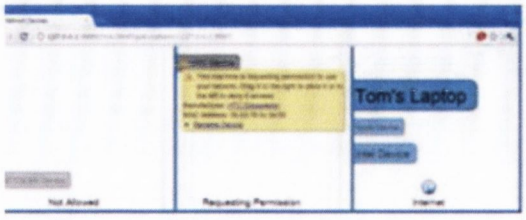



**Figure 3: Simple control interface.**

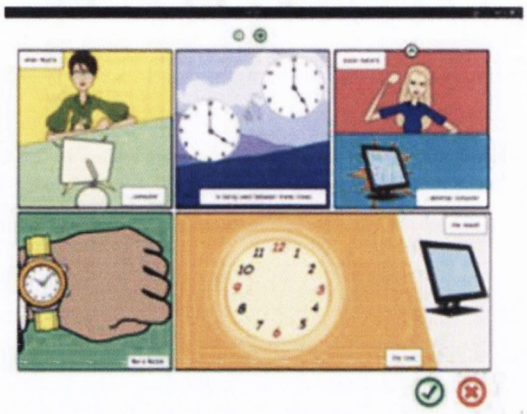


**Figure 4: Novel interactive policy interface.**

Figure 2-4 Homework project user interface

#### *2.5.1.6 Netcool*

Tivoli Netcool Performance Manager (TNPM) enables communication service providers, enterprises, and utilities to manage network performance of both fixed and mobile networks. It provides a comprehensive, flexible and scalable performance management system that supports complex, multi-vendor, multi-technology networks while providing increased visibility into total network performance. With Tivoli Netcool Performance Manager, customers can consolidate performance management of both wireless and wireline/IP-based networks to a single vendor solution for lower cost of ownership. The solution enables organizations to move toward convergence and next generation networks—while continuing to support existing mature technologies.

Tivoli Netcool Performance Manager includes an extensive library of "off-the-shelf" network interfaces called technology packs, which can be quickly deployed, extended, and modified to manage different vendors and technologies on a single system. These independent modules provide domain-specific and vendor-neutral data models, vendor-specific metrics and

key performance indicators (KPIs), and value added reports and graphs.

With operational views streamlined for managing the network using real-time data and a separate reporting module for creating ad hoc, state-of-the-art displays, Tivoli Netcool Performance Manager provides greater visibility into network performance. Both engineers and executives can utilize the large library of pre-configured calculations and KPIs in wireless or wireline, vendor-neutral or multivendor reports or create new reports and graphs using an innovative reporting engine, Through the Cognos Framework Manager, you can create a business oriented reporting data model for a technology or vendor containing reporting entities and their mappings to the underlying wireline/fixed/IP or wireless/mobile database schema (technology pack). For managing the overall network with end-to-end KPIs and the information needed to compare the performance of components from different vendors, Tivoli Netcool Performance Manager allows service providers to define cross-technology and cross-vendor KPIs, using counters provided by a specific vendor or other counters that are vendor-neutral. In addition, Tivoli Netcool Performance Manager provides a feature called composite resources for creating network and service models to report on logical entities or end-to-end network paths. For instance, composite resources can be used to measure link availability or latency across a virtual private network based on the relationship between physical resources. This ability provides a much more powerful way of looking at network and service quality than performance metrics on individual resources alone and can be used to enhance alarm dentitions, network troubleshooting, and service quality reports. Tivoli Netcool Performance Manager delivers network intelligence not only to network operations but also to other business management functions to facilitate improved decision making. While network operators review and troubleshoot detailed, low-level, network information through operational views, capacity managers can use trending and forecasting reports to plan for demand and growth. Executives can use performance data to make critical business decisions, view a national scorecard made up of key KPIs across each region, and validate their investments in the network.

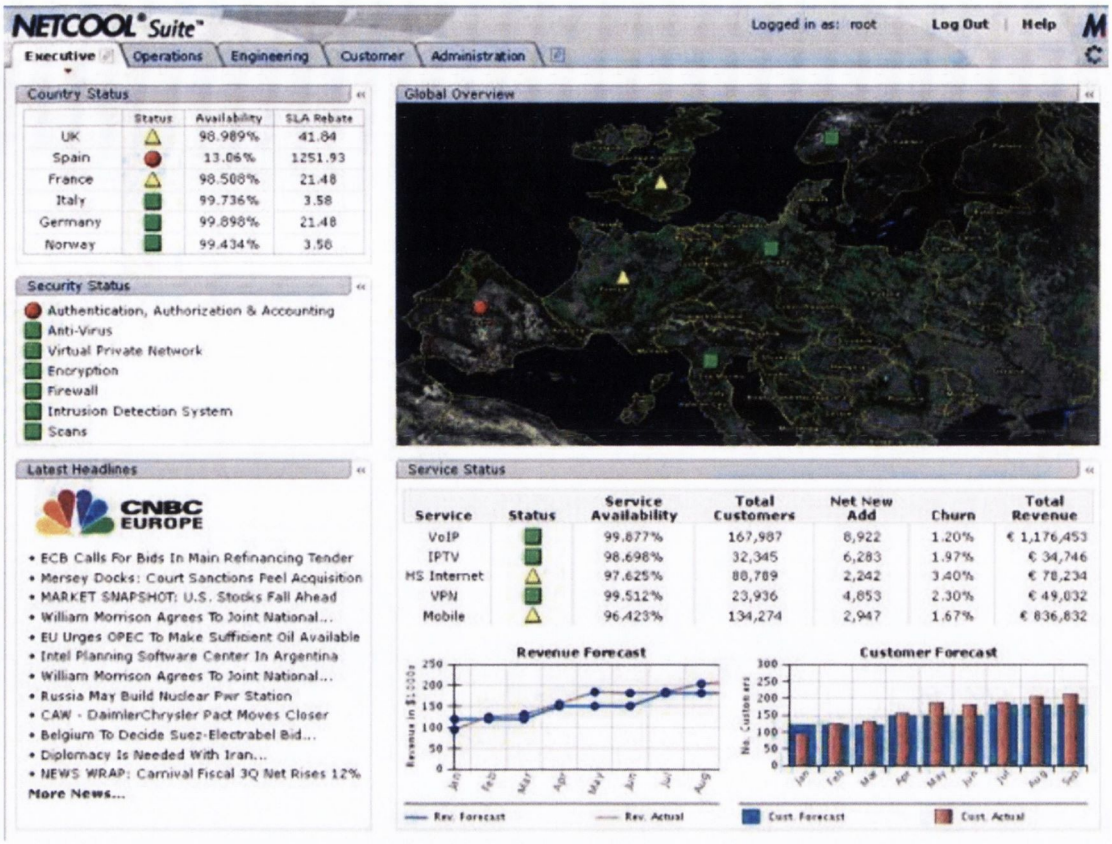



Figure 2-5 Netcool user interface

### *2.5.1.7 Analysis of Selected Network Monitoring Systems for Non-expert Users*

This analysis is performed according to a comparison of selected five innovative network monitoring systems for non-expert users to partly fulfil the challenges addressed in Section 2.2.5 for non-expert users. Then an analysis is performed after the comparison table to point out the key findings.

Table 2-2 Comparison of Existing Tools

| | **Network Magic** | **ISI Framework** | **Eden** | **Homework Project** | **Netcool** |
|---|---|---|---|---|---|
| Complete Conceptual Model (**C1**) | Limited Support with network traffics | Well Support with comprehensive data model | Well Support with Spatial + Logical models | Well Support with comprehensive data model | Well Support with traffic protocols and services |
| Difficulties for Creating and Updating Information Representations (**C2**) | No Support | Limited Support with independent semantic models | Limited Support with independent models | Limited Support with independent models | Limited Support with independent models |
| High-level Monitoring Information Representation (**C3**) | Little Support with network status | Well Support with higher level abstraction | Little Support with network status | Little Support with network status | Little Support with network status |
| Cross-domain Monitoring Information Representation (**C4**) | No Support | No Support | No Support | No Support | Limited Support with indenpended models |

| | | | | | |
|---|---|---|---|---|---|
| Degree of Autonomy (**C5**) | Little Support with embedded logic | Well Support with expert knowledge input but hard to capture | Little Support without knowledge input | Well Support with expert knowledge input but hard to capture | Well Support with expert knowledge input but hard to capture |
| Drill-down Analysis (**C6**) | Little Support with pre-defined suggestion | Little Support with human judgement | No Support | No Support | Little Support with human judgement |
| Visual Representation to Improve Usability (**C7**) | Average Support to the non-expert users | Little Support to the non-expert users | Average Support to the non-expert users | Well Support to the non-expert users | Little Support to the non-expert users |
| Visual Representation of High-level Monitoring Information (**C8**) | Little Support with only network status | Average Support with some degree of knowledge required | Little Support with only network status | Little Support with only network status | Average Support with some degree of knowledge required |

Although the tools introduced above have different academic and commercial focuses, their work showed that information modelling, information visualisation, and knowledge-driven analytic approaches can be effective when used together to assist non-expert users in coping with diverse network monitoring tasks.

From this comparison, it is obvious that the common information model is a common

solution for modelling heterogeneous network components. The information plane in Eden and Homework project and the novel semantic model in ISI framework all support a comprehensive description of heterogeneous network resources and they are also extensible to support new protocols, metrics and other network resources. From the comparison, the knowledge input is necessary to ensure the system flexibility for the network environments. Even these modelling approaches all provide a formal syntax, but network domain experts normally are not policy/semantic experts, which brings encoding difficulties for network domain experts to create and update these models. Thus, these findings are concluded:

- **Complete Conceptual Model (C1):** Information Plane and Semantic Models are effective to model the network resources.

- **Difficulties for Creating and Updating Information Representations (C2):** The knowledge input from domain expert to create and update information representation is necessary, but it is still challenges for domain expert to encode their expertise.

As discussed in Section 2.2.5, high-level information is important for non-expert to monitor network status and understand the networking problems. Most cut-edge systems still focus on presenting the network status, which is no longer sufficient to establish enough understanding for non-experts. ISI framework presents an effective semantic approach to model the higher-level meaning of network behaviour from low-level network resources models. This high-level abstraction modelling is not well-supported by current common information models [CIM 2004] [SID 2005] [Strassner 2002]. And most systems lack the support to cross-domain modelling for network resources. Only Netcool provides the models for the cross-domain network resources, like revenue, geo-location, user experience, etc., but these models still indented to each other, which is hard to be correlated to expose the inherent relationships from these network resources. Thus, these findings are concluded:

- **High-level Monitoring Information Representation (C3):** Further investigation is required to extract more comprehensive meaningful information for non-expert users, not only just network status. Semantic approach shows the possibility to model high-level abstractions.

- **Cross-domain Monitoring Information Representation (C4):** Correlated models are required to represent the information from different domians, which can provide non-

expert users better understanding of the network with correlated problems.

Expert knowledge is often required for diagnosis, analysis, and overcoming network problems. From the comparison of these systems, all tools can utilise and model some degree of domain knowledge and it is proven effective for the network troubleshooting. It is obvious that the degree of imported domain knowledge is crucial to promise the level of intelligence and autonomy of the monitoring process, which is especially important for non-expert users. The knowledge models in ISI framework, Homework, and Netcool provide a more flexible way to ensure the intelligence and autonomy. And some of them support the drill-down analysis, but it still need the user to analyse the root-cause reason by themselves, which is not appropriate for non-expert users. Thus, these findings are concluded:

- **Degree of Autonomy (C5):** The domain expert knowledge model is important to promise the intelligence and autonomy of network monitoring process.

- **Drill-down Analysis (C6):** Further investigation is still needed to enable the drill-down analysis to provide the root-cause reason for network problems without human judgments.

These systems show the existing visual dashboard can improve the understanding of non-experts users with low learning barrier. In addition, Homework provides comic style interfaces for non-experts to define their own rules, which expose the usability are crucial for non-expert users. And how to visually present the high-level monitoring information to non-expert user is still challenged. The ISI project and Netcool system made some attempts from different ways: ISI project provides a multi-resolution display to the information in different abstraction level and Netcool supports different visual views for the information in different domain. Thus, these findings are concluded:

- **Visual Representation to Improve Usability (C7):** Usability is important for non-expert users. Using existing visualisation dashboards is an acceptable way but some novel interaction approaches are also effective to improve usability.

- **Visual Representation of High-level Monitoring Information (C8):** There are two proven effective ways to present high-level information: multi-resolution display and diverse visual views.

The above discussion and analysis of the comparison of five cut-edge systems show some findings of existing monitoring challenges for non-expert users. These findings motivate the research in this thesis and also expose some findings from the technical perspective:

- **The use of Semantic Web Technologies** provides a comprehensive and formal representation for the information in the network monitoring systems. In a range of systems [Barrett et al. 2007] [Viswanathan et al. 2011] [Hussain et al. 2011], semantic web technologies are widely used to model the heterogeneous network resources, the domain expert knowledge, the higher-level abstraction and also support to visualise the semantic information.

- **Extraction of Information** is used to capture information from the models of heterogeneous network resources. The ISI framework and Netcool systems also demonstrate the information extraction can also support the extraction of high-level information.

This section chose and compared five high impact systems to clarify the findings from the challenges for non-expert users aggregated in previous section. Individual challenges were partly overcome by these systems but there is no solution to fulfil the combination of all these challenges for non-export users.. These findings highlight the challenges for non-expert and all these challenges need to be fulfilled, which will be further discussed in this thesis. They are also important to inspire the design in next chapter.

## 2.6 *Conclusion*

This chapter describes a state of art study of *Network Monitoring Tools for Non-expert Users* and *Information Representation and Uplift Approaches*. The surveys and reviews in this study examine these approaches/tools for non-expert users with advantages and disadvantages. Key findings in section 2.2.5 and section 2.3.5 are summarised into the challenges in section 2.4 which motivate and they inspire the design of the novel approach and framework discussed in following chapters. The study in this chapter also benefits the corresponding evaluations in this thesis.

# Chapter 3
# Design

## 3.1 *Introduction*

This chapter presents the design for an approach with corresponding information representations and monitoring framework that fulfil the research question and objectives stated in Chapter 1. The design is influenced by the state of the art in Chapter 2 which exposes challenges for non-expert users in understanding and monitoring network systems. There is a compelling need for an approach to bridge the understanding gap between bewildering complexity of large amount of log data from heterogeneous network components and the cognitive competencies of non-expert users. Furthermore, motivated by the fast growing network monitoring market [McGillicuddy et al. 2009], a framework is desired to leverage domain expert knowledge to support the network monitoring for non-expert users in different network systems in order to reduce the user support cost and increase the user satisfaction.

In this chapter, the influences from the state of the art are stated to inform the requirements for the design. The key findings from analysing the *Network Monitoring Tools for Non-expert Users* conclude the paradigm of common network monitoring approaches and expose the challenges to support non-expert users in understanding and monitoring network systems, which inform the requirements for the design of a knowledge-driven information uplift approach with its information representations and network monitoring framework. As general solutions applied in the network monitoring paradigm, the study of *Information Extraction Approaches for Stream Data* discusses the technical research challenges by adopting existing semantic web technologies and information extraction approaches to fulfil the challenges for network monitoring, which inform the approaches applied into the design to fulfil the requirements.

After the discussion of the influences stemming from the state of the art, the chapter concludes with some considerations of the design that relates back to the research question and objectives and discusses the novelty of the design. By analysing the requirements, an outline of the scope of design is introduced with various components to fulfil these requirements. For clarity, the design is divided into approach design, information representation design and monitoring framework design. The approach design describes the knowledge-driven information uplift approach, which underpins the corresponding information representations and monitoring framework. The design of information representations central to fit the approach then follows with four different representations for registering data sources, encoding domain knowledge, modelling network components and reasoning network problems. Finally, a monitoring framework is described in a layered structure to integrate the approach and information representations to support the monitoring in diverse network systems and visually represent uplifted information for non-expert users.

At the end of this chapter, the conclusion section presents an overview of the design, discusses the fulfilment for the requirements and analyses the novelty of the design. A technical implementation of the design is presented in the next chapter.

## 3.2 *Influences from the State of the Art*

This section discusses the influences from the state of the art to inform the design of a knowledge-driven information uplift approach with corresponding information representations and monitoring framework. These influences derived from the key findings in the state of the art led to a list of requirements that must be achieved in order to answer the research question and fulfil the research objectives. The discussion of these influences is addressed into three sections: the first section focuses on the information uplift approach, the second section is about the information representations and the last section addresses the influences on the monitoring framework.

### 3.2.1 Influences on the Knowledge-driven Information Uplift Approach

Influenced by the key findings from the state of the art, an approach is motivated to leverage domain expert knowledge to support non-expert users in understanding and monitoring network systems. By the study of *Network Monitoring Tools for Non-expert Users*, a motivation for non-expert users is clearly clarified by an analysis of challenges and key findings of current approaches/tools. This study also concludes a basic paradigm for network

monitoring systems [Comer 2007]. From this paradigm, the scope, functionality and limitation of a monitoring system are inherently linked to the available information with network elements and represented to the network users. The information obtained from network elements and inputted from domain knowledge is important to this paradigm. Thus, the representation of information is tightly coupled to all sorts of network monitoring systems. Due to the difference in origin, the representations of two types of information usually differ. Information imported from domain knowledge is always represented in logical description (e.g. policy/rule language), but the information from network elements is mostly represented in pre-defined metrics usually restricted to the manufacturer or underlying protocol. By the study in Section 2.2.3, most current representations still lack appropriate consistency for the information from heterogeneous underlying network resources and it is a challenge to harmonize inputted information from diverse network knowledge domains, like quality of service, performance of network resource, and quality of experience, for high-level monitoring goals. Furthermore, current information representations are also hard to encode and update for domain experts.

These challenges are becoming acute for non-expert users. Current network systems have increasing complexity and become essential to the daily activates of the individuals. The large amount of data sets generated from heterogeneous network resources exhibit bewildering complexity for network monitoring information and is often beyond the cognitive capability of non-expert users. The existing network monitoring approaches and tools discussed in Section 2.4 mostly are not appropriate for the non-expert users. The difference in system focus and the difference in required user training make these approaches and tools inappropriate for most non-expert users who want to monitor their networks.

By comparing five selected systems, the adapted approaches to fulfil the challenges are investigated to represent meaningful network monitoring information for non-expert users. The meaningful network monitoring information is extracted from the information generated by heterogeneous network resources. Current extraction approaches generate information presenting different characteristics of stream network log data in different monitoring activities, which requires a more general information representation. Semantic representation reviewed in Section 2.3.3 is widely adapted as a common representation for the information representation in networking systems. However, there is still an understanding gap between high-level monitoring objectives and low-level information from underlying resources for non-expert users. The understanding gap can be fulfilled by leveraging domain expert knowledge to extract

meaningful information in real time to enhance the understanding of networking for non-experts.

These findings from the state of the art have motivated and influenced the design by deriving a requirement:

**Requirement R1**: An approach must be designed to uplift meaningful information from real time data by leveraging the domain expert knowledge.

This requirement for the design contributes to the research question in Chapter 1 by addressing the research objective:

**Objective 3**: design and implement an approach to uplift meaningful information from real time log data by leveraging the domain expert knowledge.

The influences on the design of knowledge-driven information uplift approach inform the design of representation for the information endowed into the uplift approach and the design of a monitoring framework to enable this approach

### 3.2.2 Influences on the Information Representation

The representations of information obtained from network elements and inputted from domain knowledge are tight coupled in all sorts of network monitoring systems. The information from network resources is mostly represented in pre-defined metrics, which are usually restricted to the manufacturer or underlying protocol. In both industrial and academic field, people are always trying to find a consistent, uniform, internal information representation for network resources. Domain expert knowledge is the knowledge which is adapted to the affordances in coping with task situations in particular domain. In network monitoring, the domain expert knowledge means the accumulated experience and knowledge of network domain experts for diagnosis, analysis and solving network problems. By the analysis in Section 2.4, domain expert knowledge is especially required for non-expert users to monitor their network systems.

The information input from domain knowledge such as a set of policies/rules to perform the necessary computation for network monitoring. In Section 2.2.3, current approaches are reviewed for knowledge modelling. Information models embedded within systems are used to incorporate translation/code generation and policy enforcement processes that automatically

focus network elements in response to monitoring goals and/or the environmental context. However, traditional policy/rule languages lack consistency, especially for highly heterogeneous information representations from network resources, and even supported by a range of authoring tools, it is not convenient to encode and update by domain experts. Furthermore, it is also hard to interpret with information input from different domain knowledge to overall high-level monitoring goals. As an improvement, the autonomic monitoring/management approach leads to some important insights about the nature of information models that suggest more flexible representation of information enabling humans to specify their goals in a nature manner to monitor, visualise and even control autonomic systems with sufficiently expression of cost and performance. Semantic techniques are also widely used to model domain knowledge to remedy the shortcomings of some traditional representation approaches by providing a more consistent and uniform structure. The current knowledge models are mostly aiming for professional network monitoring/management, which bring challenges for non-expert users to understand the meaningful information.

These findings for information representations have motivated and influenced the design by deriving a requirement for non-expert users to understand and monitor their network systems:

**Requirement R2:** A comprehensive information representation must be defined.

This requirement for the design contributes to the research question in Chapter 1 by addressing the research objective:

**Objective 2:** design appropriate encodings and models for domain expert knowledge.

For non-expert users, the information representations are required to support more comprehensive real-time modelling for the information from network resources and present the comprehensive information for high-level monitoring objectives by leveraging domain expert knowledge.

### 3.2.3 Influences on the Monitoring Framework

The meaningful information needs to be visually presented to support non-expert users in understanding and monitoring network systems. Thus, information visualization plays an important role in the network monitoring. The study in Section 2.4 reminds the importance of

the visibility of network components for non-expert users. Because of the usability problems of network monitoring, researchers have called for network monitoring/management tools for non-expert users [Chetty et al. 2007] [Edwards 2001]. They suggested a more interactive tool for network users who have neither the sophisticated technical knowledge nor the motivation to learn complex network systems currently designed for network administrators. If non-expert users are to monitor/manage their networks successfully, they should be given accurate and complete conceptual information of their network. This information is not directly gathered from the heterogeneous network resources, but presenting meaningful information uplifted by leveraging domain expert knowledge to support high-level monitoring goals. These comprehensive representations of network information and domain knowledge require a framework to fit into different network monitoring scenarios.

These findings have motivated and influenced the design by deriving a requirement for non-expert users to understand and monitor diverse network systems:

**Requirement R3:** A framework must be designed to support non-expert users in understanding and monitoring diverse network systems.

This requirement for the design contributes to the research question in Chapter 1 by addressing the research objective:

**Objective 4:** design and implement a framework to apply the knowledge driven information uplift approach to assist non-expert user to perform different monitoring tasks in different network scenarios.

In order to support the monitoring in diverse network systems, a framework is required to apply the information uplift approach with comprehensive representations for network information and domain expert knowledge to visually present meaningful information for non-expert users.

## 3.3 *Requirements for the Design*

This thesis addresses the research question of how and to what extent domain expert knowledge may be leveraged to enable the real time uplift of meaningful information from raw data to support non-expert users in understanding and monitoring network systems. In Section 2.4, four key findings are concluded for non-expert users. A list of remaining challenges and

corresponding technical challenges is derived from the analysis of four key findings of current network monitoring approaches/tools in the state of the art. The following requirements are to fulfil these challenges to design an information uplift approach with corresponding models and framework that would help address these research objectives derived from the research question and that would contribute innovation to related research areas.

Table 3-1 Summary of Design Requirements

| Research Objectives | Design Requirements | | Challenges for Non-expert Users (C) |
|---|---|---|---|
| **Objective 2** | **R1** | **R1.1** | Complete Conceptual Model **(C1)** |
| | | **R1.2** | High-level Monitoring Information Representation **(C3)**<br>Cross-domain Monitoring Information Representation **(C4)** |
| | | **R1.3** | High-level Monitoring Information Representation **(C3)**<br>Degree of Autonomy **(C5)**<br>Drill-down Analysis **(C6)** |
| **Objective 3** | **R2** | **R2.1** | Complete Conceptual Model **(C1)**<br>High-level Monitoring Information Representation **(C3)** |
| | | **R2.2** | Cross-domain Monitoring Information Representation **(C4)** |
| | | **R2.3** | High-level Monitoring Information Representation **(C3)** |
| | | **R2.4** | Difficulties for Creating and Updating Information Representations **(C2)** |
| **Objective 4** | **R3** | **R3.1** | Visual Representation of High-level Monitoring Information **(C8)** |

| | | | |
|---|---|---|---|
| | | **R3.2** | Visual Representation to Improve Usability **(C7)** |

According to the influences from the state of the art, a couple of requirements are listed and analysed to fulfil the research question and objectives:

**Requirement R1**: An approach must be designed to uplift meaningful information from real time data by leveraging the domain expert knowledge.

- R1.1: A knowledge-driven approach must be designed to consume heterogeneous real-time data input.
- R1.2: A knowledge-driven approach must be designed to extract meaningful information from real-time data input.
- R1.3: A knowledge-driven approach must be designed to uplift information to support higher-level monitoring objectives.

**Boundary of R1**: This requirement focuses on the higher-level monitoring objectives of understanding the network problem and monitoring the network status to demonstrate the uplifted high-level information is helpful for non-expert users to achieve the high-level objectives. Other higher-level monitoring objectives will be supported in further research.

The analysis of the state of the art exposes a couple of challenges of current approaches/ tools. Due to the key finding of Visibility for Disparate Monitoring Resources in Section 2.2.5, the Complete Conceptual Model **(C1)** is a challenge to enable the visibility for heterogeneous network resources. For this challenge, the information uplift requires an approach to comprehensively model the heterogeneous data input by leveraging the domain expert knowledge, which helps to "understand" how to consume the data and what in the data. This requirement is addressed in **R1.1**. In order to achieve the High-level Monitoring Purposes for non-expert users, it is important to represent High-level Monitoring Information **(C3)** and Cross-domain Monitoring Information **(C4)**. The nature of network environment determines this uplift process executed in a real time, which is called information uplift in this thesis. A knowledge-driven approach must be designed to fulfil these challenges by extracting meaningful information from low-level to high-level and from different domain of the real-time data input (**R1.2**). As revealed in Section 2.4, the high-level information determines the degree

of autonomy **(C5)** and the effectiveness of drill-down analysis **(C6)** to achieve the high-level monitoring goals for non-expert users. As discussed, the imported expert knowledge is crucial to enable this autonomic analysis. Thus, a knowledge-driven approach must be designed to uplift information to support higher-level monitoring objectives (**R1.3**). This requirement focuses on the higher-level monitoring objectives to support non-expert users in understanding the network problem and monitoring the network status, which are the common challenges non-expert users experienced according to the research in Section 2.4. This aims to demonstrate the uplifted high-level information is helpful for non-expert users to achieve the high-level objectives. **Requirement R2**: A comprehensive information representation must be defined.

- R2.1: A comprehensive model for heterogeneous data input resources
- R2.2: A comprehensive model for the cross-domain knowledge
- R2.3: A comprehensive model for the high-level information
- R2.4: A comprehensive encoding for the domain expert's insights

**Boundary of R2**: This requirement focuses on the representation of domain knowledge to drive the information uplift approach. The invoking of existing domain knowledge (in either semantic or other knowledge representation) is not the focus of this research.

From the study of *Network Monitoring Tools for Non-expert Users*, current network systems have increasing complexity. Even non-expert users no longer satisfied the monitoring of network status, they require more comprehensive approaches to understand and monitor their networks. As concluded in Section 2.4, how to represent the information is the crucial for network monitoring systems. A comprehensive representation is required to ensure the flexibility, autonomy and intelligence of the system, which can also improve the understanding with high-level meaningful information. Derived from **C1**, a comprehensive model is required **(R2.1)** for heterogeneous data input resources, which refer to the network resources in network systems. Hence, this model should support diverse network resources and model them in a comprehensive way to enable the reasoning across different models. Semantic modelling is proven as an effective solution for this requirement. As discussed in Section 3.2.2, non-expert users especially require domain expert knowledge to assist them to understand the network monitoring information. In order to achieve a higher-level understanding for non-expert users,

the knowledge model is required **(R2.2)** to support more different monitoring domains, such as Quality of Service, network status, Quality of Experience, and most important is enable the information aggregation cross diverse monitoring domain. In Section 2.4, the high-level information is required **(R2.3)** to represent for high-level monitoring objectives. The technical challenges here indicate the research gap in semantically modelling high-level information in the network systems. Focusing on the encoding challenge for domain experts, this model should provide appropriate methods **(R2.4)** to encode the domain expertise and enable these knowledge models to support comprehensive reasoning across diverse knowledge models and heterogeneous models of network resources. This model provides a representation for the inputted expert knowledge, which derives the network diagnosis, analysis and troubleshooting across the underlying network models. This requirement addresses the research objective 2 to support the information uplift approach. As revealed in Section 2.3.3, the on-line open knowledge is widely used by a large number of knowledge-driven systems, but the knowledge for network monitoring and management is still not well presented on the internet. And there is already a series of research about how to invoke the existing knowledge representation (mostly in CIM or other models) into the semantic knowledge models. In order to achieve the research question, this requirement mostly focuses on the representation the domain knowledge to drive the information uplift approach.

**Requirement R3**: A framework must be designed to support non-expert users in understanding and monitoring diverse network systems.

- R3.1: A framework must be designed to be compatible with diverse network systems.
- R3.2: A framework must be designed to visually represent high-level monitoring information for non-expert users.

**Boundary of R3**: This requirement is not supposed to support all types of network systems for non-expert users. The network systems should be determined by the performance, accuracy and scalability boundary of this framework.

From the influences of state of the art, the information uplift approach requires a comprehensive support to leverage accurate and complete conceptual network information to achieve the monitoring purposes in diverse network environments. Due to this requirement, a

monitoring framework must be designed to contain the information uplift approach with corresponding information representations to fit into diverse network environments (**R3.1**). As a key finding for non-expert network users, the visual representation of network information is required to improve visibility of network systems, which is still challenged by the usability (**C7**) and representations for high-level monitoring information (**C8**). This key finding addresses the requirement for the monitoring framework to visually represent high-level monitoring information for non-expert users (**R3.2**). But this monitoring framework is not supposed to adapt all types of network systems for non-expert users. The adaptation for diverse network systems should be determined by the performance, accuracy and scalability boundary of this framework, which is evaluated and stated in the Evaluation Chapter.

This section analyses the influences from state of the art and concludes the remaining challenges and key findings. According to this analysis and conclusion, three requirements are processed for the information uplift approach, information representation, and the monitoring framework. Furthermore, these requirements can also be applied to the Evaluation Chapter to suggest the evaluations.

## 3.4 *Design*

According to the influences and requirements aggregated in previous sections, this section describes the design of Information Uplift Approach, Information Representation and Monitoring Framework into three sub-sections. The design in this section is illustrated with one network monitoring use case, which refers to the use case of the Home Area Network (HAN) monitoring stated in the next chapter. This design will be implemented in the Implementation Chapter with example use cases and evaluated in the Evaluation Chapter.

### 3.4.1 Design Overview

According to the design requirement, the design in this chapter is composed by three components: Information Uplift Approach, Information Representation, and Monitoring Framework.

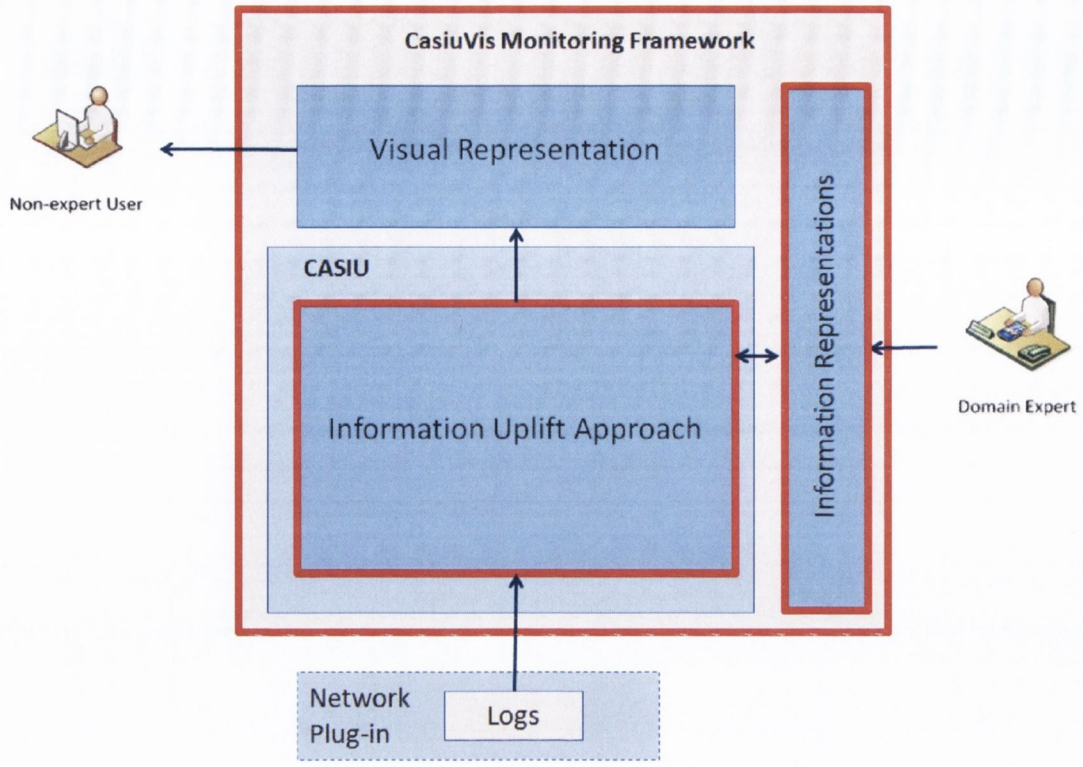



Figure 3-1 Design Overview

As the highlighted with red frames in the design overview (Figure 3-1), the Information Uplift Approach consumes the heterogeneous real-time network log data input and provides uplifted meaningful information for non-expert users to support high-level monitoring objectives via visual representation. The information is extracted from the real-time log data stream by using the information extraction technologies reviewed in Section 2.3.2. By leveraging the domain knowledge captured from the domain experts, the meaningful information is uplifted from the information modelled in appropriate representations. In order to achieve the high-level network monitoring objectives, the CASIU, visual representations and information representations are composed into a monitoring framework, called CasiuVis to support non-expert in understanding and monitoring diverse network systems. These three components will be detailed introduced in following sections.

### 3.4.2 Example Use Case

The design in this chapter is demonstrated with two example use cases, which refers to the use case descriptions of the Home Area Network (HAN) stated in the Section 4.3 in the next chapter. This HAN monitoring use case is briefly introduced as following:

The home area networks (HANs) are widely deployed with evolving complexity, which can rival that of enterprise networks of the recent past. Nonetheless there is one very important difference – HANs do not typically have trained network operations staff to administer them. Inexperienced HAN users are considered as non-expert users who are continuously confused and frustrated with even simple HAN performance and maintenance tasks [Yankee Group 1998]. Additional cost for both the network provider and HAN user will be incurred to detect and diagnose such issues. A significant impediment to recognition, diagnosis and correlation such events for non-expert users is the problem of knowing what is happening, why it is happening and how to solve it in their HANs. In the example use case, an important VoIP call on an iPad suddenly suffers degradation of service quality, which affects the Quality of Experience (QoE) for HAN users. This problem is perhaps caused by WiFi connection problem referring to some other WiFi activities initiating on the same channel – causing interference, or a signal weakens when the device antenna is obstructed, or another user may be downloading a large file on a wired PC connected to the same home network which causes network congestion. Such events may be unremarkable but will impact on the end-user's perception of the quality of the service supported by the network connection.

### 3.4.3 The Design of Information Representation

#### *3.4.3.1 Design Overview of the Information Representation*

As discussed in Section 2.2.4, in order to achieve a functional network monitoring system, the information obtained from network and inputted from domain knowledge must be imported to give the status of the network and govern decisions about network monitoring. Comprehensive representations are required to ensure the flexibility, autonomy and intelligence of the network monitoring system to improve the availability of meaningful information for non-expert users. Four comprehensive information models and encodings are designed to fulfil the requirements listed below:

**Requirement R2**: A comprehensive information representation must be defined.

- R2.1: A comprehensive model for heterogeneous data input resources
- R2.2: A comprehensive model for cross-domain knowledge
- R2.3: A comprehensive model for high-level information

- R2.4: A comprehensive encodings for domain expert's insights

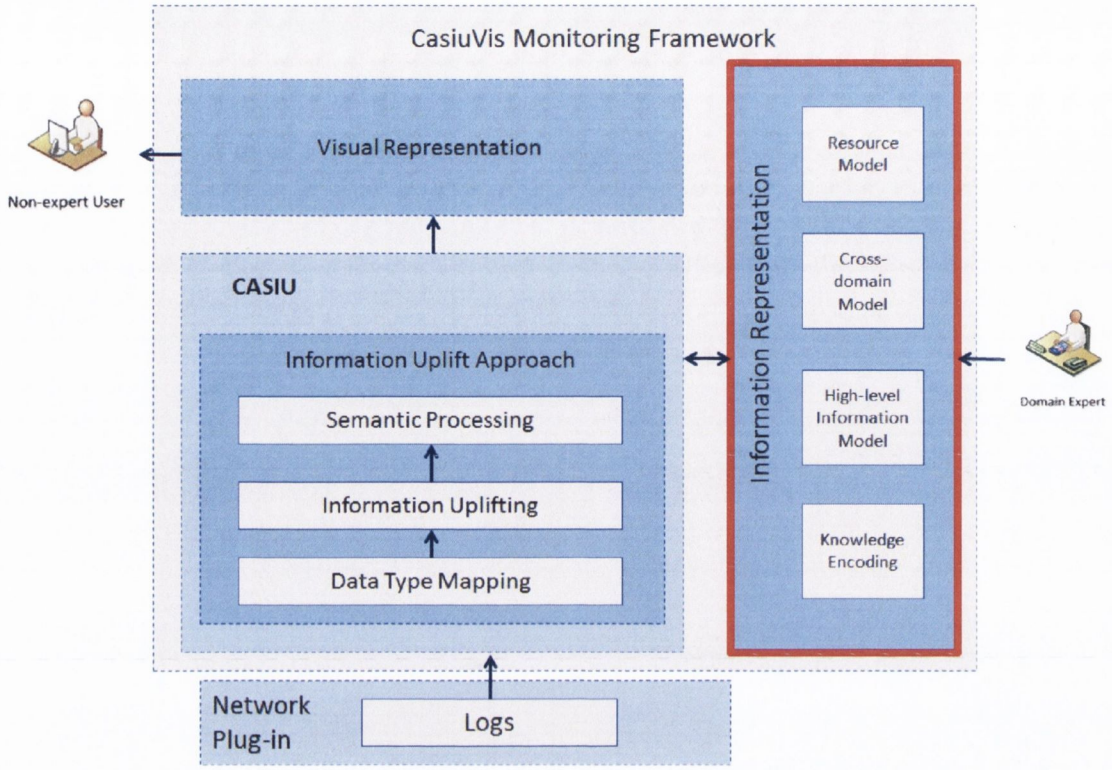



Figure 3-2 The Design of Information Representations

In this design (Figure 3-2), the information representations are designed to represent the information extracted and uplifted in the information uplift approach, which is also driven by the captured and modelled domain expert knowledge in a comprehensive way. The resource model and high-level information model are used to represent the information extracted and uplifted from the input data. The expert knowledge encoding and cross-domain model are leveraged to capture and model the domain expert's insights and the knowledge in diverse network domains. These representations play an important role in the information uplifting process, which is illustrated in Figure 3-8.

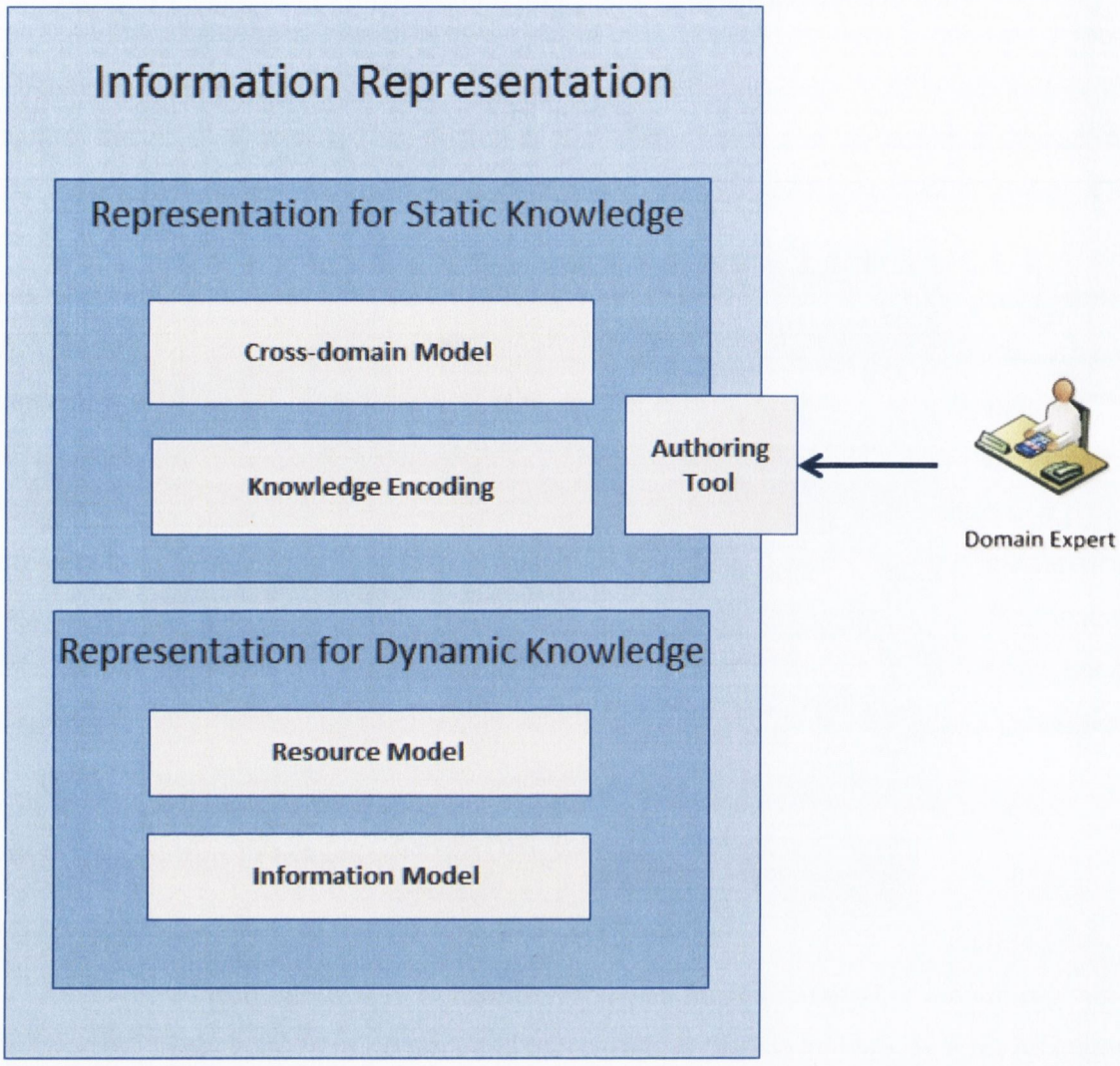



Figure 3-3 The Design of Information Representations

In the information uplifting process, the input data is modelled into Resource Model by mapping the data type elements to the classes in the Cross-domain Knowledge Model. By leveraging the knowledge in the Cross-domain Knowledge Model and the Domain Expertise Encoding, the information in the Resource Model is uplifted into the High-level Information Model. An authoring tool captures the domain expert's insights into domain knowledge encodings and the high-level information is visually represented to non-expert users to support better understanding and monitoring of their network systems.

The design of the Resource Model, the High-level Information Model, the Domain Expertise Encoding and the Cross-domain Knowledge Model is introduced in following

sections.

#### *3.4.3.2 Design of Resource Model*

The Resource Model aims to provide a comprehensive representation for the information inputted from heterogeneous network resources. Thus, this model is designed separately for network resources in different network domains. In the example use case, the network resources are modelled separately into network devices and services, whose designs are presented in the following tables (Table 3-2, Table 3-4). The semantically modelled resource is maintained in the entity pool.

Table 3-2 Summary of Components in Resource Model for Devices

| Name | Description | Representation | Data Type |
|---|---|---|---|
| Resource Type | The type of resource which generates the input data | Sub-classes of NetworkResource class | RDF URI |
| Resource ID | The unique id of network resource | Integer data associated with hasID data property | int |
| ConnectTo | The id of the network resources in the network topology | Instances of sub-classes of NetworkResource class | RDF URI |
| Data Type | The data types in the metrics of this resource | Sub-classes of DataType class | RDF URI |
| Annotated Entity | The id of the semantic entity annotated to this resource | Integer data associated with hasID data property | int |
| Description | The description of the resource | The description formatted into the description element of this schema | String (Optional) |

Table 3-4 describes the components in Resource Model for network devices. The Resource Type is referred to the ResourceType classes in the Cross-domain Knowledge Model, which enables the reasoning for the resource type during the information uplifting and semantic

processing phases. The Resource ID is the unique id for this resource in the entity pool. ConnectTo shows the connected other devices in the network topology. The data type refers to the elements in the metrics of this resource, which is mapped to the data type class in the knowledge model. Annotated Entity indicates the unique id of semantic entity in the entity pool. The model for semantic entity will be introduced in the High-level Information Model. An example of device GW001 in RDF triples is listed below:

Table 3-3 Example for Device Model in RDF triples

| **Subject** | **Predicate** | **Object** |
|---|---|---|
| rsID:GW001 | Rdf:type | netOwl:Gateway |
| rsID:GW001 | netOwl:connectTo | rsID:DSLAM003 |
| rsID:GW001 | netOwl:connectTo | rsID:IPAD001 |
| rsID:GW001 | netOwl:dataType | netOwl:PLR |
| rsID:GW001 | netOwl:dataType | netOwl:Throughput |
| rsID:GW001 | netOwl:annotation | seID:Throughput_high_34958 |
| rsID:GW001 | Rdf:description | "D-link model mk502" |

In this example, a device has resource ID (rsID:GW001) and its resource type is Gateway (netOwl:Gateway).This gateway connects to two other devices: DSLAM003 and IPAD001. Two datatypes (PLR and Throughput) from its log data are associated with this gateway. One semantic entity also annotated to this device with id: Throughput_high_34958. It also has a description, which is an optional attribute.

Table 3-4 Summary of Components in Resource Model for Services

| Name | Description | Representation | Data Type |
|---|---|---|---|
| Resource Type | The type of resource which generates the input data | Sub-classes of NetworkResource class | RDF URI |
| Resource ID | The unique id of network resource | Integer data associated with hasID data property | int |
| Source | The source of the network service in the network topology | Integer data associated with hasID data property | int |
| Destination | The destination of the network service in the network topology | Integer data associated with hasID data property | int |
| Node | The node that the network service passed through | Integer data associated with hasID data property | int |
| Data Type | The data types in the log data metrics of this service | Sub-classes of DataType class | RDF URI |

| | | | |
|---|---|---|---|
| Annotated Entity | The id of the semantic entity annotated to this resource | Integer data associated with hasID data property | int |
| Description | The description of the resource | The description formatted into the description element of this schema | String (Optional) |

Comparing to the model for devices, the model for network services has extra elements to model the source, destination and passed node of this service. An example of service IPTV001 in RDF triples is listed below:

Table 3-5 Example for Service Model in RDF triples

| **Subject** | **Predicate** | **Object** |
|---|---|---|
| rsID:IPTV001 | Rdf:type | netOwl:IPTV |
| rsID:IPTV001 | netOwl:source | rsID:VSERVER001 |
| rsID:IPTV001 | netOwl:destination | rsID:IPAD001 |
| rsID:IPTV001 | netOwl:node | netOwl:GW001 |
| rsID:IPTV001 | netOwl:dataType | netOwl:PLR |
| rsID:IPTV001 | netOwl:annotation | seID:PLR_high_32312 |
| rsID:IPTV001 | Rdf:description | "HD IPTV service" |

In this example, a service has resource ID (rsID:IPTV001) and its resource type is IPTV service (netOwl:IPTV).This IPTV service is delivered from a video server (VSERVER001) to an ipad (IPAD001) via one node (GW001). One datatype (PLR) from its log data is associated with this service. One semantic entity also annotated to this device with id: PLR_high_32312. It also has a description, which is an optional attribute.

This section introduces the Resource Model, which enables the data type mapping and information uplift approach. The High-level Information Model will be described in next section.

#### *3.4.3.3 Design of High-level Information Model*

In Section 2.4, the high-level information model is required **(R1.3)** to represent meaningful information to support non-expert users for the high-level monitoring objectives. There are three different kinds of entities encoded by domain experts to represent high-level information to enable non-expert users to achieve high-level monitoring goals by understanding the problem and monitoring the status of network systems:

- Event: a high-level description of the status or incident of network resources
- Behavior: a description of the action, reaction or functioning of network resources
- Anomaly: an event may affect the Quality of Experience (QoE) for end-users

These three kinds of high-level entities are represented in one comprehensive model.

Table 3-6 Summary of Components in High-level Information Model

| Name | Description | Representation | Data Type |
|---|---|---|---|
| Entity Type | The type of semantic entity including: event, behaviour and anomaly | Sub-classes of SemanticEntity class | RDF URI |
| Entity ID | The unique id of semantic entity | Integer data associated with hasID data property | int |
| Rely On | The id of other entities including semantic attributes relied on this entity | Integer data associated with hasID data property | int |
| TimeStamp | The time stamp of when the entity is annotated | Integer data associated with hasTimestamp data property | int |
| Duration | How many seconds this entity lasts | Integer data associated with hasDuration data property | int |

| | | | |
|---|---|---|---|
| Description | The description of the resource | The description formatted into the description element of this schema | String (Optional) |

Table 3-6 describes the components in High-level Information Model for semantic entities. The Entity Type is referred to the EntityType classes in the Cross-domain Knowledge Model, which enables the reasoning for the entity type during the information uplifting and semantic processing phases. The Entity ID is the unique id for this entity in the entity pool. The property of relyOn indicates the relationship between the entities annotated to the same resource. TimeStamp is used to record when the entity is annotated and Duration shows how long it lasts. As an example in Figure 3-6, the Event GW_unusual_transfering presents the high-level meaning on the gateway (GW#1). And this event is relied on the Behaviour GW_transfering and the Event GW_unusual_connection, which are also annotated on the same network resource (GW#1) and relied on other semantic attributes/entities.

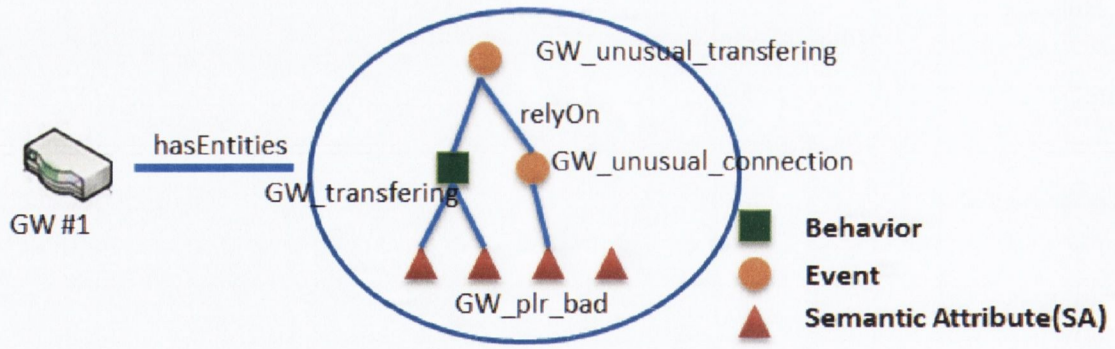



Figure 3-4 The Semantic Entities to a Network Resource in the Entity Pool

This section introduces the High-level Information Model, which represents the high-level meanings on the network resources. The Domain Expert Encoding will be described in next section.

#### *3.4.3.4 Design of Domain Expertise Encoding*

The key objective of capturing domain expert knowledge is to fulfil the requirement **R1.4** to enable an ordinary domain expert, that is one without semantic technology background, to encode their insights to the domain; to support the encoded insights of an expert to be built on top of diverse types of log data input; to promise the interoperability with existing knowledge models in other network monitoring domain; and to support semantic reasoning across higher-level meaningful information.

According to the review in Section 2.3.4, Semantic Attribute is a semantic encoding initially developed for the concept in particular knowledge domain, which is adopted and further developed in this research to capture and encode the domain expert insights. The semantic attributes in this thesis are discrete units of domain expertise that can be combined together and tailored to support non-experts monitor a specific domain e.g. consumers wishing to monitor their home network. Furthermore, semantic attributes typically act as abstractions and simplifications from the raw data, which are intended to make the data more understandable for the non-expert user. Semantic attributes are encoded in a semantic representation and contain domain rules that can be automatically converted into formal semantic rules such as SWRL [18], in order to enable automatic knowledge reasoning and querying. Importantly, a user-friendly authoring tool called SABer, is reviewed in Section 2.3.4 which can effectively capture insights from domain experts without necessitating manual semantic encoding.

As described in the design of data mapping approach in Section 3.4.4.1, the semantic concept models are linked to elements in the log data and related domain ontology classes. These mappings enable information extraction by annotating semantic attributes to a stream log data and support higher-level uplifting of meaningful information and knowledge-based semantic reasoning, which are foundations of the knowledge-driven information uplift approach.

In order to fulfil the design requirement, the semantic attribute has been adapted to support the complex, distributed and dynamic nature of network monitoring and has been refined into three sub-categories: Basic Semantic Attribute, Semantic Segment and Temporal Semantic Attribute. Each are described below:

1) Basic Semantic Attribute

Basic semantic attributes are designed to describe the domain concepts directly related to the raw data, which can be adopted by the information uplift approach to extract the meaningful information from raw data. They encapsulate the expert's subjective insights of a domain and consist of the components in following table (Table 3-7):

Table 3-7 Summary of Components in Basic Semantic Attribute

| **Name** | **Description** | **Representation** | **Data Type** |
|---|---|---|---|
| Concept Name | A semantically meaningful concept | String data | String |
| Operator | An operator of constraints related to the concept | moreThan, lessThan, equal, and temporal operators | String |
| Thresholds | Thresholds of the constraints specified by experts | Integer data (unit: millisecond) | int |
| Data Type Mapping | Links to the target element of data metrics | Instance of sub-classes of DataType class | RDF URI |
| Domain Knowledge Mapping | Links to the domain knowledge class of semantic entities | Instance of sub-classes of SemanticAttribute class | RDF URI |

In this design, the semantic attribute describes a meaningful concept related to the data with a constraint to define the condition of how to trigger this concept. This constraint is encoded with the expert-specified operator and parameter. The operator presents the constraint with a set of pre-defined logical operations to the thresholds, like moreThan, lessThan, equal, etc. Thresholds are defined and adjusted according to domain experts' subjective insight. This semantic attribute can be created and adjusted through the authoring tool. When a new semantic attribute created, a new instance is added to the semantic attribute ontology class and linked with its semantic encoding. Furthermore, the constraint that has been encoded should be automatically converted into the formal rule and query languages. This semantic attribute can only be applied on the data type specified in the semantic encoding. The instances of this semantic attribute model are generated during to information uplift process and maintained in the entity pool.

2) Semantic Segment

Semantic Segments represent definitions of higher-level semantic meanings captured from domain experts, with a combination of semantic attributes, references to domain ontology classes and corresponding logic. Semantic Segments are settled into a semantic schema to capture domain experts' insights of semantic entities like network event, behaviour, and anomaly with their conditions, and related reasons or solutions. The corresponding logic goes beyond the typical use of structured knowledge (ontologies) by enabling generic rules or temporal logic to be combined with traditional semantic technologies. This provides a highly abstracted description about logical rules and conditions for semantic entities, which are, for example, automatically decomposed into atomic rules and queries through the semantic processing approach.

Table 3-8 Summary of Components in Semantic Segment

| Name | Description | Representation | Data Type |
|---|---|---|---|
| Concept Name | A high-level semantically meaningful concept | String name | String |
| Concept Type | The type of defined high-level semantically meaningful concept | Sub-classes of SemanticEntity class | RDF URI |
| Applied Target | A target this concept can be applied on | Sub-classes of NetworkResource class | RDF URI |
| Conditions | A set of constraints to determine how this concept is triggered | A set of operators and thresholds combined with logical relationship (and, or, not, etc) | String |
| Reasons (Optional) | A set of constraints to determine what reason this concept is caused | A set of operators and thresholds combined with logical relationship (and, or, not, etc) | String (Optional) |

| | | | |
|---|---|---|---|
| Solution<br><br>(Optional) | A set of constraints to determine what solution is suggested to this concept | A set of operators and thresholds combined with logical relationship (and, or, not, etc) | String (Optional) |

Specified in the semantic segment schema, a high-level semantic concept is defined and associated with an instance of semantic segment class in the network domain ontologies. This semantic segment could be applied on a particular, or on a range of target network resources. The CASIU engine inspects the condition of this semantic segment with related semantic entities in the semantic entity pool and then the network resource type of the target instance to determine whether or not this semantic concept is applied. On the contrary, the condition can also be used to refer to the reason that caused this semantic entity. The condition is also associated with a set of constraints. These constraints are presented into formal semantic logical representations, which enable the semantic reasoning across the semantic entities in the entity pool and related knowledge models. The constraint also is stated in atomic segments to enable reasoning interoperating over instances and entities from different knowledge domains. The solution contains a set of constraints to suggest appropriate solutions for particular root cause reason of the anomaly.

3) Temporal Semantic Attribute

The dynamic and complex nature of current consumer networks requires an effective and flexible real-time knowledge reasoning and processing capability. By extending a current temporal knowledge reasoning approach, our approach focuses on enabling customized and flexible temporal reasoning, based on captured domain expert's insights. For arbitrary two events X and Y, all temporal relationships can be represented with three operators: **DURING** (one event happens within the period of the other event happening), **AFTER** (one event happens after the other), and **WITH** (two events start and end at the same time). Moreover, J. Keeney et al. [Keeney 2010] generalized these operators as: **DURING**, **AFTER (L)**, and **FILTER (OP, L)**. They introduced a time limit L and a filter for comparing any arbitrary attributes, using an arbitrary logical operator with a time limit L. In order to ease the difficulty

of encoding and enriching the semantic representation, we allow domain experts to compose wit0h the existing three operators to express the complex insight for semantic entities.

Table 3-9 Example of Expert Defined Operators

| **Expert Defined Operators** | **Description** | **Representation** |
|---|---|---|
| $X$ long_time_before $Y$ | The end time of entity $X$ happened long time before the start time of entity $Y$ | $Y_S$ **AFTER** (L>500ms) $X_E$ |
| $X$ just_overlap $Y$ | The entity $X$ just happens before event Y and also ends before $Y$ | $Y_S$ **AFTER** (L<100ms) $X_S$ $\wedge$ $Y_S$ **DURING** $X \wedge Y_E$ **AFTER** $X_E$ |
| $X$ recently_long_time_before $Y$ | The entity X recently happens long time before entity Y | $w$=3000ms; $Y_S$ **AFTER** (L>500ms) $X_E$ |

With these three basic operators, experts are able to define more complex and flexible operators (Table 3-9) for temporal reasoning. In order to balance the cost of the reasoning process and express real world requirements, we introduce a window parameter $w$ as a time limit for tracing back the historical entities in the entity pool. These expert-defined operators are available for logical representation in the definition of basic semantic attributes and semantic segments. The temporal reasoning also has the capability of interpreting heterogeneous domain knowledge by rephrasing the logical representation into formal rules.

#### *3.4.3.5 Design of Cross-domain Knowledge Model*

As discussed in Section 2.4 (**C4**), non-expert users especially require cross-domain expert knowledge to monitor network systems. Domain refers to the knowledge domain which is adapted to the affordances in coping with network task situations, e.g. the knowledge domain of network devices, network service, network quality, etc. Cross-domain indicates the correlation

of knowledge from different domain. For non-expert users, a domain knowledge model is still required to support more comprehensive real-time cross-domain reasoning and establish the understanding between high-level monitoring objectives and low-level network resources. Domain experts are typically only familiar with a sub-set of consumer network domain and their knowledge is captured with respect to specialized and discrete sub-network models. Due to the formal structure of Web Ontology Language (OWL), these sub-knowledge models have the capability to interact with other models. These sub-knowledge models are correlated by four main ontology classes in the knowledge model (Figure 3-5). They model the tangible components in the network and support anomaly identification, diagnosis and analysis.

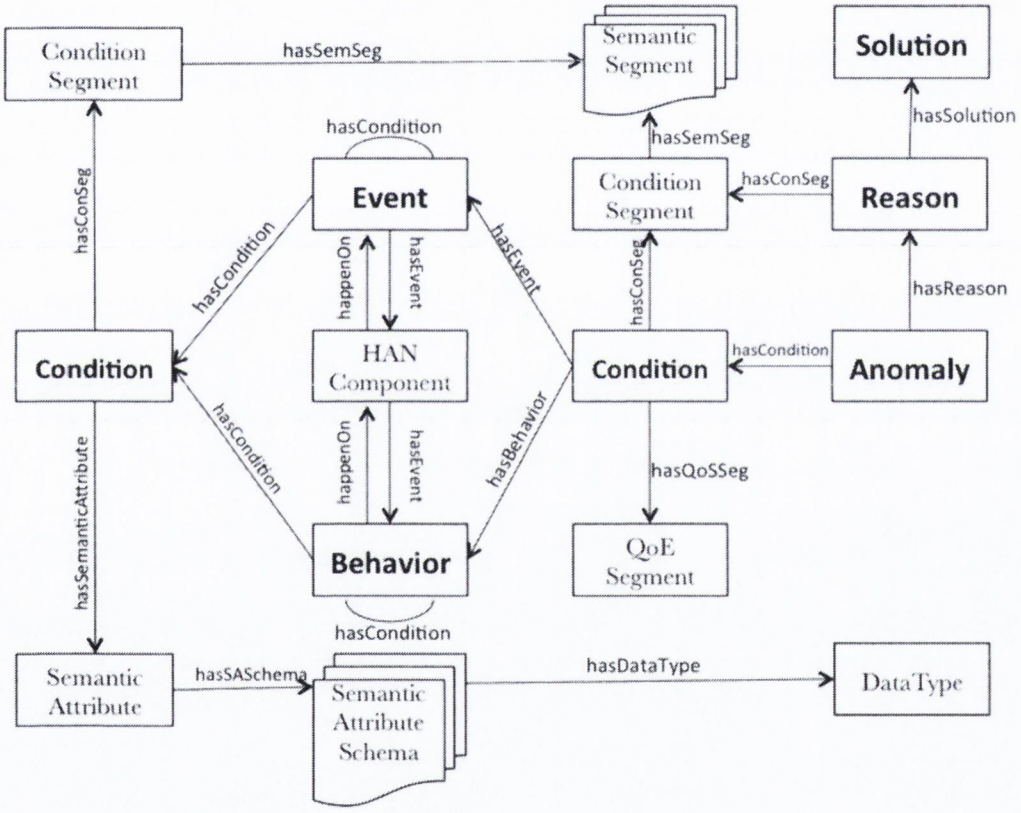



Figure 3-5 The Cross Domain Knowledge Model

The domain expert knowledge model (Figure 3-5) enables network monitoring for non-expert users. It acts as a bridge between expert insights, network logs and network visualizations for non-experts. Rather network being a single over-arching network knowledge

model, the domain expert knowledge model is an upper or meta-model that enables the easy integration of multiple domain specific models, for example for individual devices. Crucially it defines a framework for linking human expert insights about these models or systems and system artifacts such as device logs or events. It also allows experts to encode knowledge about system states, behaviors and potential network or service anomalies. This is significant because these upper model concepts can then be used to span multiple device or network models. In the meta-model, the semantic attribute and semantic segment are the two key concepts used to enable efficient processing and combination of domain expert insights based on heterogeneous network component models.

In addition the domain expert knowledge model provides ontology classes to support problem identification, diagnosis and analysis. These are (Figure 3-10): *Condition*, *Semantic Entity* (*Event*, *Behavior*, and *Anomaly*), *Reason*, and *Solution*. These represent conditions that could be a trigger for another event, behaviour or anomaly. The *Event* class is used to describe the network performance status and sudden changes in state. The *Behavior* class indicates the behavior happened on/between network components. The *Anomaly* class is used to represent events or behaviors that affect the Quality of Experience (QoE) for users. The *Reason* class is used to relate expert-defined reasons to an anomaly of a given type. The *Solution* class is used to describe expert-defined solutions for combinations of reason and anomaly.

### 3.4.4 The Design of Information Uplift Approach

#### *3.4.4.1 Design Overview of the Information Uplift Approach*

Central to an information uplift approach is the availability of data in a highly structured form that references representations of information from heterogeneous network resources. This approach consumes the real-time data input and provides the interface to visualise the uplifted information. This approach is realised in a Semantic Information Uplift Engine (CASIU), which is described in the following diagram:

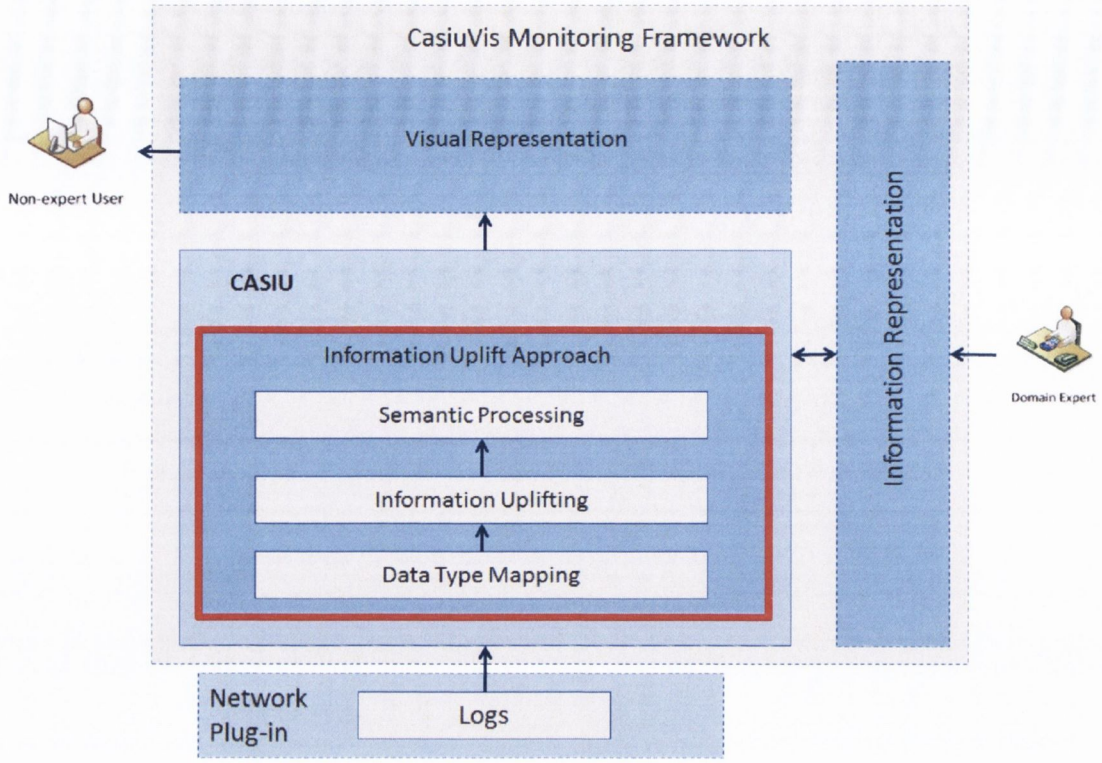



Figure 3-6 Overview of the Information Uplift Approach

In the overview (Figure 3-6), the information uplift approach receives data input from the real time log data. These log data are generated by the usage of network by non-expert network users. In the network environment, the log data sets are normally collected from the network central node, like the gateway in the Home Area Network or DSLAM, Core Router, Video Server in the IPTV delivery network. In practice most network nodes produce structured logs, which follow diverse log metrics. Thus the first problem to be addressed is to "understand" this data. The information implied in the large volume data set is always overloaded. The imported expert knowledge can help to determine how to extract the meaningful information from real-time log data stream by using the information extraction technologies reviewed in Section 2.3.2. This knowledge is captured from the domain expert or invoked from the knowledge models required in **R1**, and then modelled into appropriate knowledge representations. The section problem is how to leverage the domain expert knowledge to extract the meaningful information from the real-time log data stream and maintain them in appropriate storage. In order to achieve the high-level monitoring objectives for non-expert users, the third problem is to uplift higher-level meanings by enabling a certain degree of autonomy and the drill-down analysis. This uplifted information is visually represented to support non-experts in

understanding and monitoring their networks. The requirements proposed for information uplift approach are:

**Requirement R1**: An approach must be designed to uplift meaningful information from real time data by leveraging the domain expert knowledge.

- R1.1: A knowledge-driven approach must be designed to consumer heterogeneous real-time data input.
- R1.2: A knowledge-driven approach must be designed to extract meaningful information from real-time data input.
- R1.3: A knowledge-driven approach must be designed to uplift information to support higher-level monitoring objectives.

In order to fulfil these requirements, this domain expert knowledge-driven information uplift approach (Figure 3-2) is designed in three sub-approaches: data type mapping, information uplifting and semantic processing. The design of these sub-approaches is introduced in following sections.

#### *3.4.4.2 Design of Data Type Mapping*

In order to fulfill the requirement **R1.1**, Figure 3-3 shows how to "understand" the meaning of the element in the log data metric. The Data Type Mapping maps the entity in domain expert knowledge model to the element in the log data metric. This mapping process is promised by a number of mapping schemas, which are encoded by the domain expert. The outputs of this approach are a set of resource models, which refers to the domain knowledge model to make them understandable by the information uplift engine.

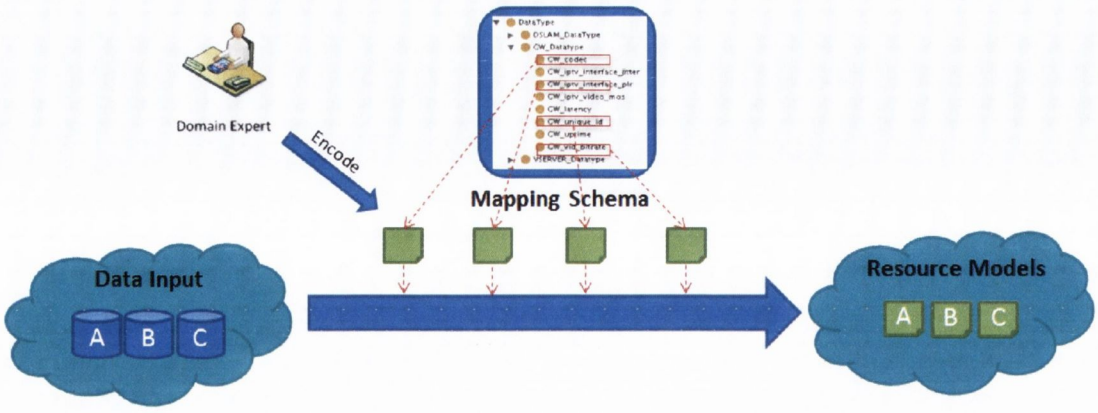



Figure 3-7 The Design of Data Type Mapping

The components and models adapted by the Data Type Mapping approach are described in Figure 3-7 and listed in Table 3-10.

Table 3-10 Summary of Components and Models in Data Type Mapping Approach

| Name | Description | Representation |
|---|---|---|
| Data Input | The data input formatted in heterogeneous metrics | CSV, XML, etc. |
| Mapping Schema | The schema encoded by domain expert to map the element between data metrics and domain knowledge model | See Table 3-3 |
| Domain Knowledge Model | The model to represent the domain expert knowledge | See Section 3.4.2.2 |
| Resource Model | The model to represent the network resources | See Section 3.4.2.1 |

**Data Input:** As discussed in Section 3.2.1, the input data in the network environment is highly heterogeneous log data. They are generated by a number of diverse network devices and

services and collected from the central nodes. The CSV and XML format are chosen as representatives, which show how our approach processes plain data and markup tags. The supported format could be easily expanded. The log data is formatted in different metrics, like the traffic log of gateway formatted in CSV file with data columns for throughput, packet loss, latency, uptime, etc. and the event log of video server formatted in XML file with elements for event name, event timestamp, event type, etc. These columns or elements in the log files are called data type element in this research.

**Mapping Schema:** The mapping schema is the key component in this approach. It is used to indicate the relationship between data type element and the data type class in the cross-domain knowledge model, and then the resource models are generated according to this relationship mapping. By consuming the generated resource models, the CASIU can understand the meaning of the input data and then trigger suitable rules or invoke a corresponding knowledge model for the information uplifting on that input data. When a new type of data input arrives or new metrics updates, this schema can be encoded or adjusted by the domain expert. The mapping schema should have following components:

Table 3-11 Summary of Components in Data Type Mapping Schema

| Name | Description | Representation | Data Type |
|---|---|---|---|
| Resource Type | The type of resource which generates the input data | Sub-classes of NetworkResource class | RDF URI |
| Resource Format | The format of log file from resource | CSV, XML, etc. | String |
| Element Name | The name of the element in the input data | Sub-classes of DataType class | String |
| Data Type Mapping | The element mapped to the data metrics | Column in CSV log file, data element in the XML file, etc. | String |
| Knowledge Mapping | The URI of the class in knowledge model | The URI of OWL class | RDF URI |
| Description | The description of the element | The description formatted into the description element of this schema | String (Optional) |

**Resource Model:** See Section 3.4.3.2.

**Domain Knowledge Model**: See in Section 3.4.3.5.

### *3.4.4.3 Design of Information Uplifting*

The information uplifting approach extracts information by annotating semantic meanings onto the captured characteristics of identified network stream log data and models the extracted information in appropriate representation, which references to the domain expert knowledge model. As shown in Figure 3-8, this information uplifting approach is divided into two processes: the semantic attribute annotation process and the semantic entity annotation process.

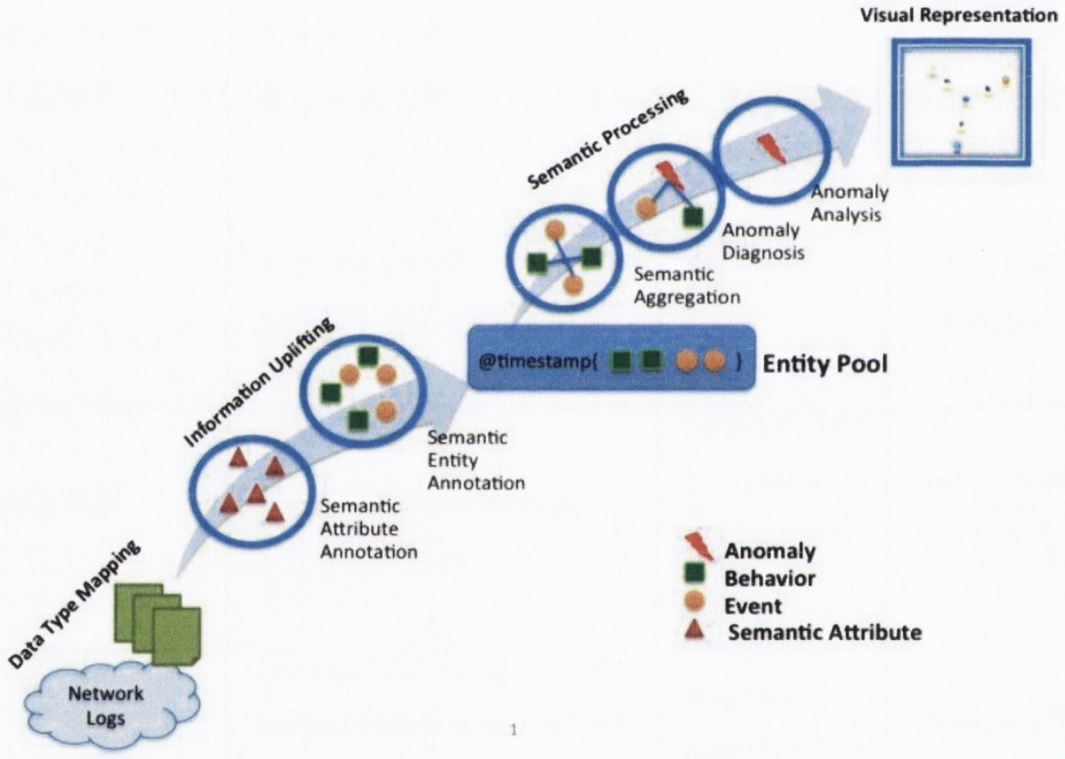



Figure 3-8 The Design of Information Uplift Approach

1) Semantic Attribute Annotation Process

The semantic attribute annotation process aims to extract meaningful information from real-time data stream to fulfil the design requirement **R1.2**. Although this real-time data is fed into the semantic attribute annotation process based on highly heterogeneous metrics, the data

types (e.g. packet_loss_rate in the HAN Use Case) of metrics are aggregated and mapped to corresponding data type elements in the knowledge model. Hence related semantic attributes can be applied to the same data type to simplify the annotation process. This process supports diverse information extraction and annotation patterns for semantic attributes, which are pieces of semantic encodings captured from domain experts (details in Section 3.4.2.4). When processing the real-time data streams, the pattern detection algorithms have been applied to aggregate and detect data value changes that capture the characteristics of the data stream by dividing the data into discrete intervals of moderately varying behaviour or time-stamped change points where there are abrupt changes of the steady state metric values. The appropriate semantic attributes are associated with these characteristics in the raw log streams or metrics. Information extraction techniques are applied to capture the characteristics of the stream data. As an example in Figure 3-9, in a given time interval, heterogeneous log data from devices and services in the network is collected and aggregated. The pattern detection algorithm A is applied to detect the changes of the steady state metric values of the real time data stream. This algorithm also divides the data stream into discrete intervals and points. Another pattern detection algorithm B aggregates the data value and captures the characteristics in each discrete interval. Then these captured characteristics are annotated with semantic attributes like "throughput_high" and "throughput_low" in the HAN Use Case.

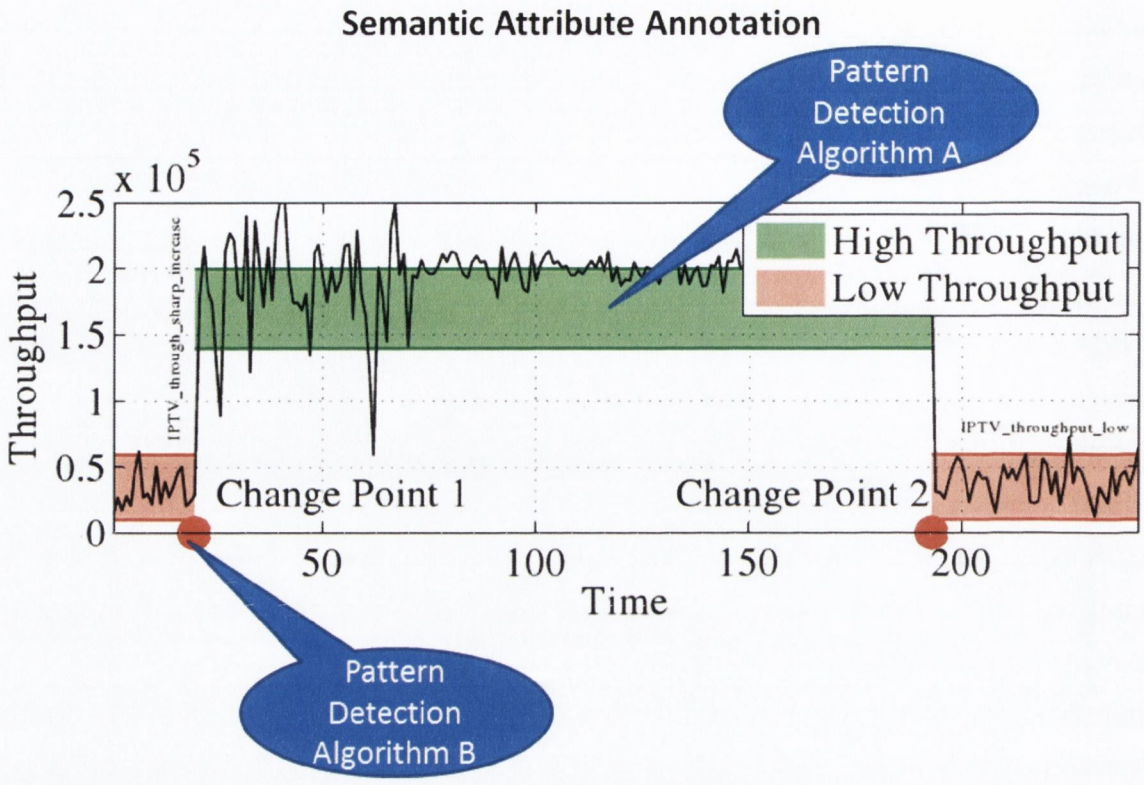



Figure 3-9 The Pattern Detection Algorithms Applied on the Real Time Data Stream

As an example of Pattern Detection Algorithms, a Change Point Correlator algorithm based on [Athanasopoulos et al. 2008] is described below to detect the change point in real time data stream. This detection relies on parameters like *window*, *α_fast*, *α_slow*, which can be adjusted by domain experts in different scenarios.

**Algorithm 1:** CHANGE POINT CORRELATOR

**Input**: $currentValue$ of input steam data
$w$ of current window
$fast$ parameter for fast moving
$slow$ parameter for slow moving
**Output**: annotation on $currentValue$

```
window ← w
α_fast ← fast
α_slow ← slow
timeseries.add(currentValue);
check = window;
n = timeseries.Count;
if n == 1 then
    basePerf = currentValue;
    return annotation(CP);
end
if n ¡ window then
    basePerf = α_slow*currentValue+(1-α_slow)*basePerf;
    currentPerf = basePerf;
    return annotation(currentPerf);
else
    currentPerf = α_fast*currentValue+(1-α_fast)*currentPerf;
    if Abs(currentPerf - basePerf)¿Threshold then
        check=check-1;
        if check==0 then
            check=window;
            return annotation(CP);
        end
    else
        basePerf = α_slow*currentValue+(1-α_slow)*basePerf;
        check = window;
        return annotation(basePerf);
    end
end
return annotation(basePerf);
```

Figure 3-10 The Change Point Correlator Algorithm

According to the expert-defined semantic attribute schema (details in Section 3.4.2.5), the information is extracted by annotating characteristics of data stream and modelled into

corresponding semantic attributes. According to the captured characteristics, there are several types of the real-time annotation process to generate the annotated semantic attribute stream (P) with corresponding time stamps:

- Discrete Annotation: This process is the real-time discrete point annotation (like change point in the data stream), which could be considered as a sequence of semantic meaning points (S) annotated as a semantic attribute stream (P), i.e. $P=\{S_1\ldots,S_m\}$, where $S_i=(s,t)$ is a pair with the semantic meaning (s) at timestamp t.

- Continuous Annotation: This process is used to annotate a piece of data with corresponding meanings, which annotates the data status (S) to data intervals, i.e. $P= \{S_1\ldots,S_m\}$, where $S_i=(s,t_1,t_2)$ is a triple with the data status (s) in a period $(t_1,t_2)$.

The annotated semantic attribute streams are maintained for the further extraction of the meaningful information, which enables another annotation process.

2) Semantic Entity Annotation Process

In the semantic entity annotation process, the semantic attributes describing log entries are linked to higher-level semantic entities like events and behaviours in the domain defined by domain experts. This enables a dynamic picture of the network to be built up from the annotated semantic attribute stream, allowing features such as the network topology status changes to be available in a more meaningful way for the visual representation to non-expert users in real time.

Through these information extraction and annotation patterns, semantically meaningful information is extracted from raw data. According to annotated semantic attributes, all related entities in the domain knowledge model are checked one by one in an event diagnosis loop, in which the information is iteratively annotated with events from low-level to high-level. This checking is based on the rule encoded by a domain expert in the semantic entity schema (details in Section 3.4.3.5). For example, a particular semantic attribute could be considered as a low-level annotation, and if there is another entity whose condition is based on this initial annotation, this can refer to higher-level events, and so events are annotated level by level. All annotated events are kept in an entity pool. In the semantic entity annotation process, the entity pool constantly checks the semantic annotation loop until there are no more new events (and no rules to fire) and at that time, the uplifting of the data in this time interval is finished. The

semantic entities in the entity pool are then maintained for use in other approaches. There are several types of annotation processes for this pattern-driven annotation stream (P):

- High-level Meaning Annotation: This process aims to annotate the high-level event (S) onto the low-level semantic attribute stream. The high-level semantic meaning (s) with the corresponding low-level semantic meanings ($s_1..,s_n$) are determined according to the expert encoded semantic segments, i.e. $P=\{S_1...,S_m\}$, where $S_i=(s,\{s_1..,s_n\})$.

- Behaviour Annotation: This process annotates the behaviour (b) onto the raw data stream, which is based on semantic segment of behaviour events (S), i.e. $P= \{S_1...,S_m\}$, where $Si=(b,t_1,t_2)$ is a triple with the behavior (b) happened in a period (t1,t2), and e.g. "Play" is a behavior for an IPTV service. When the IPTV service is playing, the semantic attribute playing is dynamically annotated into the log data flow.

#### *3.4.4.4 Design of Semantic Processing*

The semantic processing approach aims to apply further knowledge-driven aggregation, diagnosis and analysis on uplifted information either in response to user interactions with the visual widgets or for deeper semantic analysis for example to determine the root-cause of events or to support multi-level problem description in an analytic view. All annotated semantic entities are maintained in an entity pool with a semantic structure, which means the entities are linked to each other according to the relationship extracted from the knowledge model and encodings. Figure 3-11 shows an example of semantic entities relevant to a network resource model in the entity pool. The blue link indicates the semantic relationship between two linked entities. This linked structure enables the further semantic reasoning through these entities. Time stamps are associated with entities to enable temporal semantic reasoning during real time diagnosis and analysis.

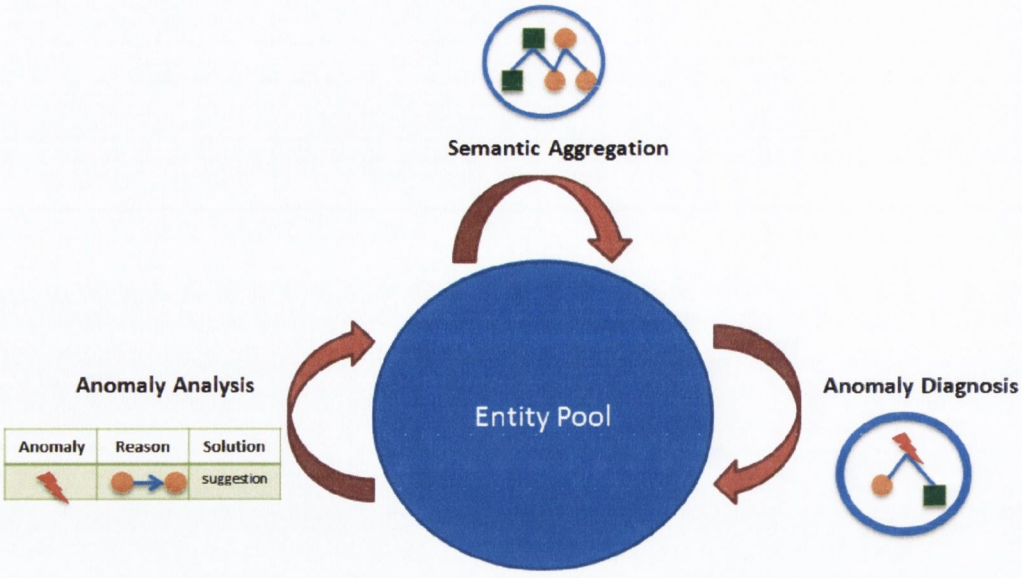



Figure 3-11 The process of Semantic Processing Approach

The semantic processing approach enables drill-down analysis across the monitoring domain to support the higher-level monitoring objectives for non-expert users, which aims to fulfil the design requirement **R1.3**. Semantic entities uplifted and modelled from heterogeneous log data are linked to enable semantic aggregation, anomaly diagnosis and anomaly analysis if required. Thus, this semantic processing approach is executed in three steps:

1) Semantic Aggregation

In the information uplifting approach, the semantic entities are uplifted and modelled based on particular network resources. As further information is uplifted, the semantic aggregation process reviews all the entities extracted from different domains currently in the entity pool to ensure that they include references to appropriate higher-level entities such as network services.

2) Anomaly Diagnosis

The anomaly diagnosis process detects and indicates the anomaly happened among the current uplifted semantic entities. Events that cause network health degradation or that affect the quality of user experience are labelled as an anomaly. The diagnosis process is a knowledge-driven process that relies on the cross-domain knowledge model to enable the semantic reasoning across the semantic entities in different network monitoring domains. This will be further introduced in Section 3.4.3.3.

3) Anomaly Analysis

The anomaly analysis process adopts a drill-down analysis across the knowledge domains to find out the root-cause reason and models the analysis process step by step to support non-expert users in understanding network problems. If an anomaly is detected in the anomaly diagnosis process then a root-cause analysis process is applied to it, e.g. a VoIP quality degradation anomaly is defined as potentially caused by an "AntennaNoise_Bad" status for the source device in the HAN Use Case. The aggregation, diagnosis and analysis result is also semantically modeled to represent what is happening, what will happen, what caused the problem, and the available solutions. The results of the semantic aggregation, diagnosis and analysis are represented in a display-independent schema for consumption by the visual representation. Thus a wide range of widgets can be developed to enable human-centric visual arrangements. The analysis process will be further introduced with the cross-domain knowledge model in Section 3.4.3.3. The visual representation developed so far include network monitoring and troubleshooting tasks is described in the monitoring framework section.

## 3.4.5 The Design of Monitoring Framework

### *3.4.5.1 Design Overview of the Monitoring Framework*

The framework focuses on bridging the gap between an expert and a typical user's view of the network and combining multiple sources of monitoring data to provide useful, dynamic visualizations of network state with specific support for troubleshooting activities. The requirements of this design are addressed:

**Requirement R3**: A framework must be designed to support non-expert users in understanding and monitoring diverse network systems.

- R3.1: A framework must be designed to be compatible with diverse network systems.
- R3.2: A framework must be designed to visually represent high-level monitoring information for non-expert users.

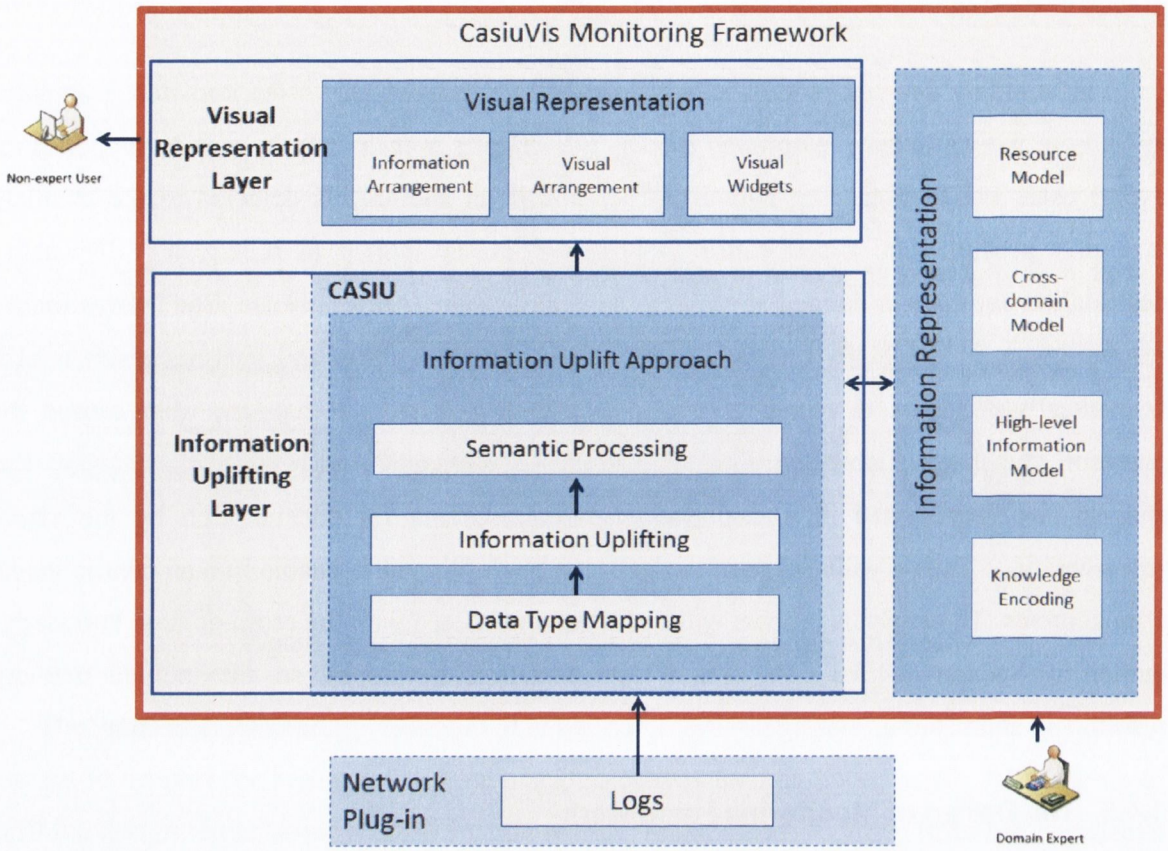



Figure 3-12 Design Overview of Monitoring Framework

In order to achieve these requirements, the monitoring framework is designed with three major components: a semantic uplift engine that consumes raw network monitoring data and transforms it into a common knowledge-based (semantic) model of the specific network, an expert-specified knowledge model of the network domain and a visual representation layer. The visual representation layer allows analysed and aggregated network information to be arranged and visualized via a range of interactive widgets. Each of these is discussed in the sections that follow, along with an introduction to the main technologies employed.

#### *3.4.5.2 Design of the Layered Structure*

1) Information Up-lifting Layer

In the information uplift stage, appropriate network log or event data is identified and annotated with references to the domain expert knowledge model. In a given time interval, the log data of monitored resources in the network is collected and aggregated into pre-defined data

metrics. Although this real-time data is fed into the semantic information uplift process based on highly heterogeneous metrics, the data types of metrics are aggregated and mapped to corresponding data type instances in the knowledge model. Hence related semantic attributes and segments can be applied to the same data type to simplify the annotation process. When processing the real-time data streams, an improved change point algorithm has been applied to detect metric changes that divide the data stream into discrete intervals of moderately varying behaviour and timestamped change points where there are abrupt changes of the steady state metric values. The appropriate semantic attributes are associated with these intervals and points in the raw log streams or metrics. Subsequently in the semantic entity annotation phase, the semantic attributes describing log entries are linked to events and behaviours in the domain expert knowledge model. This enables a dynamic picture of the network to be built up from the event stream, allowing features such as the network topology changes to be available for visualisation in real time.

In the semantic processing, the uplifted information from lower layers undergoes further knowledge-driven aggregation, diagnosis and analysis either in response to user interactions with the visual widgets or for deeper semantic analysis for example to determine the root-cause of events or to support multi-level problem description in an analytic view. All annotated semantic entities are maintained in an entity pool with an RDF triple structure. Semantic entities from heterogeneous resources are linked to raw data log sources, to enable further display, post-processing or analysis of the data if required. Time stamps are associated with entities to enable temporal semantic reasoning during real time diagnosis and analysis. The entity aggregation process reviews all the entities currently in the entity pool to ensure that they include references to appropriate higher-level entities such as network services. Events that cause network health degradation or that affect the quality of user experience, are labelled as an anomaly. If an anomaly is detected then a root-cause analysis process is be applied to it, e.g. a VoIP quality degradation anomaly is defined as potentially caused by an "AntennaNoise_Bad" status for the source device. The results of the semantic aggregation, diagnosis and analysis are represented in a display-independent schema for consumption by the visual representation layer. Thus a wide range of widgets can be developed to enable human-centric visual arrangements. Example widgets developed so far include novice network monitoring and troubleshooting tasks.

2) Visual Representation Layer

In the Visual Representation Layer, several user-friendly widgets are designed for the non-expert users to understand and monitor the network according to the aggregated and up-lifted information through the communication middleware. It is particularly noteworthy that the information received from the semantic processing is independent of any particular visualization widget, so the visualization layer can embed additional expertise-driven logic to select or personalize the most appropriate presentation widget for a given combination of information and user. This process is called information arrangement.

This separation of domain-specific expertise from visualization-specific expertise improves on the current approach of embedding domain reasoning, and associated domain-level assumptions, in the presentation layer. The aggregated and uplifted information from the semantic processing is arranged into the appropriate information model for different visual views. This model depends on the type of widget. This process is considered as the visual arrangement process.

The visual representation layer provides a number of widgets that expose views and manipulators for the semantic model of the network. These widgets aim to support the requirements of non-expert users monitoring and troubleshooting. This allows them to understand, reason about and to make network administration decisions by themselves.

Thus a holistic yet abstracted view of the network must be presented. This simplified view contains visual representations of both physical and virtual network components. It also acts as an entry point to additional information, drill downs into event details and root-cause and solution analysis based on domain expert knowledge. Two major types of views are currently supported: strategic and analytic views and these are described in more detail next. The current prototype also includes a number of other widgets for: playback of raw log data, visualization of service execution rates and so on. There is also a specialized set of widgets for the collection of expert knowledge to populate the domain expert knowledge model.

- Strategic Views

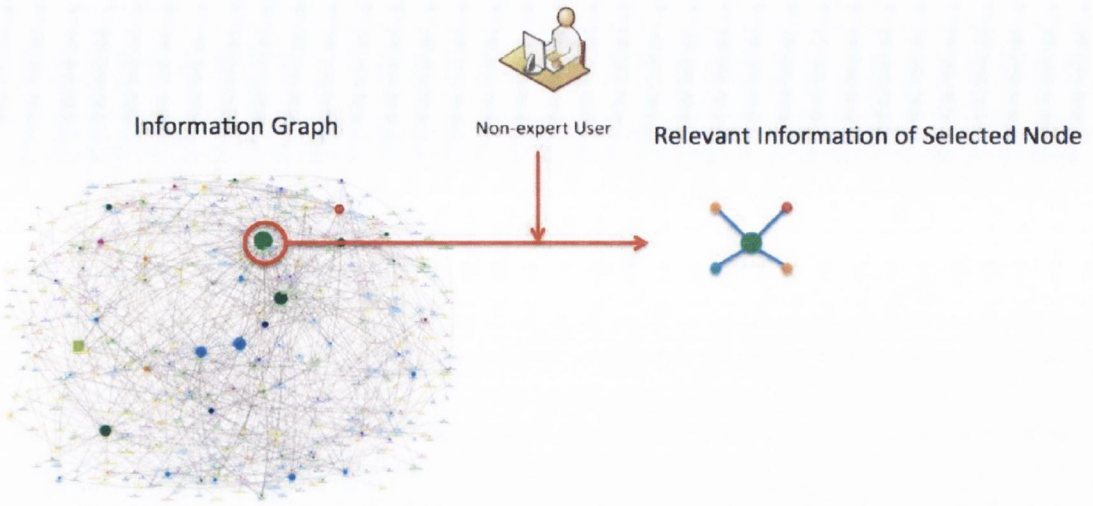



Figure 3-13 Design of Strategic View

The strategic view (Figure 3-13) aims to provide non-expert users with a quick overview of the network. This is to help them understand and monitor the state of their network and its components. This view mainly relies on semantic information harvested by the information uplift process. The device and service information is arranged according to the network topology in a real time display, changing for example as devices join and leave the network.

- Analytic Views

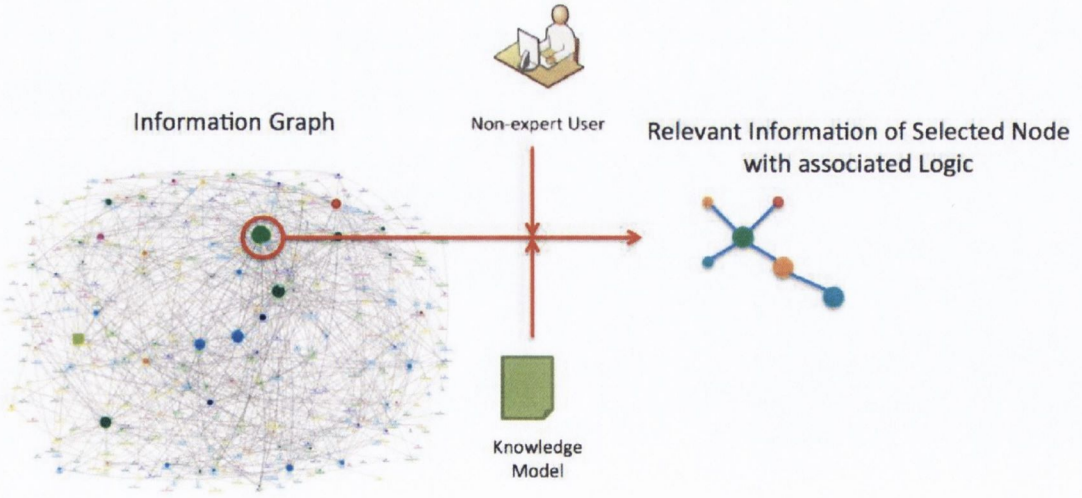



Figure 3-14 Design of Analytic View

In our approach the key to improving network user understanding of network anomalies is to provide accessible root-cause analysis within an appropriate analytic context. The representation of this analysis process requires an analytic view of user-selected information, which is driven by the domain knowledge model. In the CasiuVis framework, event root cause information is aggregated, diagnosed and analysed in the semantic processing. The results of this analysis are then incorporated into the knowledge model of the network and made available to the visual representation layer.

## 3.5 *Conclusion*

This chapter has described a novel approach to leverage domain expert knowledge to support non-expert users in understanding and monitoring network systems. The requirements for this approach are based on an analysis of influences from state of the art and the research question and objectives stated in Chapter 1. This chapter detailed all components to fulfil these requirements. The design detailed in this chapter will be used as a basis for a technical implementation of the information uplift engine called CASIU engine and its visual framework, CasiuVis. The detail of implementation is described in the next chapter.

# Chapter 4
# Implementation

## 4.1 *Introduction*

The previous chapter describes the design of a knowledge-driven information uplift approach with corresponding information representations and framework to support non-expert users in understanding and monitoring network systems. The design is derived from the requirements influenced by the State of Art Chapter, which is also aggregated and stated to fulfil the research question proposed in Chapter 1. By following the design in the previous chapter, this chapter will discuss in detail how these design elements for the information uplift approach, information representations and the monitoring framework have been implemented into network monitoring scenarios to address design requirements, as well as the technical details. The design was implemented into the Information Uplift Engine (CASIU) and the monitoring framework (CasiuVis) with corresponding information representations and visual widgets. This implementation addresses the design in an evolving process, which was implemented into a series of prototypes in two different network monitoring use cases, Home Area Network (HAN) and IPTV delivery network. This chapter then describes a series of iteratively evolved prototypes to support network monitoring for non-expert users. By following the requirements outlined in the Design Chapter, the evolving implementation process makes the theoretical design into a technological reality with the real-world network monitoring use cases and this implementation process is also evaluated in an iterative process which will be described in next chapter. An overview of some of the technologies leveraged in this chapter was addressed in the State of the Art Chapter, e.g. OWL, RDF, SPARQL, and SWRL.

## 4.2 *Evolution of Prototype Implementation*

This research follows an iterative research process (as stated in Section 1.3) process. Focusing on one or several research challenges in the network monitoring scenarios, new/improved components of the design are implemented into each iterative prototype. Followed by well-performed evaluations, each iterative prototype will be examined against initial requirements stated in the Design Chapter (Section 3.3) to fulfill the research challenges. Each of these iterative processes could be considered as an experiment. The evaluation result of each experiment will also provide feedbacks to adjust and improve the initial implementation. During the iterative process, the implementation of the Information Uplift Engine (CASIU) and the monitoring framework (CasiuVis) with corresponding information representations and visual widgets are keeping evolving until they achieve all research objectives.

The design of semantic information uplift approach in Section 3.4.1 is implemented into a serious of iterative evolved prototypes of CASIU (Figure 4-1), which consumes the heterogeneous stream data input, and uplift the high-level information by leveraging domain knowledge input via APIs. According to the review and analysis of information extraction in Section 2.3, CASIU adopts knowledge-driven semantic annotation and reasoning techniques to process the raw data and uplift high-level meaningful information. Focusing on the design requirement (**R1**), the sub-approaches of information uplift approach are embedded into the CASIU structure. The sub-approaches refer to corresponding design requirements in Section 3.4.1.1, which are evolutionally achieved through four experiments as listed in Table 4-1.

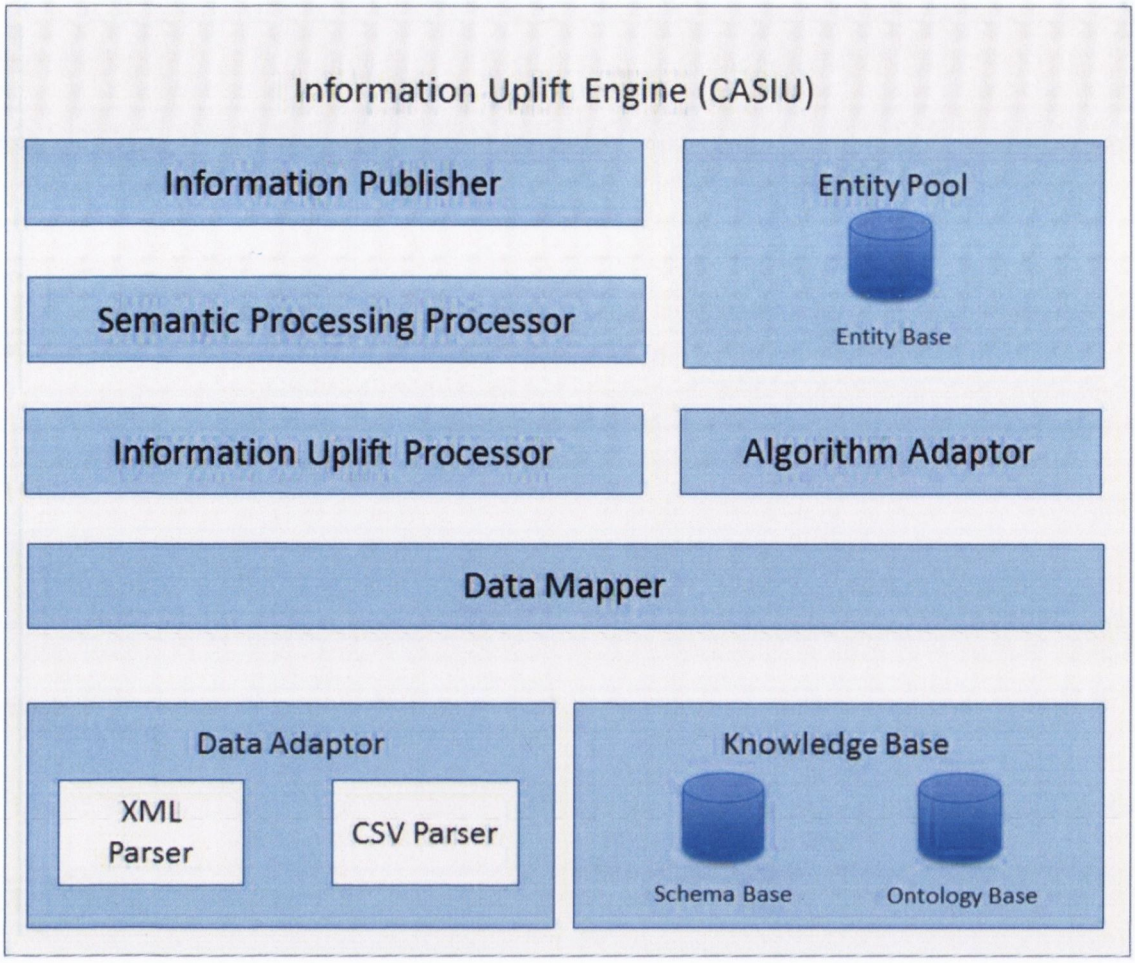



Figure 4-1 Architecture of Information Uplift Engine (CASIU) Implementation

The designs of the information representation in Section 3.4.2 and monitoring framework in Section 3.4.3 are implemented into CasiuVis with evolutional prototypes (Figure 4-1), which contains the Information Uplift Engine (CASIU), expert defined knowledge models, and visual widgets for non-expert users. The CasiuVis framework is designed in a layered structure and its components in each layer refer to different design requirements (as descripted in Figure 4-1). In the implementation process, Semantic Web and Information Visualisation techniques are used to represent information, model the expert knowledge and visualise the uplifted information for non-expert users. The components of the CasiuVis framework are evolutionally achieved through four experiments (**Exp1** to **Exp4**) within two network monitoring use cases as listed in Table 4-1. The summary of the evolutional prototypes are listed below:

Table 4-1 Summary of the Prototype Evolution

| **Research Objectives** | **Design Requirements** | **Prototype Evolution** | | | |
|---|---|---|---|---|---|
| | | **Exp1** | **Exp2** | **Exp3** | **Exp4** |
| Design and implement an information uplift approach **(Objective 3)** | A knowledge-driven approach must be designed to consume heterogeneous real-time data input. **(R1.1)** | Partly Achieved | Fully Achieved | | |
| | A knowledge-driven approach must be designed to extract meaningful information from real-time data input **(R1.2)** | Partly Achieved | Improved | | Fully Achieved |
| | A knowledge-driven approach must be designed to uplift information to support higher-level monitoring objectives **(R1.3)** | Partly Achieved | | Improved | Fully Achieved |
| Design appropriate encodings and models for domain expert knowledge | A comprehensive model for heterogeneous data input resources **(R2.1)** | Partly Achieved | Improved | Fully Achieved | |
| | A comprehensive model for the cross-domain knowledge **(R2.2)** | | Partly Achieved | | Fully Achieved |

| | | | | | |
|---|---|---|---|---|---|
| **(Objective 2)** | A comprehensive model for the high-level information **(R2.3)** | Partly Achieved | Improved | Improved | Fully Achieved |
| | A comprehensive encoding for the domain expert's insights **(R2.4)** | Partly Achieved | | Improved | Fully Achieved |
| Design and implement a monitoring framework **(Objective 4)** | A framework must be designed to be compatible with diverse network systems **(R3.1)** | | Partly Achieved | Fully Achieved | |
| | A framework must be designed to visually represent high-level monitoring information for non-expert users **(R3.2)** | Partly Achieved | | | Fully Achieved |

As summarized in Table 4-1, the research objectives and design requirements are partly achieved, improved and then fully achieved in an evolutional process within four iterative experiments (**Exp1** to **Exp4**). These experiments are implemented based on two inherently related network use cases. **Exp1** and **Exp2** are implemented in a use case to support HAN users to independently understand and monitor their networks. **Exp3** and **Exp4** focus on a use case to support network administrators to simplify the Quality of Experience based IPTV delivery network monitoring. These use cases and technical details of each experiment are introduced in following sections to illustrate how the evolutional implementation process achieves the research objectives and design requirements. And corresponding evaluation of each experiment is discussed in the next chapter.

## 4.3 *USE CASE 1: Home Area Network (HAN) Monitoring*

Advances in both consumer electronics and communications technology have ensured that

the home has become a nexus of networked, multimedia devices and services. These are dynamic, evolving home area networks (HANs) whose complexity can rival that of enterprise networks of the recent past. Nonetheless there is one very important difference – HANs do not typically have trained network operations staff to administer them. Unfortunately as the market for HANs grows, this administration skills deficit increases. The inherent complexity of these networks ensures that monitoring and user intervention plays a vital role in keeping HANs operational. Inexperienced HAN users are considered as non-expert users who are continuously confused and frustrated with even simple HAN performance and maintenance tasks [Yankee Group 1998]. For example, an important VoIP call on an iPad suddenly suffers degradation of wireless connection quality, perhaps caused by some other WiFi activities initiating on the same channel – causing interference, or a signal weakens when the device antenna is obstructed, or another user may be downloading a large file on a PC wired connected to the same home network which causes network congestion. Such events may be unremarkable but will impact on the end-user's perception of the quality of the service supported by the network connection. Additional cost for both the network provider and HAN user will be incurred to detect and diagnose such issues. A significant impediment to recognition, diagnosis and correlation such events for non-expert users is the problem of knowing what is happening, why it is happening and how to solve it in their HANs. However, most existing tools have limited capacity to provide relevant information except through rudimentary but hard-to-understand logging analysis (as analysed in Section 2.5.5). An approach is needed in HAN to best visualise network information to help users reasoning about and understanding the behaviour of their HAN or to aid them in making reconfiguration decisions.

In some ways controlling a HAN presents a traditional service or network management problem. However the HAN environment has a number of special challenges. It is typically administered by non-technical users; it exhibits a great diversity of devices and is highly dynamic with services frequently delivering through it. HAN devices generally lack the advanced management functionality associated with carrier-grade equipment. Even if the HAN devices support some form of dynamic co-ordination mechanism, such as UPnP (Universal Plug and Play), there is often a dependency on both local services and over the top or internet-based services. Thus there is often no single point of management authority and consequently no holistic views of network and service state or capabilities are available. Effective HAN configuration and control by users may be hampered by a poor understanding of the service

requirements or underlying technologies. Any viable approach must somehow bridge between user experience and technical requirements in the presence of highly heterogeneous information sources such as router logs, UPnP events and generic network performance metrics.

Based the analysis for monitoring challenges for non-expert users, the challenges for HAN users are summarized in the following table (Table 4-2):

Table 4-2 Summary of the Monitoring Challenges for HAN Users

| **Challenges for Non-expert Users (C)** | **Challenges for HAN Users** |
|---|---|
| Complete Conceptual Model **(C1)** | *Partly Challenged* (limited diversity of network components) |
| Difficulties for Creating and Updating Information Representations **(C2)** | *Fully Challenged* (lack of domain expertise) |
| High-level Monitoring Information Representation **(C3)** | *Fully Challenged* (lack of domain expertise) |
| Cross-domain Monitoring Information Representation **(C4)** | *Partly Challenged* (limited diversity of monitoring domain) |
| Degree of Autonomy **(C5)** | *Partly Challenged* (lack of management support) |
| Drill-down Analysis **(C6)** | *Fully Challenged* (lack of domain expertise) |
| Visual Representation to Improve Usability **(C7)** | *Fully Challenged* (lack of domain expertise) |
| Visual Representation of High-level Monitoring Information **(C8)** | *Partly Challenged* (small-scale network) |

The lack of the technical knowledge required to digest HAN information is the first major challenge for any effective HAN monitoring system. Given the potential volume of information collected and the likely irrelevance of much of the data to specific tasks such as network trouble-shooting it will be important that any solution to this challenge has the ability to represent the network, services or events at multiple levels of abstraction, thus supporting a drill-down approach to the revelation of detail or to enable focus on specific aspects of a problem or event while de-emphasising others. Ideally such abstractions would be encapsulated in meta-data descriptions that could be combined with the data-streams, enabling dynamic analysis or view generation (specialized, aspect-based visualizations) rather than demanding all views be based on pre-analysed network data.

The second major challenge for effective monitoring of the HAN is the ability to fuse data flows from diverse sources into a single coherent model that supports a number of views based on the activity at hand or perhaps even user preferences or feedback. These elemental information flows are likely to be based on heterogeneous information models and hence require some form of semantic (meaning-based) alignment to allow them to be combined, analysed and presented.

The HAN monitoring scenario meets part of the monitoring challenges for non-expert users discussed in Section 2.5.5. The HAN is normally small in scale and presents limited diversity of network components. The monitoring logs are mostly gathered from the home gateway, which constrains the monitoring can only be approached from limited diversity of network resources and domain knowledge. In addition, the lack of standard support on HAN devices and services also affects the degree of autonomy for monitoring systems. These partly referred challenges will be covered in use case 2.

## 4.4 *The Implementation in HAN Use Case (Exp1 & Exp2)*

### 4.4.1 Overview

In the Home Area Network (HAN) use case, the monitoring challenges require an approach to support non-expert users in understanding and monitoring their HANs. The information uplift approach with corresponding information representations and monitoring framework is designed in the previous chapter to meet proposed monitoring challenges. In this use case, this design was initially implemented into a prototype of CASIU embedded into CasiuVis on a HAN test bed and then followed by an evaluation. The experiment environment, evaluation

details and results will be described in Section 5. The implementation goals in HAN use case follow the addressed research objective and design requirements (as listed in Table 4-1):

- Fully implement a knowledge-driven approach to consume heterogeneous real-time data input. (**R1.1**)
- Implement and improve a knowledge-driven approach to extract meaningful information from real-time data input (**R1.2**)
- Partly implement a knowledge-driven approach to uplift information to support higher-level monitoring objectives (**R1.3**)
- Implement and improve an information model for heterogeneous network resources (**R2.1**)
- Partly implement an information model for the cross-domain knowledge (**R2.2**)
- Implement and improve an information model for the high-level network monitoring information (**R2.3**)
- Partly implement knowledge encodings for the domain expert's insights (**R2.4**)
- Partly implement a framework to be compatible with HANs (**R3.1**)
- Partly implement visual widgets to present high-level monitoring information for non-expert users (**R3.2**)

According to these goals, the implementation in **Exp1** aims to initially investigate the approach in Design Chapter to support non-experts in understanding and monitoring their HAN via a visual interface. In this experiment, the information uplift approach was implemented into a primary version of CASIU to consume the real-time log data from HAN devices and uplift the meaningful information to support higher-level monitoring objectives. The diversity of network resource, uplift and correlation of higher-level meaningful information will be addressed in further experiments. Related information representations were also initially implemented to model the network resources, high-level monitoring information and domain expert's insights. A monitoring framework, CasiuVis, was implemented to embed the CASIU engine with information representations to visually represent meaningful information for non-

expert HAN users. The implementation in **Exp1** will be evaluated and its results contribute to the implementation in **Exp2**, which further developed the information uplift approach and adapted it with more heterogeneous input from different network resources. Information representations were also improved in **Exp2** to model the higher-level semantic meanings and enable the reasoning across domain knowledge models. The CasiuVis monitoring framework was also implemented in **Exp2** to contain the CASIU, information representations and visual widgets to support monitoring tasks in HAN for non-expert users. The implementation with technical details in **Exp1** & **Exp2** will be introduced in following sections.

### 4.4.2 Implementation of CASIU

The knowledge-driven information uplift approach is enforced into an Information Uplift Engine (CASIU), which was partly achieved in this experiment. CASIU takes heterogeneous data input (**R1.1**) from HAN devices and extracts meaningful information from real-time data stream (**R1.2**) to support higher-level monitoring objectives (**R1.3**) for non-expert users. The architecture and its implementation details are described in following sections.

#### *4.4.2.1 Architecture and Technologies Employed*

The implementation architecture of CASIU shows in Figure 4-3 and closely follows the design of information uplift approach outlined in Section 3.4.3. CASIU is implemented as a Java web application that supports the extraction and uplifting of meaningful information and visually represents to non-expert users via Flex-based widgets. This layer (see fig. 4-1) has been developed within FAME as a general-purpose tool for consuming both semantically annotated logs/events and structured domain expert knowledge for semantic event processing (aggregation, anomaly diagnosis and anomaly analysis). The event information is stored internally in an ontology that is periodically updated with network events and inferred knowledge. It builds upon the outputs of the HAN simulator and the semantic uplift engine. It has both an Adobe BlazeDS and XML file-based interface to the visualization layer above it. To date the main focus of our research has been on the information uplift component and as such the semantic processing is currently provided as both an example application of the semantic uplift outputs and to enable us to demonstrate an end to end system in operation. The work undertaken at this approach was focused on the development of a HAN domain model based on the rules and captured domain expert's insights. In addition to this the system had to be tested for HAN network topology and event processing for hand-off to the visual representation layer.

#### 4.4.2.2 Implementation of the Information Uplift Approach

The information up-lift layer could support diverse annotation patterns and processes. In a given time interval, log data of all monitored devices and services in the HAN is collected and aggregated. One of our patterns is applied to detect the change point (CP) of the real time data stream. Our pattern is based on an existing CP detection algorithm (Figure 3-10). With the detected change points, we could divide the data stream into different intervals and discrete points. As shown in Figure 4-2, the linear fitting method is applied to the interval between two CPs. According to the slope and mean of the line segment, we annotate data between two CPs with semantic attributes like "Throughput_sharp_increase", "Throughput_low", and so on.

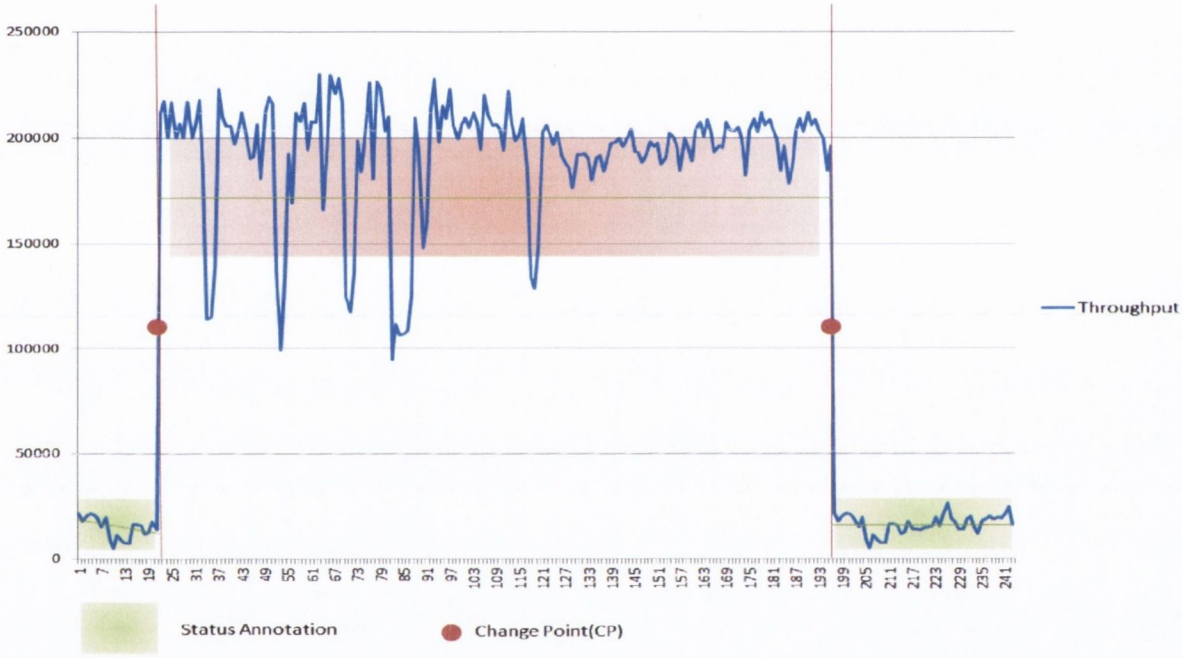



Figure 4-2 The Example of Stream Data Annotation based on CP detection Algoritm

According to the expert-defined semantic attribute schema, the intervals and discrete points are annotated with the corresponding semantic attributes, e.g. "lost_connection", "new_service" and so on. There are several types of annotation process for this semantic annotation pattern(P): The first process is the real-time change point annotation, which could be considered as a sequence of semantic meaning points(S) annotated for a real-time data stream, i.e. P={S1...,Sm}, where Si=(s,t) is a pair with the semantic meaning (s) at timestamp t. The second process is a status annotation, which annotates status events like AntennaNoise_Bad to data intervals, i.e. P= {S1...,Sm}, where Si=(b,t1,t2) is a triple with the data status in a period

(t1,t2). The third process is a high-level semantic meaning annotation. The high-level semantic attribute with the corresponding semantic meaning (s) is determined according to other semantic attributes (s1..,sn), i.e. P={S1...,Sm}, where Si=(s,{s1..,sn}). The last process is the behavior annotation, which is based on behavior events in the raw data, i.e. P= {S1...,Sm}, where Si=(b,t1,t2) is a triple with the behavior (b) happened in a period (t1,t2), and e.g. "Play" is a behavior for an IPTV service. When the IPTV service is playing, the semantic attribute playing is dynamically annotated into the log data flow.

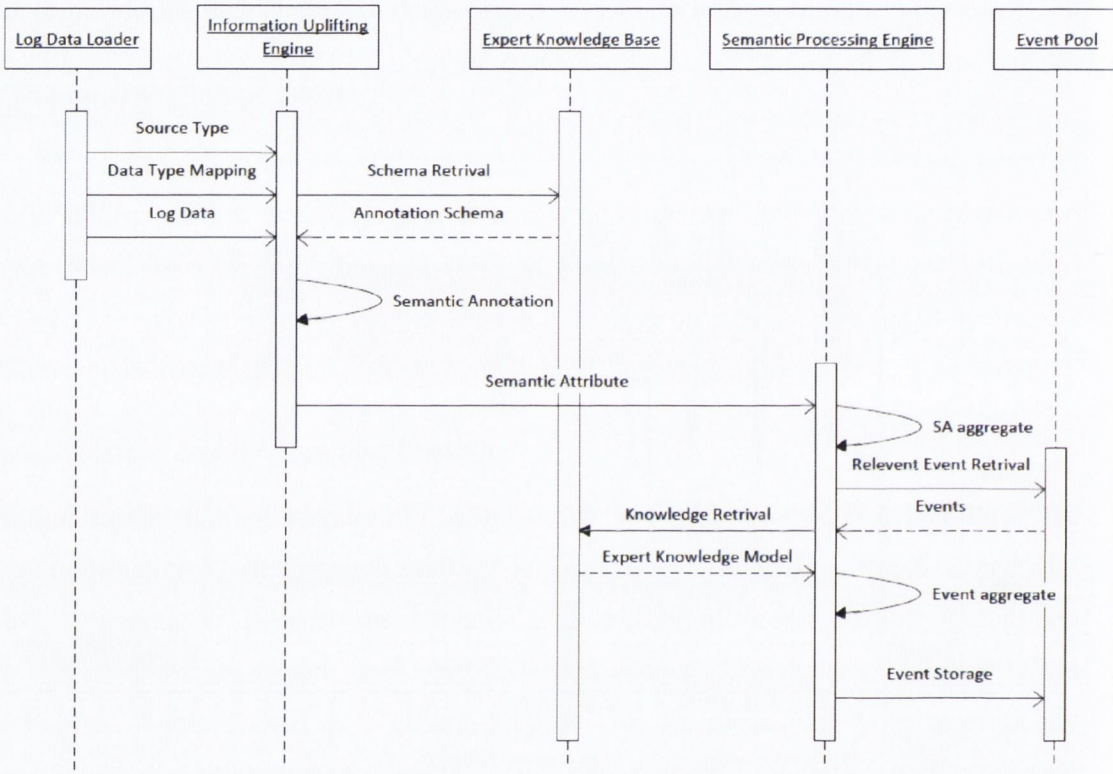



Figure 4-3 The Implementation of Information Uplift Process

Through these semantic annotation patterns and processes, semantically meaningful information is extracted from raw data (Figure 4-3). According to detected data metrics and service type, the information up-lifting engine annotates raw low data with new semantic attributes or existing ones in every time interval. This annotation process is driven by corresponding expert-defined schemas. The annotated semantic attributes are fed into the semantic processing engine. Driven by the domain expert knowledge model, the semantic processing engine aggregates these semantic attributes and refers related events in the event pool to generate new event in a dynamic diagnosis loop, in which the information is iteratively

annotated with events from low-level to high-level. For example, the a particular semantic attribute could be considered as a low-level annotation, and if there is another event whose condition is based on this initial annotation we can refer to higher-level events, and so events are annotated level by level. All annotated events are kept in an event pool. In the up-lifting process, the event pool constantly checks the semantic annotation loop until there are no more new events (and no rules to fire) and at that time, the up-lifting of the data in this time interval is finished. The events in the event pool are then maintained for use in other layers.

Central to a semantic approach is the availability of data in a highly structured form that references a HAN domain knowledge model. In practice most HAN sources produce XML or structured text. Thus the first problem to be addressed is to "uplift" this data into a semantic form (RDF). The HAN information is uplifted, aggregated and processed by our semantic uplift engine. This domain expert knowledge-driven information uplift process is executed in two stages: information uplift and semantic processing.

In the information uplift stage, appropriate HAN log or event data is identified and annotated with references to the domain expert knowledge model. In a given time interval, the log data of monitored devices and services in the HAN is collected and aggregated into pre-defined data metrics. Although this real-time data is fed into the semantic information uplift process based on highly heterogeneous metrics, the data types (e.g. packet_loss_rate) of metrics are aggregated and mapped to corresponding data type instances in the knowledge model. Hence related semantic attributes and segments can be applied to the same data type to simplify the annotation process. When processing the real-time data streams, an improved change point algorithm has been applied to detect metric changes that divide the data stream into discrete intervals of moderately varying behaviour and timestamped change points where there are abrupt changes of the steady state metric values. The appropriate semantic attributes are associated with these intervals and points in the raw log streams or metrics. Subsequently in the semantic entity annotation phase, the semantic attributes describing log entries are linked to events and behaviours in the domain expert knowledge model. This enables a dynamic picture of the HAN to be built up from the event stream, allowing features such as the HAN topology changes to be available for visualisation in real-time.

In the semantic processing, the uplifted information from lower layers undergoes further knowledge-driven aggregation, diagnosis and analysis either in response to user interactions

with the visual widgets or for deeper semantic analysis for example to determine the root-cause of events or to support multi-level problem description in an analytic view. All annotated semantic entities are maintained in an entity pool with an RDF triple structure. Semantic entities from heterogeneous resources are linked to raw data log sources, to enable further display, post-processing or analysis of the data if required. Time stamps are associated with entities to enable temporal semantic reasoning during real time diagnosis and analysis. The entity aggregation process reviews all the entities currently in the entity pool to ensure that they include references to appropriate higher-level entities such as HAN services. Events that cause network health degradation or that affects the quality of user experience are labelled as an anomaly. If an anomaly is detected then a root-cause analysis process is be applied to it, e.g. an IPTV quality degradation anomaly is defined as potentially caused by an "AntennaNoise_Bad" status for the source device. The results of the semantic aggregation, diagnosis and analysis are represented in a display-independent schema for consumption by the visual representation layer. Thus a wide range of widgets can be developed to enable human-centric visual arrangements. Example widgets developed so far include novice HAN monitoring and troubleshooting tasks. These are described in the next section.

### 4.4.3 Implementation of Information Representation

The information representations designed to capture and model the domain knowledge were partly achieved in this use case to support the knowledge-driven information uplift approach. An information model was implemented in **Exp1** and improved in **Exp2** for heterogeneous network resources (**R2.1**), which refer to a partly implementation in **Exp2** of an information model for the cross-domain knowledge **(R2.2)**, and an information model for the high-level network monitoring information was implemented in **E1** and improved in **E2** (**R2.3**) based on knowledge encodings for the domain expert's insights (**R2.4**) captured and modelled in **Exp1**. The implementation details are described in following sections.

#### *4.4.3.1 Technologies Employed*

This section presents a brief overview of the key technologies being used for the information representations in the HAN use case.

- RDF and OWL

The Resource Description Framework (RDF) is the W3C standard for meta-data. It is

centred on making three part entity-attribute-value assertions called "triples" that can be combined into a directed graph-based data, information or knowledge model. The base RDF specification has no inherent typing mechanisms until it is extended with the RDF schema (RDFS) specification. RDF/RDFS are appropriate for flexibly representing data about entities that have a very large range of potential attributes, e.g. if the attributes are unknown, such as the descriptions of devices joining a HAN. The second property of RDF that is especially useful in gathering monitoring information in a HAN is the ability to easily merge data about a single entity from multiple sources.

The Web Ontology Language (OWL) is a set of semantic web representation languages designed to capture ontological concepts, instances of concepts and relationships in a more complex knowledge model than RDF. It comes in a variety of flavours, differentiated by their semantic expressiveness, ranging from lightweight through formally defined description logic semantics – OWL DL, to a very expressive OWL Full. OWL builds extensively on RDF and RDFS, but provides additional vocabulary and semantics to better capture the meaning of concepts, relationships, and instances. OWL ontologies are commonly made available in RDF/XML format. One of the main advantages of OWL's formal semantics over other ontological representation approaches is the ability to run automatic inference engines over the ontology to extract additional semantic statements that were implicit in the ontology and make them directly accessible.

- Semantic Query (SPARQL) and Rule Language (SWRL)

As a part of the W3C standards, there is a formal query and rule language to express the accessibility and logical extension of RDF/OWL. SPARQL (SPARQL Protocol and RDF Query Language) is a protocol and query language for RDF that became an official W3C Recommendation in 2008 [5]. SPARQL is applied in our framework as a native way to access the knowledge repository and performance queries consisting of triple patterns, conjunctions, disjunctions, and optional patterns across diverse knowledge sources, whether the knowledge is stored natively as RDF or viewed as RDF via middleware. Results from SPARQL queries can be expressed as result sets (tabular data) or RDF graphs, which enables the further interaction with other semantic technologies.

SWRL (the Semantic Web Rule Language) was proposed as a standard rule language for the semantic web in 2004. It is based on a combination of a subset of the Web Ontology

Language (OWL) with the Unary/Binary Datalog Rule Markup Language (RuleML). SWRL supports more complex logical reasoning by providing for more flexible semantic logical definitions as part of our knowledge model represented in RDF/OWL. The rules defined in SWRL are in the form of an "if" clause followed by an action clause ("if X then Y"). For example, the condition AnntenaNoise_Bad or SignalStrength_Bad specified in the "if" clause is true, then the condition WirelessConnection_Bad specified in the "then" clause must also hold. This is especially useful for event processing. Another benefit is these semantic query and rule languages are widely supported by semantic tools and APIs.

#### *4.4.3.2 Implementation of Information Representations*

The domain expert knowledge model enables human-centric HAN monitoring within the CasiuVis framework. It acts as a bridge between expert insights, HAN logs and network visualizations for non-experts. Rather than being a single over-arching HAN knowledge model, the domain expert knowledge model is an upper or meta-model that enables the easy integration of multiple domain specific models, for example for individual devices. Crucially it defines a framework for linking human expert insights about these models or systems and system artifacts such as device logs or events. It also allows experts to encode knowledge about system states, behaviors and potential network or service anomalies. This is significant because these upper model concepts can then be used to span multiple device or network models. In the meta-model, the semantic attribute and semantic segment are the two key concepts used to enable efficient processing and combination of domain expert insights based on heterogeneous HAN component models.

Semantic Attributes are used to annotate raw log or event data from the network. They support heterogeneous data collection because a domain expert can define multiple sources of evidence a network condition as equivalent (say evidence of low effective bandwidth via events from multiple services). Once annotated these events can all be treated equivalently by the ontology-level semantic reasoning and hence bridge the gap between raw log data and the formal domain expert knowledge model. Semantic attributes are encoded in Resource Description Framework knowledge models (see later). These encapsulate an expert's subjective insights into the HAN. They consist of a concept definition, a set of constraints and links to both the raw log data or metrics and a specialized knowledge model for the device, network or service. For example, the semantic attribute "antenna_noise_bad" could be defined as occurring when a "high" wifi antenna noise is recoded in a specific type of access point log file, where

"high" is defined by the expert-specified constraint "morethan -80dBM". It also links to the "antenna_noise" concept in a detailed wireless device metrics knowledge model.

Semantic Segments are used in the meta-model to represent a combination of semantic attributes, domain ontology classes and corresponding logic to capture network state transitions, anomaly detection or resolution. This logic goes beyond the typical use of structured knowledge (ontologies) by enabling generic rules or temporal logic to be combined with traditional semantic technologies. This provides a highly abstracted description about logical rules and conditions for semantic entities, which are, for example, automatically decomposed into atomic SWRL rules and SPARQL queries during the semantic processing.

In addition the domain expert knowledge model provides OWL classes to support problem identification, diagnosis and analysis. These are (fig. 2): *Condition*, *Semantic Entity* (*Event*, *Behavior*, and *Anomaly*), *Reason*, and *Solution*. These represent conditions that could be a trigger for another event, behaviour or anomaly. The *Event* class is used to describe the network performance status and sudden changes in state. The *Behavior* class indicates the behavior happened on/between network components, like "data_transferring between a *laptop* and *gateway*". The *Anomaly* class is used to represent events or behaviors that affect the Quality of Experience (QoE) for users. The *Reason* class is used to relate expert-defined reasons to an anomaly of a given type. The *Solution* class is used to describe expert-defined solutions for combinations of reason and anomaly.

The problem identification, diagnosis and analysis classes are associated with either a single or a combination of several Semantic Attributes (and hence raw log or event data).

### 4.4.4 Implementation of CasiuVis

The CasiuVis framework focuses on bridging the gap between an expert and a typical user's view of the network and combining multiple sources of monitoring data to provide useful, dynamic visualizations of network state with specific support for troubleshooting activities (**R 3.2**) implemented in **Exp1** and improved in **Exp2**, which are also implemented in a compatible framework (**R 3.1**) in **Exp2.**

The framework has three major components: a semantic uplift engine (CASIU) that consumes raw network monitoring data and transforms it into a common knowledge-based (semantic) model of the specific HAN, an expert-specified knowledge model of the HAN

domain and a visual representation layer. The visual representation layer allows analaysed and aggregated HAN information to be arranged and visualized via a range of interactive widgets. Each of these is discussed in the sections that follow, along with an introduction to the main technologies employed.

#### *4.4.4.1 Implementation of the Visual Representation Layer*

The visual representation layer provides a number of widgets that expose views and manipulators for the semantic model of the HAN. These widgets aim to support the requirements of novice HAN users monitoring and troubleshooting the HAN. This allows them to understand, reason about and to make network administration decisions by themselves.

Thus a holistic yet abstracted view of the HAN must be presented. This simplified view contains visual representations of both physical and virtual HAN components. It also acts as an entry point to additional context information, drill downs into event details and root-cause and solution analysis based on domain expert knowledge. Two major types of views are currently supported: strategic and analytic views and these are described in more detail next. The current prototype also includes a number of other widgets for: playback of raw log data, visualization of service execution rates and so on. There is also a specialized set of widgets for the collection of expert knowledge to populate the domain expert knowledge model.

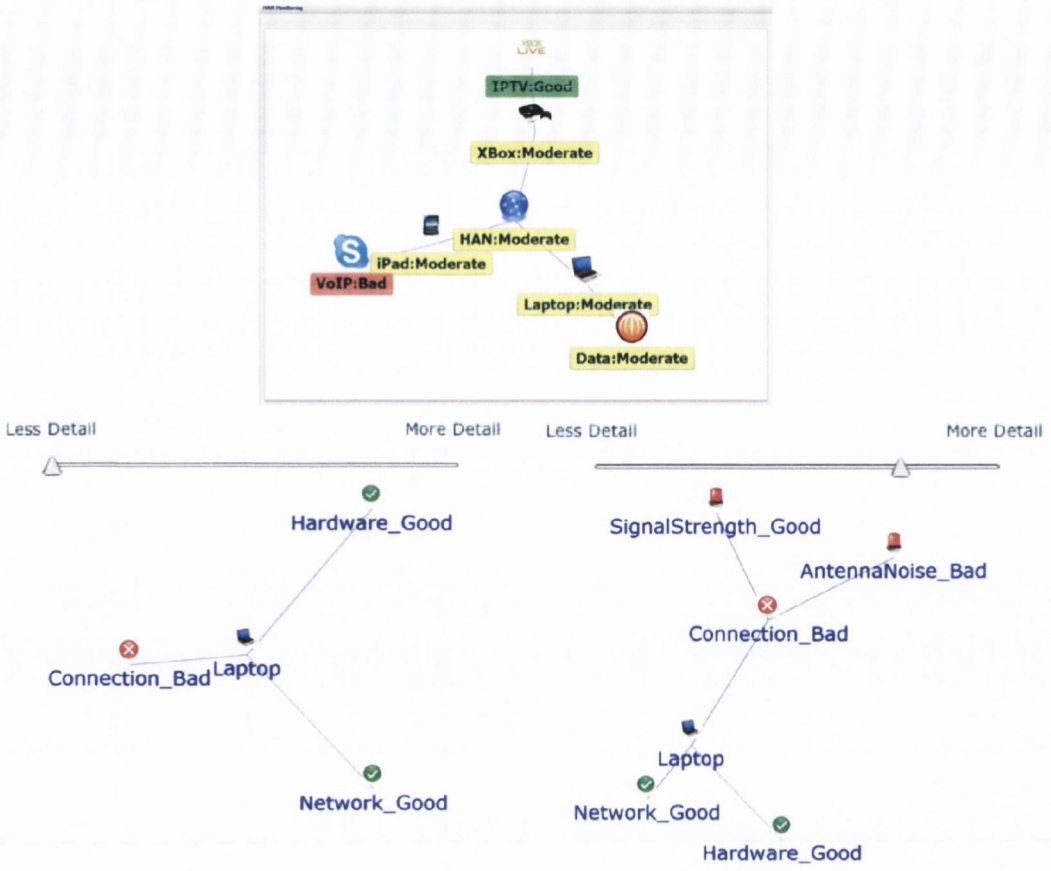



Figure 4-4 Strategic Views: (top) Network Topology Widget (bottom) Layered Description Widget showing slider positions for both less detail (left) and more detail (right)

- Strategic Views

The strategic view (Figure 4-4) aims to provide novice HAN users with a quick overview of the network. This is to help them understand and monitor the state of their HAN and its components. This view mainly relies on semantic information harvested by the information uplift process. The device and service information is arranged according to the HAN topology in a real time display, changing for example as devices join and leave the network.

The network topology widget can be seen in the upper part of figure 4. This widget displays both tangible elements of the HAN like the gateway or services being monitored in the

network and also inferred context between elements such as the relationships between nodes and the current status of each node. Each node model includes underlying links to relevant data metrics, related HAN concepts and domain knowledge. This enables rich, dynamic context to be calculated or displayed for each node. For example a node name label in a green or yellow box indicates normal operation whereas a red label box indicates a problem has been detected for that node. In figure 4 the node with a label in a red box, a Skype VoIP service, has changed color in this way. The node detail widget in the lower part of figure 4-4 is an example of semantic context. It enables the user to view the strategic information associated with a selected node at different levels of abstraction. This widget is triggered when user clicks on any node in the network topology widget. At a low detail level, as shown on the left hand side, only the semantic entities directly linked to the node are exposed. This is a representation of the semantic surroundings of the node within the knowledge model. For other slider settings it is easy to display ever greater degrees of semantic surroundings, eventually showing indirectly related entities with less relevant semantic relationships. This combination of high level overviews with inferred context and clickable drill downs to provide ever greater context has been effective for users.


Figure 4-5 Analytic View: troubleshooting network problems

- Analytic Views

In our approach the key to improving HAN user understanding of network anomalies is to provide accessible root-cause analysis within an appropriate analytic context. In the HuMonVis framework, event root cause information is aggregated, diagnosed and analysed during the semantic processing. The results of this analysis are then incorporated into the knowledge model of the HAN and made available to the visual representation layer.

The anomaly analysis widget is opened by double-clicking on the problem (red) node in the network topology widget; see the top of figure 4-4. It draws upon the expert insights embedded in the knowledge of the HAN to explain what aspect of the Skype VoIP service has an anomaly. It also identifies the likely root cause of this anomaly, while showing a visualization of the inference path it used to come to that conclusion. The objective of this form of display is to provide additional context for the user when troubleshooting network problems.

The graph-charts that describe the inference path semantic concepts and relationships are widely used in semantic visualization systems. In the example shown, the anomaly of the Skype VoIP service is "VoIP_Quality_Low". The "hasAnomaly" relationship between service and anomaly is also stated under the icon, so that users can easily understand the meaning of the node and relations. The next step is to analyze what caused this anomaly through a drill-down path and to display this analysis path step by step. In the analysis path, the anomaly VoIP_Quality_Low is evaluated as "probably_caused_by" the Network_Congestion problem on the network; and then the Network_Congestion problem is "probably_caused_by" the status "Heavy_Upload" on the network. This analysis is based on the knowledge-driven semantic reasoning. The anomaly is referred to a particular reason and the reason is associated with another anomaly, event or behavior. This analysis is iterated until no more matching reasons can be found. Thus it is a drill-down process that decomposes the anomaly into atomic semantic entities. The last step is to identify the root-reason that caused the previous anomaly on Skype, which is the Heavy_Upload status on two other devices in the HAN. Finally, if the root-reason is clicked then the solution widget will pop-up and provide suggested corrective actions for the problems based on the domain knowledge model.

## 4.5 *USE CASE 2: IPTV Delivery Network Monitoring*

The continued success of IP-based TV is now seen as critical for assuring revenues for many traditional network operators. Unfortunately IPTV also presents new challenges for managing content delivery networks, especially when protecting the Quality of Experience (QoE) for customers. Of course IPTV QoE monitoring and management systems must perform the typical tasks of any service management application – for example problem identification, localisation and correlation. Yet the environment in which they perform these tasks has a number of unique technical challenges. Hence new approaches are required.

The relationship between network performance and perceived video quality is complex: it is no longer practicable to monitor the network and treat it as a proxy for service behaviour. Separate QoE and service or network models must be combined in order to maximise the accuracy of any monitoring system. For example, video QoE is a subjective measure based on a wider range of human inputs than simple audio. In fact a leading cause of dissatisfaction with video is either poor audio quality or poor audio synchronisation with the visual content –

without any reference to the quality of the video stream itself. Cross-layer correlation problems must be addressed by any monitoring system.

The IPTV deployment scenario is further complicated by the fact that it is a mass market service which hopes to leverage efficiencies resulting from economies of scale: There are large numbers of subscribers involved. Yet each subscriber has their own view of the QoE that they are receiving (and this must be monitored at least occasionally for effective control). This contrasts strongly with classic Service Level Agreements (SLAs) that are more typically enforced between businesses and in scenarios where the numbers of interconnections is limited.

Another technical hurdle to be crossed is that the deployments of these networks and network elements are in their infancy, and not well understood. A direct consequence is the lack of published best practices and useful strategies for monitoring these networks. Even questions as simple as how best to monitor new nodes such as the IP-DSLAMs (digital subscriber line access multiplexers) used to integrate the last mile of service with the telco's core network can cause confusion for operators.

Fundamentally there is always a trade-off between network performance and cost when it comes to network or service deployment. If IPTV service delivery is to provide new revenues at a reasonable cost then it must be possible to effectively monitor and adapt IPTV service delivery networks based on QoE concerns rather than traditional network layer metrics. This means developing service monitoring solutions that are able to monitor QoE on a per-customer basis, that can flexibly configure and adapt the network, can merge many sources of network and service information and that can reduce OPEX by supporting operators with expert insights captured as part of a flexible knowledge base concerning this dynamic service delivery network type. Our system addresses each of these concerns with novel metrics, an OpenFlow based controller and semantic uplift and visualisation of both network and service information.

Before we discuss our approach to QoE monitoring in IPTV service delivery networks it is useful to briefly describe a typical network. First we must note that IPTV refers to the transport of any video signal and is not limited to broadcast TV, although broadcast TV is our main focus. Other common IPTV services are video on demand, pay per view events, premium channels and network personal video recorders. Thus there is an emphasis on multicast traffic but unicast traffic must also be carried for some services such as network personal video recorders.

The network itself is arranged in a hierarchical fashion with content being stored or transmitted by relatively centralized sources at the Super Head End or the Video on Demand server. These video sources transmit onto a core network at a regional or national level and finally traffic is fed into access and aggregation rings served by DSLAMs (DSL Service Access Multiplexers). Video traffic enters the customer premises through a home router or home gateway device, crosses their home area network and is delivered to a Set-Top Box (STB) that decodes and renders the content for a display device. Video is delivered over IP using the real-time transport protocol (RTP) carrying a MPEG Transport Stream which is used to multiplex and transport the individual channels (composed of audio and video content). Hence the protocol stack used looks like: IP/UDP/RTP/MPEGTS. The dominant video encoding scheme is H.264, also known as MPEG-4 Part 10.

A good way to deliver a consistently high quality service through such a complex, multi-domain network is through a managed infrastructure that is capable of responding to change. Figure 1 also illustrates the customer QoE monitoring and control infrastructure that we describe in this chapter. At the lowest level in the network, all devices are instrumented with network and video service metric monitors. Within the distribution network all core and edge routers are equipped with OpenFlow interfaces to enable customised reporting and fine-grained, off-switch control of packet forwarding in the network. This control takes place at a centralised management function which also interfaces with our semantic information uplift engine. This engine combines log and event data from the network with knowledge models based on expert insights. The semantic processing there enables service anomaly detection, root cause analysis and inference of corrective actions. Finally these sematic models can also be consumed by a set of visual widgets to assist network operations staff monitoring, diagnosing and maintaining the IPTV service delivery network.

Table 4-3 Summary of the Monitoring Challenges for Network Administrators

| **Challenges for Non-expert Users (C)** | **Challenges for Network Administrators** |
|---|---|
| Complete Conceptual Model **(C1)** | *Fully Challenged* (diversity of network components) |
| Difficulties for Creating and Updating Information Representations **(C2)** | *Fully Challenged* (lack of domain expertise) |
| High-level Monitoring Information Representation **(C3)** | *Fully Challenged* (lack of domain expertise) |
| Cross-domain Monitoring Information Representation **(C4)** | *Fully Challenged* (limited diversity of monitoring domain) |
| Degree of Autonomy **(C5)** | *Fully Challenged* (lack of management support) |
| Drill-down Analysis **(C6)** | *Fully Challenged* (lack of domain expertise) |
| Visual Representation to Improve Usability **(C7)** | *Partly Challenged* (lack of domain expertise) |
| Visual Representation of High-level Monitoring Information **(C8)** | *Fully Challenged* (large-scale network) |

Comparing to Use Case 1, the lack of the technical knowledge from different domain is the still first major challenge for effective IPTV monitoring system. Even the network administrators require requires a combination of knowledge about heterogeneous network infrastructures, topology of delivery network, and quality of IPTV service to enable a QoE-based monitoring. Given the potential large volume of information collected and the likely irrelevance of much of the data to specific tasks such as network trouble-shooting it will be

important that any solution to this challenge has the ability to represent the network, services or events at multiple levels of abstraction, thus supporting a drill-down approach to the revelation of detail or to enable focus on specific aspects of a problem or event while de-emphasising others. Ideally such abstractions would be encapsulated in meta-data descriptions that could be combined with the data-streams, enabling dynamic analysis or view generation (specialized, aspect-based visualizations) rather than demanding all views be based on pre-analysed network data.

The second major challenge for effective monitoring in IPTV delivery network is the ability to present the over-load information from large-scale network into a single coherent model that supports a number of views based on the activity at hand or perhaps even user preferences or feedback. These elemental information flows are likely to be based on heterogeneous information models and hence require some form of semantic (meaning-based) alignment to allow them to be combined, analysed and presented.

The IPTV monitoring scenario meets part of the monitoring challenges for non-expert users discussed in Section 2.4. The IPTV network is large in scale and presents diversity of network components. The monitoring logs are gathered from different network resource, which are normally delivered in a variety of formats and require knowledge from different domain. In addition, the complexity and diversity nature of IPTV delivery network also affects the degree of autonomy for monitoring systems. These partly referred challenges will be covered in use case 2.

## 4.6 *The Implementation in IPTV Network Use Case (Exp3 & Exp4)*

In the IPTV delivery network use case, the monitoring challenges require an approach to support network administrators in understanding and monitoring their networks. The information uplift approach with corresponding information representations and monitoring framework is designed in the previous chapter to meet proposed monitoring challenges. In this use case, this design was initially implemented into a prototype of CASIU embedded into CasiuVis on an IPTV delivery network test bed and then followed by an evaluation. The experiment environment, evaluation details and results will be described in Chapter 5. The implementation goals in the IPTV delivery network use case follow the addressed research

objective and design requirements (as listed in Table 4-1):

- Fully implement a knowledge-driven approach to consume heterogeneous real-time data input. (**R1.1**)
- Fully implement a knowledge-driven approach to extract meaningful information from real-time data input (**R1.2**)
- Fully implement a knowledge-driven approach to uplift information to support higher-level monitoring objectives (**R1.3**)
- Fully implement a comprehensive information model for heterogeneous network resources (**R2.1**)
- Fully implement a comprehensive information model for the cross-domain knowledge (**R2.2**)
- Fully implement a comprehensive information model for the high-level network monitoring information (**R2.3**)
- Fully implement comprehensive knowledge encodings for the domain expert's insights (**R2.4**)
- Fully implement a framework to be compatible with different network systems (**R3.1**)
- Fully implement visual widgets to present high-level monitoring information for non-expert users (**R3.2**)

According to these goals, the implementation in **Exp3** aims to initially investigate the approach in Design Chapter to support non-experts in understanding and monitoring their IPTV delivery network via a visual interface. In this experiment, the information uplift approach was implemented into a primary version of CASIU to consume the real-time log data from IPTV delivery network devices and uplift the meaningful information to support higher-level monitoring objectives. The diversity of network resource, uplift and correlation of higher-level meaningful information will be addressed in further experiments. Related information representations were also initially implemented to model the network resources, high-level monitoring information and domain expert's insights. A monitoring framework, CasiuVis, was

implemented to embed the CASIU engine with information representations to visually represent meaningful information for non-expert users. The implementation in **Exp3** will be evaluated and its results contribute to the implementation in **Exp4**, which further developed the information uplift approach and adapted it with more heterogeneous input from different network resources. Information representations were also improved in **Exp4** to model the higher-level semantic meanings and enable the reasoning across domain knowledge models. The CasiuVis monitoring framework was also implemented in **Exp4** to contain the CASIU, information representations and visual widgets to support monitoring tasks in IPTV delivery network for non-expert users. The implementation with technical details in **Exp3** & **Exp4** will be introduced in following sections.

## 4.7 *IPTV QoE Management Architecture*

In this section we present our architecture for advanced quality of experience management in IPTV service delivery networks. A schematic diagram of the architecture is presented in figure 2. This shows the major components and illustrates the layered nature of our design where added value and adaptivity is provided at multiple levels. This fits with our experience of real-world systems where there is a trade-off between the sophistication or flexibility of controls and the likely reaction time of those controls. For example experienced human operators provide the most flexible control mechanism but are unable to react to network events in real time. This has led us to enable controls at different time-scales and proximities to the network:

- Algorithmic: Fastest, least flexible.
- Rule-based: leverages expert insights in a modular way that adapts to new knowledge as well as current network state.
- Operator-based: most flexible but slowest.

Our architecture may be split into 3 major contributions: new video metrics, an openflow-based network controller and semantic log uplift, analysis and visualisation. These correspond to the layers in our network architecture. The new video quality metrics are focused on detecting QoE degradation events and are computationally efficient enough to be calculated within the network. The OpenFlow-based network controller enables dynamic control of the network and flexible monitoring based on custom metric collection to enable algorithmic

network adaption mechanisms. The semantic uplift, aggregation and processing of network events combined with domain knowledge models and expert insights allows us to analyse logs and support administrators. We extend this with semantic visualisation of IPTV service delivery network state and customer QoE measures. This means that the visual interfaces are dynamically generated from self-describing data, leading to rich and flexible interfaces.

The sub-sections below discuss these contributions in more detail.

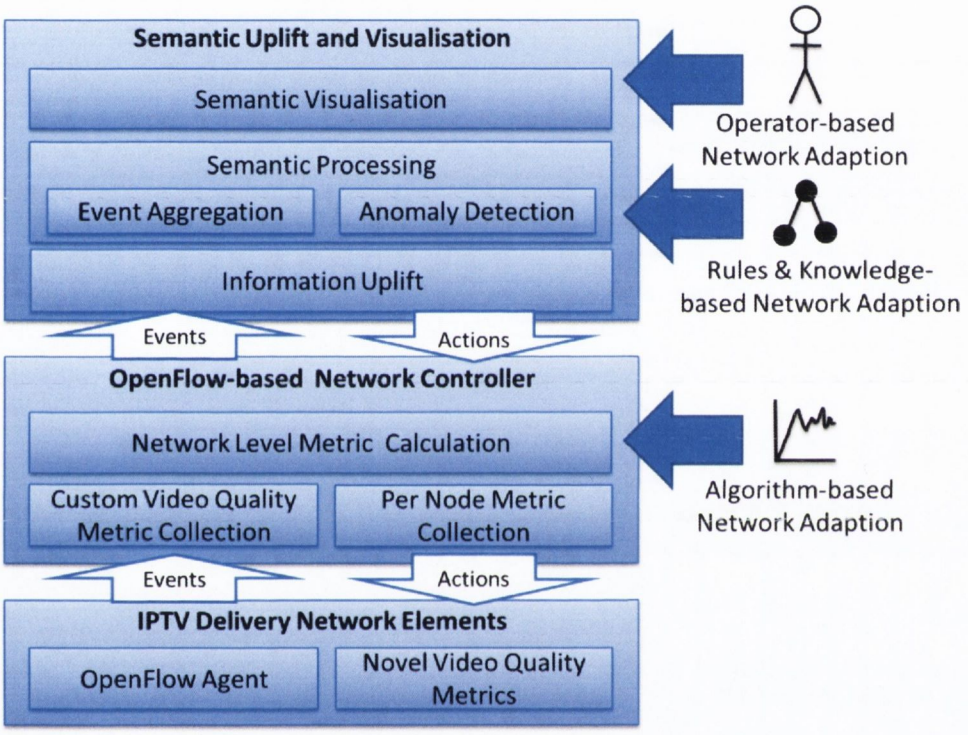



Figure 4-6 The IPTV Service Delivery Network Quality of Experience Monitoring Architecture

### 4.7.1 Requirements for Advanced Video Quality of Experience Metrics

As IPTV traffic traverses the network, it may become interspersed with other IP-based traffic such as voice and data. Hence the first problem when calculating IPTV QoS is often to isolate the IPTV traffic. To localise IPTV QoS failures, a network operator needs a method to evaluate the condition of IPTV traffic at each network node responsible for delivering IPTV to the user. Once a mechanism for evaluating QoS is in place, the network operator requires inference techniques in order to be able to locate and identify the problem in order to remedy

the situation with minimal delay.

Ascertaining an exact understanding of a customer's QoE may only be achieved by interaction with the user, an undertaking whose feasibility is typically constrained by resources and expense. However, if we assume that the non-QoS metrics have been satisfied by the service, it is reasonable to hypothesize that the only factor affecting QoE are fluctuations in QoS parameters. Thus video quality metrics are of vital importance in determining QoE events. However most effective video quality metrics at the current time are full reference metrics, requiring access to uncompressed video streams for their calculation. These full reference metrics are unsuitable for deployment in the service delivery network due to the storage requirements they would impose. Any new metric must also be more computationally efficient, making it suitable for calculation in real time. Hence metrics that can process an individual video stream in isolation in order to detect QoE events have been developed.

## 4.8 *Implementation of CASIUv2*

### 4.8.1 Semantic Processing

This layer has been developed as a general-purpose tool for consuming both semantically annotated logs/events and structured domain expert knowledge for semantic event processing (aggregation, anomaly diagnosis and anomaly analysis). The event information is stored internally in an ontology that is periodically updated with network events and inferred knowledge. It builds upon the outputs of the IPTV network simulator and the semantic uplift engine. It has both an Adobe BlazeDS and XML file-based interface to the visualization layer above it.

To date the main focus of our research has been on the semantic uplift component and as such the semantic processing is currently provided as both an example application of the semantic uplift outputs and to enable us to demonstrate an end to end system in operation.

The work undertaken at this layer for this deliverable of the FAME-IBM Tivoli workplan was focused on the development of an IPTV QoE domain model based on the rules and expert knowledge specified in Section 5.4.3. In addition to this the system had to be tested for IPTV network topology and event processing for hand-off to the visual representation layer.

### 4.8.2 Event Processing

The main work of the semantic processing is to implement the event loop illustrated in figure 4-7. This takes incoming semantic events, from diverse nodes of the IPTV network and using domain knowledge and rules fits them into a model of the IPTV network domain. The first steps in this process are loading domain knowledge and event inspection. The events generated in the semantic up-lift engine are highly heterogeneous, structured and appear in real time. They are "heterogeneous" in the sense that they come from different resources and potentially different annotation patterns and processes. "Structured" indicates all these events are maintained in a formal and explicit structure based on RDF, which exposes the source, time stamp and even some relationship to the domain model and hence between different events. These events are processed in real-time to support online anomaly diagnosis.

Semantic reasoning based on the Jena reasoner is then used to classify the events, establish relationships to other events (temporal, common network-elements or services and even casual relationships) and if necessary create any derived events such as "high level" or more abstract events related to the network event detected in the logs. At this point the local ontology reflects the current state of knowledge of the network.

Then a problem identification process is started. We break this down into two stages – anomaly diagnosis and anomaly analysis. Driven by the domain knowledge model, the event aggregation engine reviews all the events in the event pool to evaluate the health and status of all devices and services in the network and to detect existing and potential problems. If some problems lead to the health degradation of devices, networks or services, we consider that this kind of problem is an anomaly. Once the anomaly is detected, a root cause analysis process (see below) will be applied to this anomaly.

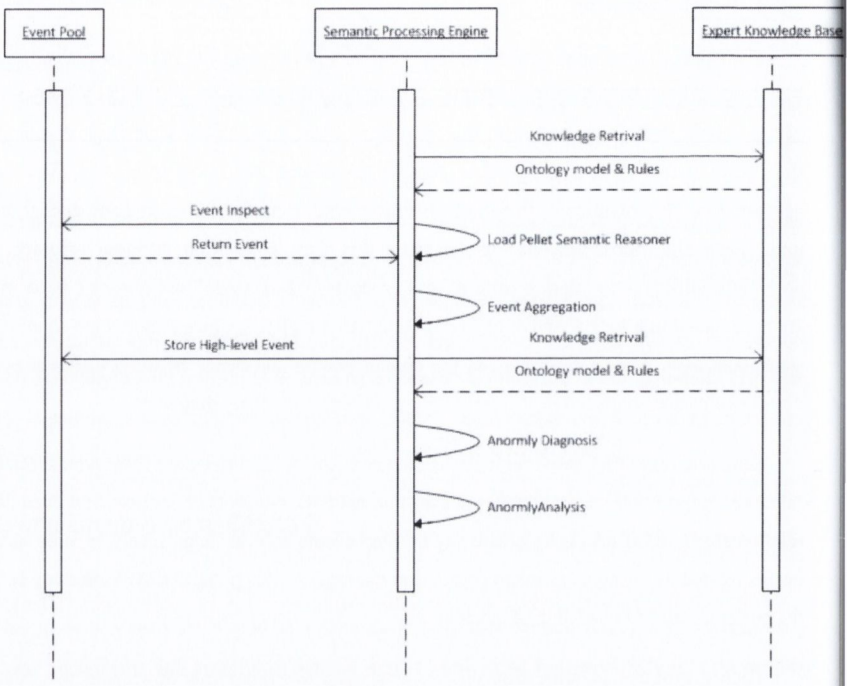



Figure 4-7 Event Processing Loop

### 4.8.3 Anomaly/Root Cause Analysis

This procedure is based on the application of the high level rules for QoE monitoring an IPTV environment described in Deliverable 3. These are implemented as a combination of SWRL rules and structured domain knowledge in the IPTV domain model. An example rule for inferring the root cause of "Bad QoE" being detected at a particular gateway node (gateway66) in the network:

if gateway66 hasEvent iptv_interface_plr_low, then trigger event QoE_bad

QoE_bad is an instance of QoE_event class. iptv_interface_plr_low is an event on gateway66(an instance of Gateway class) Current IPTV service go through gateway66.

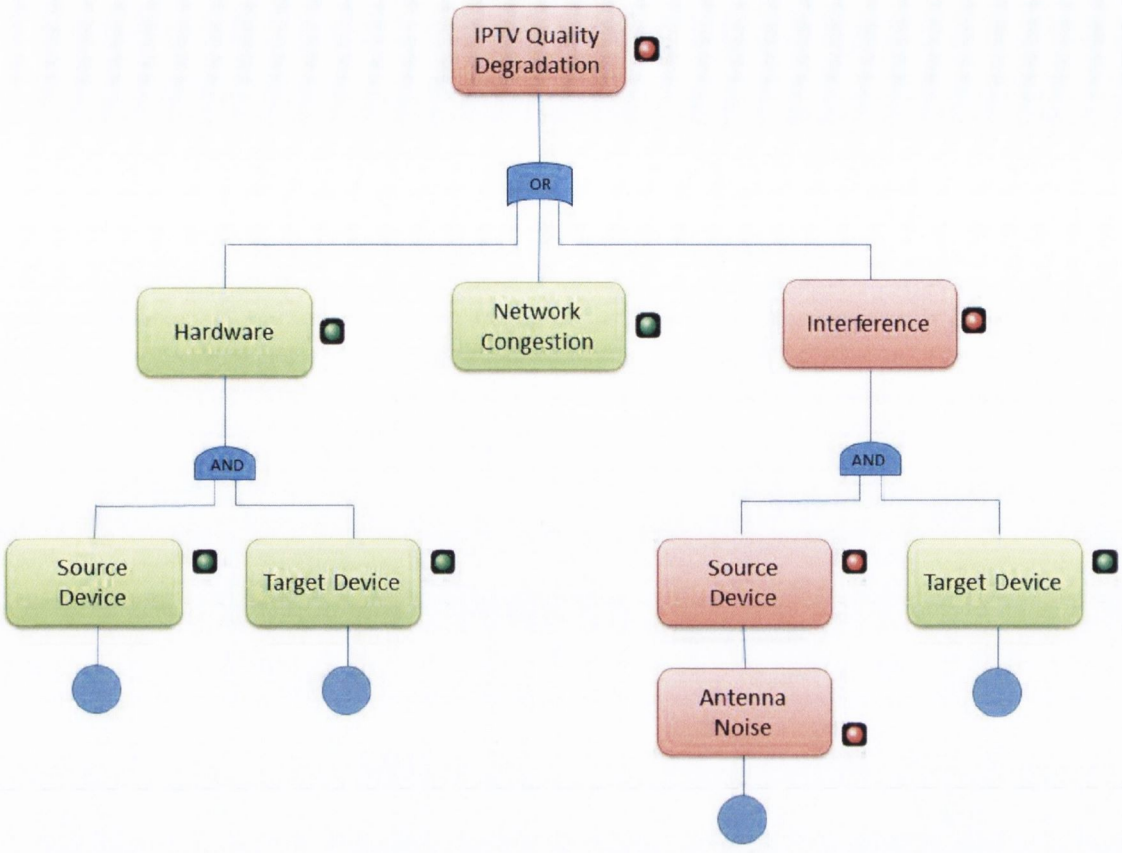



Figure 4-8 Anomaly/Root Cause Analysis in IPTV Network Use Case

The events generated in the information uplifting phase are highly distributed, structured and in real time. This process supports events from heterogeneous resources and different annotation patterns and processes. All these events are maintained in a formal and explicit structure (RDF triple), which exposes the source, time stamp and even the relationship between different events. These events are also highly dynamic to support real time anomaly diagnosis. These RDF triples could generate a tree structure based on domain knowledge encodings. Driven by the domain knowledge model, the event aggregation engine reviews all the events in the event pool to evaluate the health and status of all devices and services in the network and detect existing and potential problems. If some problems lead to the health degradation of user experience, we consider that this kind of problem is anomaly. Once the anomaly is detected, a root cause analysis process will be applied on this anomaly. In Figure 4-8, an IPTV quality degradation problem is referred to be caused by the AntennaNoise_Bad of source device. The aggregation, diagnosis and analysis result is also represented in the visual user interface , which

allows non-expert users to explore what is happening, what will happen, what caused the problem, and the available solutions.

## 4.9 *Implementation of Information Representation*

The domain knowledge model is a basic component in our approach. It acts as a combination of expert insights and domain ontologies for high-level semantic information uplift and the cross-domain root-cause analysis for network anomalies.

Domain experts are typically only familiar with a sub-set of consumer network domain and their knowledge is captured with respect to specialized and discrete sub-network models. Due to the formal structure of Web Ontology Language (OWL), these sub-knowledge models have the capability to interact with other models. These sub-knowledge models are correlated by four main ontology classes in the knowledge model (Fig. 4-9). They model the tangible components and contexts in the network and support anomaly identification, diagnosis and analysis. The four ontology classes are: Semantic Entity, Condition, Reason, and Solution. Currently, there are four Semantic Entity classes in the knowledge model: Semantic Attribute, Event, Behaviour and Anomaly. Semantic Attribute is the low level concrete semantic meanings. The Event class is used to describe the network performance status, and changes in appropriate situations e.g. "Antenna_Signal_Bad" or "Disconnection". The Behaviour class indicates the behaviour happening on/between network components e.g. data_transferring between laptop and gateway. The Anomaly class is the event or behaviour that affects the Quality of Experience (QoE). These semantic entity classes are retrieved from different domain ontologies during the uplift process. The Condition class indicates a condition that could be used to trigger an anomaly based on the knowledge from QoE and QoS ontologies. The Reason class indicates the expert-defined reasons that may cause an anomaly of a given type. The Solution class describes expert-defined solutions that could be applied against one particular reason for the anomaly.

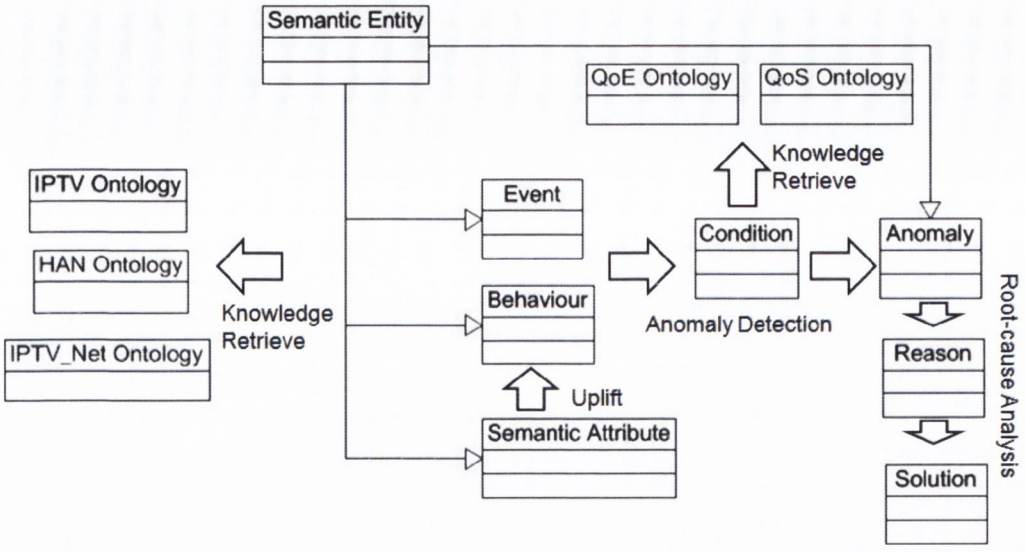



Figure 4-9 A Part of Domain Expert Knowledge Model

The key objective of our knowledge capture approach is to meet the following requirements: (a) enable an ordinary domain expert, that is one without semantic technology background, to encode their insights to the domain; (b) support the encoded insights of an expert to be built on top of multiple types of distributed data; (c) enable interoperability with existing knowledge models; (d) support analysis, reasoning and the composition of higher-level semantic meanings.

Semantic Attributes are the key concept used in this research to enable the efficient processing and combination of domain expert insights. They are discrete units of domain expertise (generated from multiple heterogeneous data sources) that can be combined together and tailored to support non-experts manage a specific domain e.g. consumers wishing to monitor their home network. Furthermore, semantic attributes typically act as abstractions and simplifications from the raw data, which are intended to make the data more understandable for the ordinary, non-expert user.

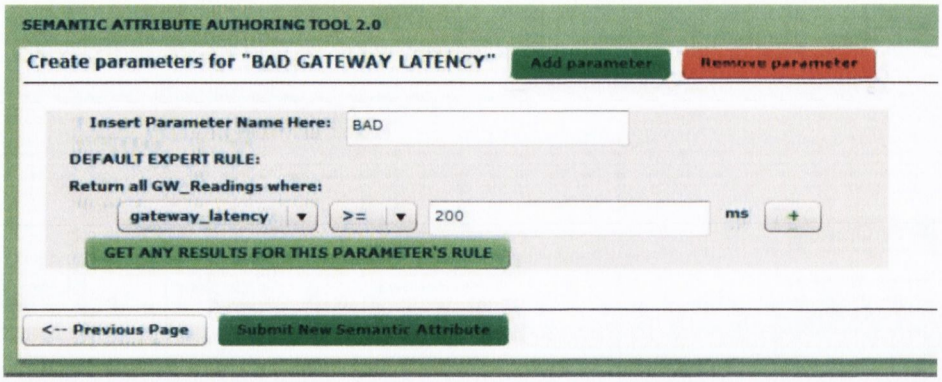



Figure 4-10 SABer: Semantic Attribute Authoring Tool

Semantic attributes are encoded in an XML model and contain domain rules that can be automatically converted into formal semantic rules such as SWRL, in order to enable automatic knowledge reasoning and querying. Importantly, a user-friendly authoring tool called SABer [Hampson et al. 2010] (Fig. 4-10), is used to support knowledge capture from domain experts without necessitating manual semantic encoding by experts. Extending the work of Hampson [Hampson et al. 2010], the semantic attribute concept has been adapted to support the complex, distributed and dynamic nature of IPTV consumer networks and has been refined into three sub-categories: Basic Semantic Attribute, Semantic Segment and Temporal Semantic Attribute. Each are described below.

### 4.9.1 Basic Semantic Attribute

Basic semantic attributes encapsulate the expert's subjective insights of a domain and consist of a:

- A semantically meaningful concept
- Constraints related to the concept
- Parameter/Thresholds specified by experts
- Links to the domain ontology class
- Links to the target element of data metrics

For example, the semantic attribute "GW_latency_bad" describes when a gateway in the HAN knowledge model is in an undesirable condition. This is encoded by the (expert-

specified) threshold constraint ">= 200ms". When this semantic attribute is created in the authoring tool SABer, a new instance "GW_latency_bad" is added to the ontology class "GW_basic_sa" and linked with its model in the HAN knowledge domain. Furthermore, the following constraint that has been encoded in SABer:

<Constraint> GW_latency >= 200 </Constraint>

is automatically converted into the following SWRL rule:

greaterThan([?value, ?threshold])=> addTriple(currentIns, ns:hasSA, ns:GW_latency_bad)

This semantic attribute can only be applied on an instance of "GW_latency". If the 200ms threshold is triggered during the uplift process, a new RDF triple is created to link this semantic attribute to the current gateway instance model.

### 4.9.2 Semantic Segment

Semantic Segments represent definitions of higher-level semantic meanings captured by domain experts, with a combination of semantic attributes, domain ontology classes and corresponding logic.

Specified in the semantic segment schema, a semantic concept "IPTV_QoS_bad" is defined as a semantic segment instance in the IPTV knowledge domain. This semantic segment could be applied on any IPTV_Flow instance. In order to determine this concept, the CASIU engine inspects every IPTV_Flow instance and related semantic entities in the semantic entity pool. It then collects the context of the IPTV flow by checking every node the IPTV flow has passed through. The definition is also associated with a set of constraints:

passVia(?xT, ?xS) && type(?xS, ns:IPTV_Net#VSERVER) && hasSA(?xS, ns: IPTV_Net#VSERVER_plr_bad) => hasSA(?xT, ns: IPTV#IPTV_QoS_bad);

passVia(?xT, ?xD) && type(?xD, ns: HAN#GW) && hasSA(?xD, ns: HAN#DSLAM_plr_bad) => hasSA(?xT, ns: IPTV#IPTV_QoS_bad);

passVia(?xT, ?xP) && type(?xP, ns: IPTV_Net#DSLAM) && hasSA(?xP, ns: IPTV_Net#DSLAM_plr_bad) => hasSA(?xT, ns: IPTV#IPTV_QoS_bad);

In this constraint, if the semantic entity VSERVER_plr_bad is specified on video server, DSLAM_plr_bad is associated with DSLAM, or GW_plr_bad happens on the home gateway, the "IPTV_QoS_bad" could be considered happened on this IPTV flow instance. The constraint is stated in atomic SWRL and SPARQL segments to enable semantic reasoning interoperating over instances and entities from different knowledge domains.

### 4.9.3 Temporal Semantic Attribute

The dynamic and complex nature of current consumer networks requires an effective and flexible real-time knowledge reasoning and processing capability. By extending a current temporal knowledge reasoning approach, our approach focuses on enabling customized and flexible temporal reasoning, based on captured domain expert's insights. For arbitrary two events X and Y, all temporal relationships can be represented with three operators: **DURING** (one event happens within the period of the other event happening), **AFTER** (one event happens after the other), and **WITH** (two events start and end at the same time). Moreover, J. Keeney et al. generalized these operators as: **DURING**, **AFTER (L)**, and **FILTER (OP, L)**. They introduced a time limit L and a filter for comparing any arbitrary attributes, using an arbitrary logical operator with a time limit L. In order to ease the difficulty of encoding and enriching the semantic representation, we allow domain experts to compose with the existing three operators to express the complex insight for semantic entities.

With these three basic operators, experts are able to define more complex and flexible operators for temporal reasoning. In order to balance the cost of the reasoning process and express real world requirements, we introduce a window parameter $w$ as a time limit for tracing back the historical entities in the entity pool. These expert-defined operators are available for logical representation in the definition of basic semantic attributes and semantic segments. The temporal reasoning also has the capability of interpreting heterogeneous domain knowledge by rephrasing the logical representation into SWRL rules.

## 4.10 *Implementation of CasiuVisv2*

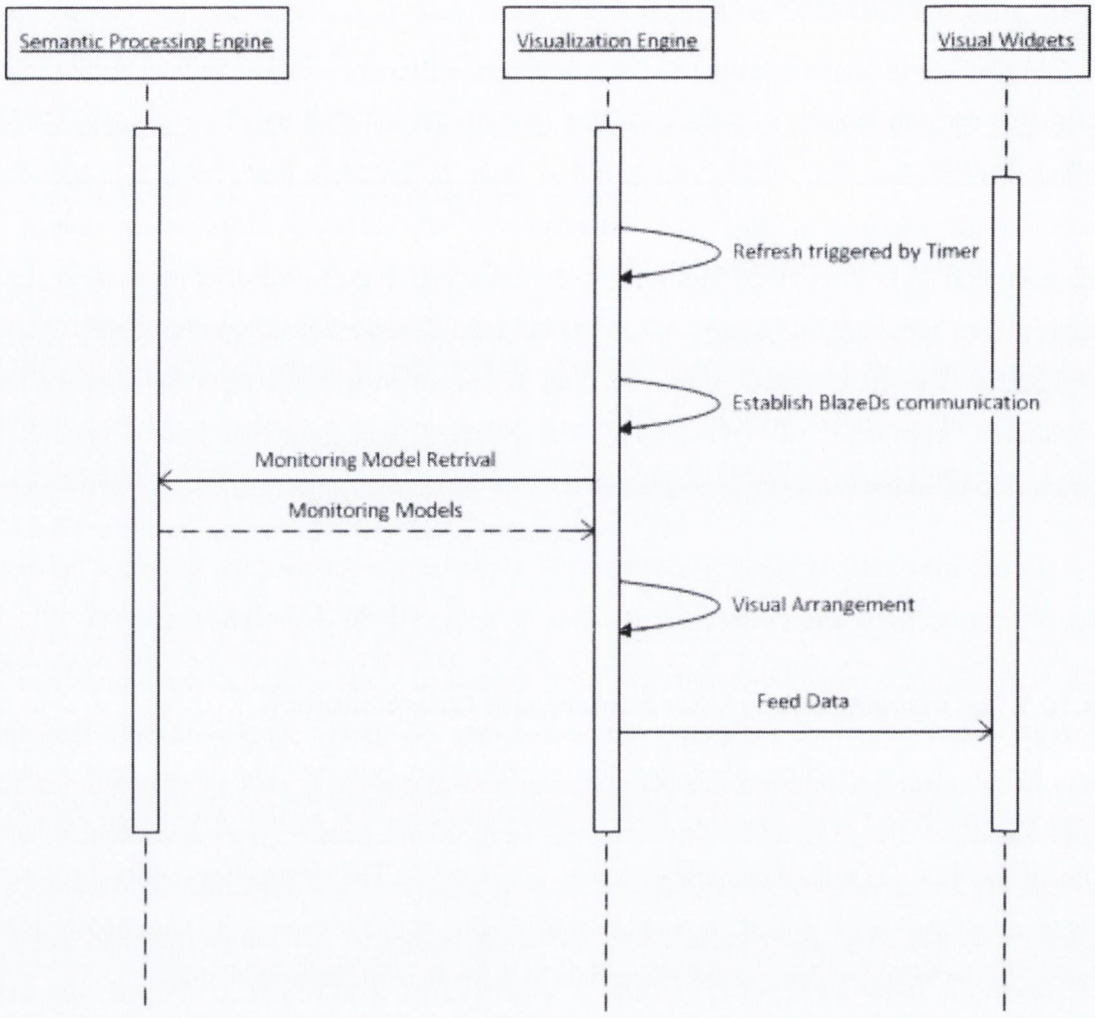
In the Visual Representation Layer, several user-friendly widgets built in Adobe Flex are available for non-experts to understand and monitor the network based on the aggregated, up-lifted, and enriched log information retrieved from the semantic processing. It is important to note that the information retrieved is independent of any particular visualization widget, so the visualization layer can embed additional expertise-driven logic to select or personalize the most appropriate presentation widget for a given combination of information and user. This separation of domain-specific expertise from visualization-specific expertise improves on the traditional approach of embedding domain reasoning, and associated domain-level assumptions, in the presentation layer itself.

In the sub-sections below we discuss the visualization process, the interface between the semantic processing and visual representation layers and the widgets themselves.

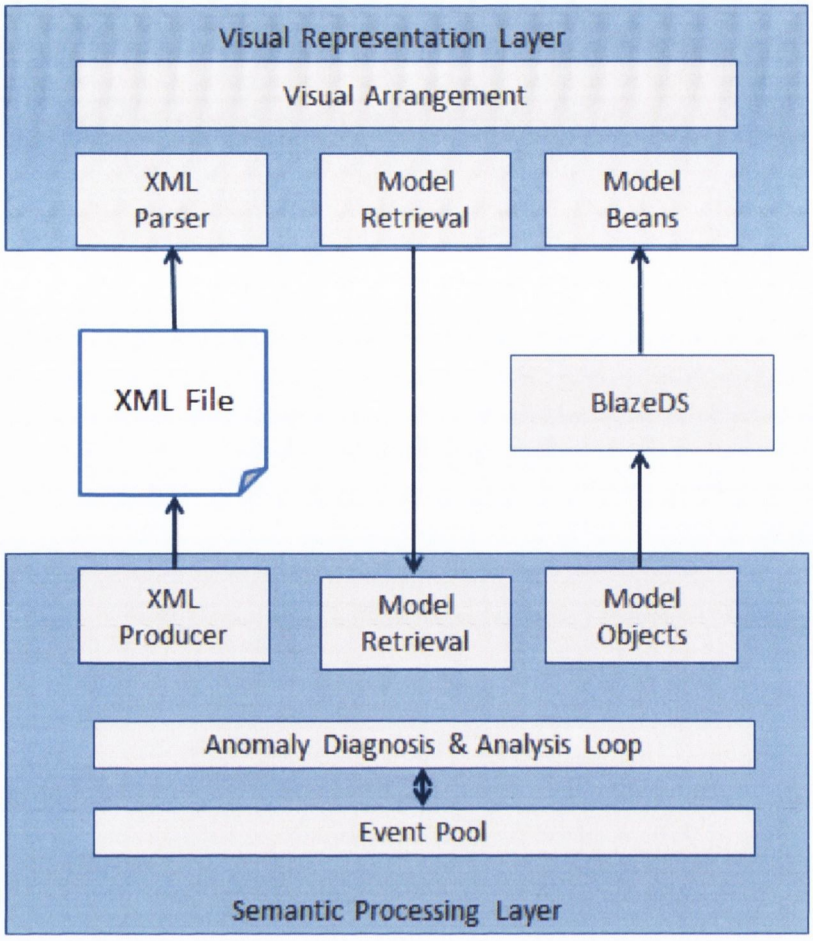
### 4.10.1 The Visualisation Process & Inter Layer Communication

Figure 4-11(a) below illustrates the visualization process, that is the communication between the visual representation layer and the semantic processing. It is based on a polling model (with a default of an update every 2 seconds). The controlling entity in the visual representation layer is called the visualization engine and it manages the communications, the layout of the visual widgets and feeding data to them as it becomes available.

Normally communication is based on the Adobe BlazeDS middleware since this can automatically convert the Jena java representations of the semantic processing ontology into Flex for rendering by the visual widgets. The interface is illustrated in figure 4-11(b).


Semantic Processing Engine
Visualization Engine
Visual Widgets
Refresh triggered by Timer
Establish BlazeDs communication
Monitoring Model Retrival
Monitoring Models
Visual Arrangement
Feed Data

(a)




(b)

Figure 4-11 (a) The Visualisation Process (b) Interface between Semantic Processing and Visual Representation Layers

In addition some of the visual widgets utilize direct access to raw log data, e.g. for log data display, and to facilitate an XML file-based transfer interface is also available. When the visualization engine is linking specific models with widgets it is necessary to use basic JRE calls to load the initial model data before instance data is transferred across the BlazeDS interface.

### 4.10.2 Visual Widgets

Figure 4-12 below shows a screen shot of the system in operation, monitoring the events on a simulated IPTV service delivery network. In the upper right hand corner the network

topology widget can be seen. This widget provides the main overview of the network in operation. It displays the networks, nodes and services being monitored in the network, their relationships and the status of each node. A yellow node name label below a node indicates normal operation whereas a red/pink label indicates a problem has been detected for that node. For example in fig.5 the central node, a DSLAM, has changed colour in this way.

Directly below of the Network Topology widget is the problem analysis and diagnosis widget which draws upon the expert knowledge of the domain embedded in the semantic processing phase to explain what aspect of the DSLAM has an error and identifies the likely root cause of the problem, while showing a visualization of the inference path it used to come to that conclusion. The objective of this form of display is to provide additional context for the user when troubleshooting network problems. As shown in the bottom line of this widget, it is also possible to associate suggested corrective actions with problems in the domain knowledge model. This widget is opened by double-clicking on the problem node in the network topology widget above.

Finally on the left hand side of the screen a more raw form of monitoring widget is shown, the realtime event monitoring widget. This shows simple visual alerts (the orange-brown spots) on a time axis where problems have been detected in the system.

There are also a number of other widgets available for playback of raw log data, for visualization of service execution rates and so on. There is an important set of widgets related to collecting expert knowledge for defining semantic attributes in the system.

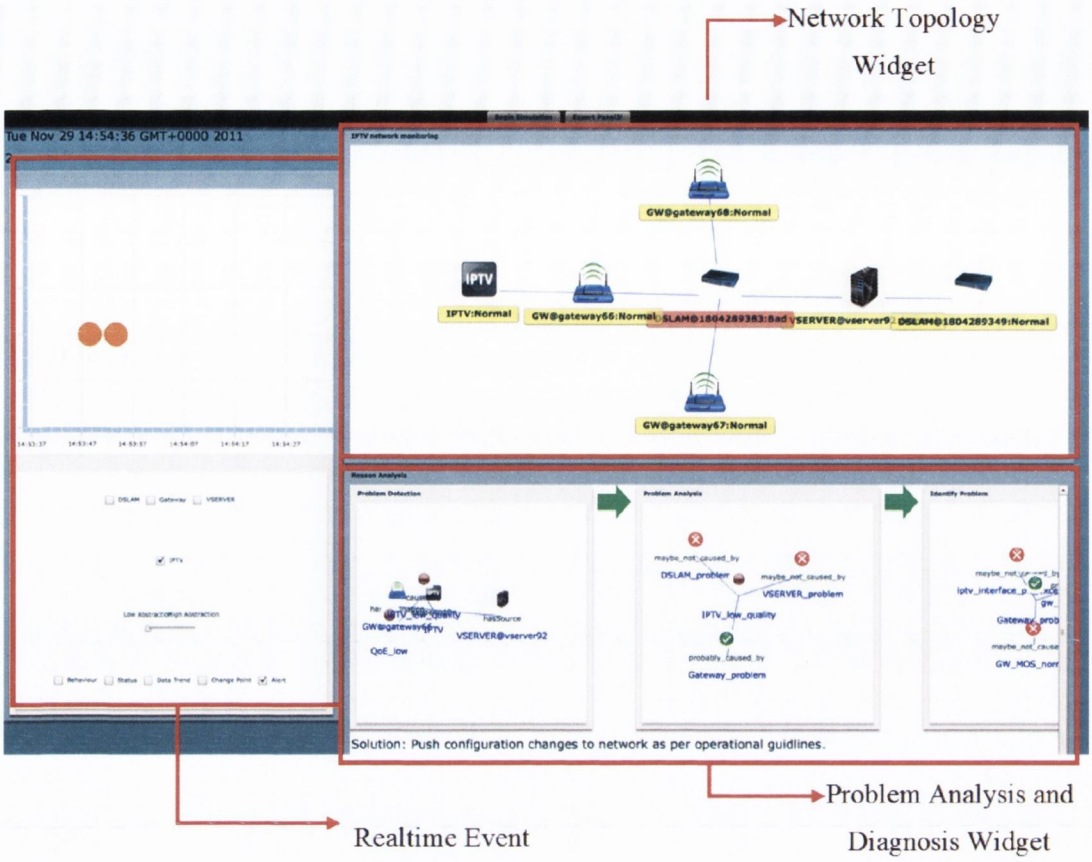



Figure 4-12 The Troubleshooting Visual Widgets

## 4.11 *Conclusion*

This chapter has described how the evolving implementations of CASIU and CasiuVis in two scenarios to support the design of knowledge-driven information uplift approach with information representations and visualization framework. Each of these components and the interfaces and models necessary to support them were described in detail, as well as case studies in the HAN monitoring and IPTV domain that highlighted the features our design offer. The following chapter will detail the different ways that these implementations were evaluated throughout the course of this thesis.

# Chapter 5
# Evaluation

## 5.1 *Introduction and Evaluation Overview*

This chapter describes the overall evaluation to examine how the research performed in previous chapters answered the research question and addressed the limitation and boundary of the research in this thesis. The evaluation is performed in different aspects, including the functionality, feasibility, performance and usability evaluations. This evaluation is incorporated with research objectives derived from the research question in Chapter 1 and validates if the implementation of CASIU and CasiuVis fulfils the design requirements in Chapter 3, which is influenced by remaining challenges in Chapter 2 for supporting non-expert users in understanding and monitoring network systems. The evaluation approach in this chapter is enforced in a series of iterative experiments concluded with an analysis of the evaluation results, a brief comparison with the state of the art, and an overall summary.

## 5.2 *Evaluation Strategy*

The evaluation strategy in this thesis is aiming to validate the requirements of design and answer the research question proposed in Chapter 1. The study for Objective 1 is established as a foundation for the other research carried out in this thesis. In Chapter 2, the surveys of existing network monitoring tools for non-expert users expose the motivation of our research. The review of current information representation and uplift approaches provides this research with a general grounding. It helps the study of what the research challenges of existing approaches are and review what techniques could assist in fulfilling the requirements of network monitoring scenarios. Furthermore during categorizing of related research, similar approaches and tools are compared to indicate the remaining research challenges. The

description about how Objective 2, 3, and 4 were attained in Chapters 3 and 4. The research for Objective 2 aims to design a comprehensive information representation for network information and domain expertise. This research further displays how the captured and modelled domain expertise could drive the information uplift approach to represent the network information in a meaningful way. The research for Objective 3 aims to design and implement an approach to extract the information from raw data and uplift the meaning from low-level to high-level to support network monitoring for non-expert users. For Objective 4, a framework is designed to support network monitoring tasks in different network systems for non-expert users. This design and implementation are in an iterative process distributed in four experiments and needed to be evaluated in separate network scenario with different monitoring task and domain expertise.

This chapter focuses specifically on **Objective 5**, which intends to investigate and answer ***what extent*** this research could support non-expert users in understanding and monitoring network systems. The evaluation is performed in an iterative way to refine, prototype and validate the design from the perspectives of functionality, effectiveness, performance and usability. These evaluations are enforced in a series of experiments. In order to increase the granularity of this evaluation objective, it was necessary to refine them into specific features to ensure the research question is fully addressed. The iterative evaluation experiments described in this chapter are thus used to provide evidence that the following features are being supported:

Table 5-1 Evaluation Goals

<table>
<tr><th>Research Objective</th><th colspan="2">Design Requirement</th><th colspan="3">Evaluation Goal</th></tr>
<tr><td rowspan="3">Objective 2</td><td rowspan="3">R1</td><td>R1.1</td><td rowspan="2">E1</td><td>E1.1 (Functionality)</td><td rowspan="3">FE (Feasibility), PE (Performance)</td></tr>
<tr><td>R1.2</td><td>E1.2 (Functionality)</td></tr>
<tr><td>R1.3</td><td></td><td>E1.3 (Functionality)</td></tr>
<tr><td rowspan="4">Objective 3</td><td rowspan="4">R2</td><td>R2.1</td><td colspan="3" rowspan="4">E2 (Functionality)</td></tr>
<tr><td>R2.2</td></tr>
<tr><td>R2.3</td></tr>
<tr><td>R2.4</td></tr>
<tr><td rowspan="2">Objective 4</td><td rowspan="2">R3</td><td>R3.1</td><td rowspan="2">E3</td><td colspan="2">E3.1 (Functionality)</td></tr>
<tr><td>R3.2</td><td colspan="2">E3.2 (Usability)</td></tr>
</table>

**Evaluation 1 (E1):** CASIU is able to uplift meaningful information from real time data by leveraging the domain expert knowledge.

- **E1.1:** CASIU is able to support heterogeneous real-time data input.
- **E1.2:** CASIU is able to uplift meaningful information from real-time data input.
- **E1.3:** CASIU is able to uplift information to support higher-level monitoring objectives.
- **Feasibility Evaluation (FE):** The processing capability of CASIU should be evaluated and measured to indicate the boundary and factors that could affect or limit the

processing capabilities.

- **Performance Evaluation (PE):** The performance evaluation of CASIU to see under what circumstances it is a usable approach.

**Requirement R1** states CASIU must be designed to uplift meaningful information from real time data by leveraging the domain expert knowledge. It needs an evaluation to validate if the design and implementation of CASIU is able to fulfil **Objective 2**. CASIU is designed to comprehensively model the heterogeneous data input by leveraging domain expert knowledge, which helps to "understand" how to consume the data and what in the data. This requirement is addressed in **E1** with evaluations from functionality, feasibility, and performance perspectives. The nature of network environment determines this uplift process executed in a real time, which requires the CASIU is capable to process the real-time data input. Therefore, the goal of functional evaluation **E1.1** is to validate to what extent CASIU is able to consume heterogeneous real-time data input. CASIU is also designed to fulfil these challenges by extracting meaningful information from the real-time data input (**R1.2**). **E1.2** aims to validate if CASIU is able to extract meaningful information from real-time data input from a functional point of view. As discussed in Chapter 2, the imported expert knowledge is crucial to enable high-level monitoring objectives. Thus, CASIU is designed to leverage domain knowledge to enable information uplifting to support higher-level monitoring objectives (**R1.3**). This requirement focuses on the higher-level monitoring objectives to support non-expert users in understanding the network problem and monitoring the network status, which are the common challenges non-expert users experienced according to the research in Section 2.4. This aims to demonstrate the uplifted high-level information is helpful for non-expert users to achieve the high-level objectives. The goal of evaluation **E1.3** is to validate to what extent CASIU is able to uplift information to support higher-level monitoring objectives. CASIU is designed for real time processing. Therefore, a trade-off exists on the balance of processing time and load. This trade-off needs to be evaluated and measured as a goal of feasibility evaluation (**FE**) to indicate the boundary and factors that could affect or limit the processing capabilities. Finally, as CASIU can cause an extra bottleneck that client applications must pass data through, it is also prudent to evaluate the performance of CASIU in order to help quantify to what extent it increases process latencies. This procedure can be summarised as a performance evaluation (**PE**) to see under what circumstances it is a usable approach.

**Evaluation 2 (E2):** The comprehensive information representation needs to be validated to represent the network information and domain expertise.

This functional evaluation **(E2)** focuses on the representation the domain knowledge to drive the information uplift approach. The representation of the information is the crucial for network monitoring systems. A comprehensive representation is required to ensure the flexibility, autonomy and intelligence of the system, which can also improve the understanding with high-level meaningful information. The evaluation of **E2** is based on the evaluation result from other evaluations, which validate the information representation could support multi-data input, diverse domain expertise, and also enable the information uplift approach.

**Evaluation (E3)**: CasiuVis is able to support non-expert users in understanding and monitoring diverse network systems.

- **E3.1:** CasiuVis is able to be compatible with diverse network systems. .
- **E3.2:** Non-expert users can monitor and understand complex network information by using CasiuVis.

By the influences of state of the art, the information uplift approach requires a comprehensive support to leverage accurate and complete conceptual network information to achieve the monitoring purposes in diverse network environments. Due to this requirement, CasiuVis framework needs to be validated to support the information uplift approach with corresponding information representations to fit into diverse network environments (**E3.1**). As a key finding for non-expert network users, the visual representation of network information is required to improve visibility of network systems, which is still challenged by the usability and representations for high-level monitoring information. From the usability perspective, this evaluation addresses the requirement for the monitoring framework to visually represent high-level monitoring information for non-expert users (**E3.2**).

The evaluation goals will be put into practise in this chapter, and the evaluation findings presented, and the research objectives of this thesis validated. Furthermore, because the implementation of CASIU and CasiuVis closely follow the approach and framework design, their successful evaluation help provide validation of this approach and its associated framework.

## 5.3 *Iterative Experiments*

One of the main aims of this thesis' evaluation approach was to get feedback from the key stakeholders at different stages, so that this information could feed directly back into the design and implementation process. Thus there was a need for initial user-centred feedback and technical measurement of the prototypes, as well as further evaluations on the refined systems. In order to achieve the proposed research objectives, there were four main iterative experiments undertaken in this research and each experiment has its evaluation, which used a number of different evaluation techniques such as structured interviews, questionnaires, performance tests and user trials. The design and implementation of these experiments was discussed in Chapter 3 and 4. This chapter focuses on describing the evaluation goals, evaluation setup and evaluation results of these experiments. The evaluation plan of these experiments is listed below:

Table 5-2 Evaluation Plan for Iterative Experiments

| **Research Objectives** | **Objective 5** | **Iterative Experiments** | | | |
|---|---|---|---|---|---|
| | | **Exp1** | **Exp2** | **Exp3** | **Exp4** |
| Design and implement an information uplift approach (**Objective 3**) | **E1.1** | | Partly Achieved | | Fully Achieved |
| | **E1.2** | Partly Achieved | Improved | | Fully Achieved |
| | **E1.3** | Partly Achieved | | Improved | Fully Achieved |
| | **FE** | | Partly Achieved | | Fully Achieved |
| | **PE** | | Partly Achieved | | Fully Achieved |
| Design appropriate encodings and models for domain expert knowledge **(Objective 2)** | **E2** for Resource Model | Partly Achieved | Improved | Fully Achieved | |
| | **E2** for Cross-domain Model | | Partly Achieved | | Fully Achieved |
| | **E2** for High-level Information Model | Partly Achieved | Improved | Improved | Fully Achieved |
| | **E2** for Knowledge Encoding | Partly Achieved | | Improved | Fully Achieved |

| | | | | | |
|---|---|---|---|---|---|
| Design and implement a monitoring framework **(Objective 4)** | **E3.1** | | Partly Achieved | Fully Achieved | |
| | **E3.2** | Partly Achieved | | | Fully Achieved |

As summarized in Table 5-2, the research objectives and evaluation goals are partly achieved, improved and then fully achieved in an evolutional process within four iterative experiments (**Exp1 to Exp4**). These experiments are implemented based on two inherently related network use cases. **Exp1** and **Exp2** are implemented in a use case to support HAN users to independently understand and monitor their networks. **Exp3** and **Exp4** focus on a use case to support network administrators to simplify the Quality of Experience based IPTV delivery network monitoring. These use cases and technical details of each experiment are introduced in the following sections to illustrate how the evolutional implementation process achieves the research objectives and design requirements with corresponding evaluation of each experiment. An initial experiment was needed to serve two main purposes. Firstly, it was necessary to examine if the design implemented in the prototype, where it acted in different scenarios, was appropriate from a technical perspective. Secondly it was crucial to get some qualitative feedback from end users as to whether CASIU could support them in understanding and monitoring network systems. Hence, this experiment examined whether the features described in Chapter 3 were being supported by CASIU and CasiuVis. Furthermore, by gathering this information early in the development process it meant that user feedback could be quickly implemented into next iterations of the design until the research objectives are fully achieved. The details of each evaluation are introduced in the following sections.

## 5.4 *Test-bed Setup*

The description of two test-beds is introduced in this section, which support the evaluations in this research. The setup of HAN and IPTV delivery network test-bed is collaborated on with other engineers and researchers from IBM Tivoli (Ireland), University College Dublin and Waterford Institute of Technology.

### 5.4.1 Home Area Network (HAN) Test-bed Setup

The setup of the HAN test-bed shown in Figure 5-1 is deployed on a mesh network consisting of Mesh Access Points (MAPs) and Gateways (GWs), these GWs having a high bandwidth wired connection to the Internet. This work is collaborated on with research partners in University College Dublin. In most cases the charging functionality only monitors traffic at the GWs, hence traffic that is internal to the mesh and does not pass through a GW cannot be monitored. As we anticipate increasing hop count in Wireless Mesh Networks (WMN) and increasingly localised services, it is interesting to examine the possibilities of both monitoring such traffic as it may have a significant effect on performance and also to explore the possibility of monitoring for such localised services. This test-bed is to monitor the traffic between nodes at each MAP and report it to the gateway. All the data collected at the GW will be stored in a database for further processing by an agent for obtaining relevant billing information for the Internet Service Providers (ISPs) of the mesh or to evaluate the network performance. The agent will secure the filtering function on all the information stored in the database based on the IP address of the clients and based on the ISPs will be able to monitor its clients accordingly.

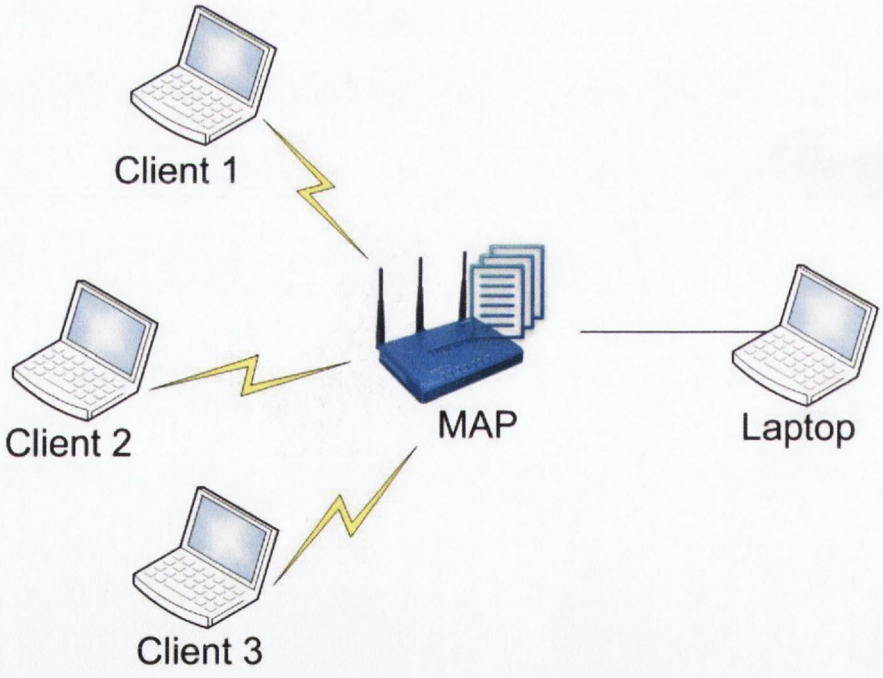



Figure 5-1 The Implementation of HAN Test Bed

To examine the possible impact of localised services and to build the monitoring function at

the core of the HAN system, we have initially used two test cases with a single cell system as shown in Figure 5-1.

The first case assumes the Access Point (AP) and the clients are static and there is video, Voice over Internet Protocol (VoIP) and TCP traffic that flows between the laptop and the three clients connected wirelessly to the AP. The traffic has been simulated using Iperf, a tool to measure the bandwidth performance and the quality of a network link. There has been considered video traffic running from the Laptop to the first client, four VoIP sessions of ten minutes each with the second client and TCP traffic running from the Laptop to the third client. During the tests, exchanged packets have been recorded by the MAP using Tshark [Tshark 2013] and relevant information such as number of bytes exchanged, number of MAC retransmissions, antenna signal, antenna noise values, Signal-to-Noise Ratio (SNR), and through- put have been monitored.

The second case aims to analyse how different parameters of the network change accordingly to the mobility of the clients in the mesh. In this case there is considered only TCP traffic between the Laptop and the three clients. We considered the scenario of the third client moving away from the MAP and then approaching and we analysed the data recorded at the AP using Tshark.

### 5.4.2 IPTV Delivery Network Test-bed Setup

A IPTV delivery network test-bed was set up to support a set of problem scenarios for validating monitoring solution in this research. The establishment of this test-bed was collaborated with other researchers in IBM Tivoli and University College Dublin. This also serves as a problem definition for a candidate IPTV monitoring solution. This test-bed underlines the importance of taking a consolidated approach: semantic reasoning is limited by the quality of the metrics gathered from the network –in turn, the utility of collecting good quality metrics is only maximized when good semantic reasoning is performed. We propose a test topology that specialises the problem to a smaller set of meaningful test scenarios that cover some of the most important aspects of the IPTV monitoring challenge. The IPTV monitoring problem definition is arranged as a series of challenges.

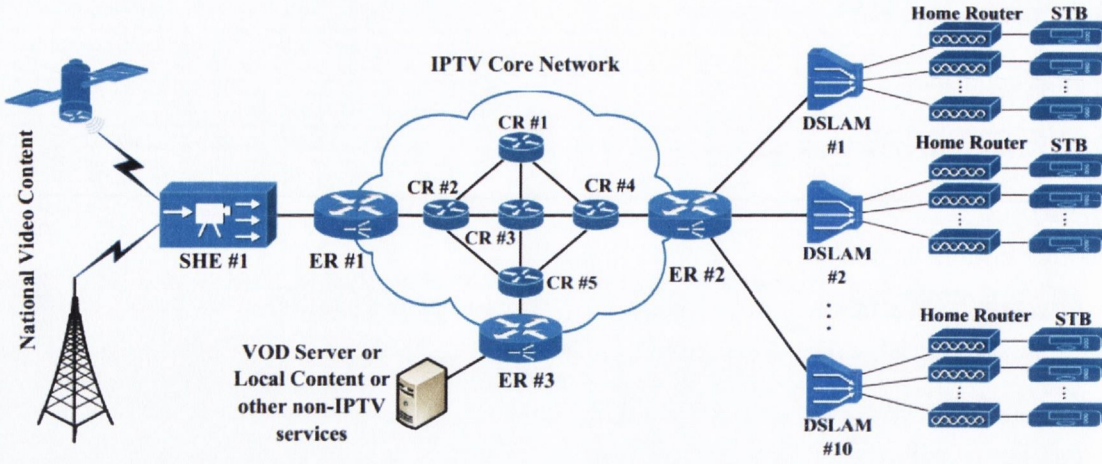



Figure 5-2 The Topology of IPTV Delivery Network Test-bed

The following considerations must be taken into account when planning a test-bed monitoring topology and also when planning what metrics should be collected: the metrics and topology are intrinsically interlinked. The topology should be designed in such a way as to render metrics interesting. The characteristics of a good evaluation topology are defined as follows:

a) Knowledge of outage: The topology should allow for simulation of outages and demonstration that the solution makes the network monitoring cognizant of the problem (the customer will be aware of a problem regardless of whether or not the service provider is aware of it).

b) Timeliness: The topology should allow us to determine the feasibility of gathering monitoring data from an arbitrary network topology in a timely manner. Two modes of monitoring may be evaluated: monitoring for real-time analysis and problem detection/resolution, and monitoring for off-line outage analysis for longer term topology planning and/or optimization etc..

c) Magnitude of outage (scale of problem): The network topology should allow us to vary the magnitude of the outage and to determine the sensitivity of the solution to outage size. For example, it may be useful to compare large outages with smaller outages such as periodic video pixelization and/or audio artefacts. This will enable us to examine the resolution of the proposed solution. The effect of one monitoring threshold in the topology may trigger a disproportionate number of alarms and messaging.

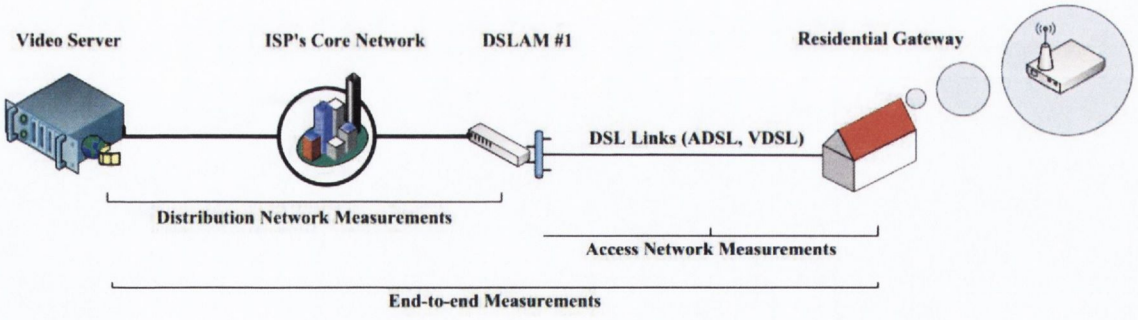
d) System scalability: The network topology should allow for additional emulated or simulated network components in order to investigate the scalability of the system. What data needs to be reported for a large versus small network? How often should we sample? How often should we report? Where should we perform aggregation? Can we aggregate the data in a meaningful way such that the monitoring data is tractable?

e) Scope of outage: The network topology should be amenable to simulating outages of different scale, for example, at the Head End, at the Central Office/Hub site, at the DSLAM (Digital Subscriber Line Access Multiplexer) etc. For example, if you shut down a DSLAM can we list out the users/home gateways affected?

f) Topology analysis: The network topology should help us gain an understanding of the calibration thresholds/parameters and patterns that may be used to trigger alarms for the service provider (in arbitrary networks perhaps). This analysis can then be used for inferring heuristic calibration guides for arbitrary networks.

g) Justifying monitoring cost: The network topology should help give an understanding of the number and effect of different outages on customer experience (QoE) and the resulting effect of customer dissatisfaction on churn.

The specification of metrics in this test-bed determines the rules and consequently the level of fault analysis that may be applied. Concurrently, we consider that the types of inferences that can be made from a set of metrics are dependent on the source of the various metrics




. Figure 5-3 Categorizing IPTV problem regions

To address these considerations, we start by specialising the unconstrained monitoring topology in Figure 5-2 to the reduced set of elements in Figure 5-3. Ideally, we perform

monitoring at various interfaces, servers and network elements for user impacting impairments from Super-Head End to SetTop-Box. However, a simplified IPTV network can be viewed as having two distinct parts; the Distribution Network (DN) and the Access Network (AN). The DN carries the IPTV traffic from the Video Server (VServer) to the Digital Subscriber Line Access Multiplexer (DSLAM) via the ISP's Core Network (CN). The AN (DSLAM to Residential Gateway (RG)) aggregates the traffic from multiple DSL connections for transmission on the ISP's CN; the AN is also responsible for distributing traffic to each customer's DSL connection from the CN. This simplified architecture is depicted in Figure 5-6. In terms of collecting metrics, monitoring agents are implemented in each of these network elements: RG, DSLAM and VServer. In the next section, we describe the nodes that should be monitored and the node specific metrics that should be monitored. Once monitoring data is collected, it is written to a monitoring CSV file. This simplified IPTV topology is used in the remaining sections to describe how a subset of the challenges above is addressed. The various components in the test topology are emulated using the network simulator NS-3.

This test-bed also takes a hardware emulation approach in order to duplicate each network element's behaviour: emulation is a well-established capability of many network simulators (NS-2, NS-3, Qualnet and OPNET); the wide-spread acceptance of NS-3's ability to accurately emulate the functionality of real network elements underpins the accuracy of these experimental results. An emulation approach is taken here in order to address the physical constraints and CAPEX associated with building a real test IPTV network. The Simulation Core simulates the test topology which consists of Edge Routers and DSLAMSs in this paper. Some nodes in the Simulation Environment are connected to the Simulation Core and to real network devices via sockets.

In this evaluation, DSLAMs and IP Edge Routers are emulated which allows us to simulate the types of problems identified in different regions in the exemplar topology. The combined emulation-simulation configuration is summarized in Fig. 5-10. The Simulation Host computer hosts the simulation and has real world connectivity through real network devices. In the Simulation Environment (NS-3) a Simulation Core simulates the desired topology of simulated-only nodes. The Simulation Core is comprised of components common across all protocols, hardware, and environmental models: the Simulation Core is used to build-up the entire simulation engine. This part of the system has no connection with the real components.

On the other hand, some nodes in the Simulation Environment are connected to both the Simulation Core and to real network devices installed on the real Simulation Host. The binding to the real devices is made using sockets. Furthermore, the real devices are then connected to Real Hosts.

The IPTV simulation/emulation system is presented in Fig.5-11(a). In summary, all components are interconnected using Ethernet cables using a single network switch. Each computer hosts a part of the IPTV system. PC1 is the Simulation Host running NS-3 as the Simulation Environment. PC2 plays the role of the video streaming server. PC3 is a computer with multi-port Gigabit Ethernet capability. PC3 plays the role of the end-users. For simplicity of exposition we illustrate one DSLAM and Edge Router in Fig. 5-11(b): More server and end-user instances are then instantiated using virtualization solutions in our experiments. To ease the reproducibility of the simulation/emulation environment the IP routing tables for all computers used are available on request.

The topology emulated by the NS-3 environment is illustrated in Fig. 5-11(b). Traffic pushed by the Video Server is forwarded through the ingress point of the Simulation Environment. From there, a simulated Gigabit per second (Gbps) line forwards the traffic to an IP Edge Router. The IP Edge Router serves a DSLAM through a Gbps connection. For simplicity, we have used only one DSLAM here, but the simulation can be scaled-up to include multiple DSLAMs. We have implemented our own DSLAM model in NS-3, which is able to collect and push monitoring reports to the central entity. Up to 100

DSL lines are served by the DSLAM. We have implemented an ADSL model with upload and download data rates of 10 megabits per second (Mbps) and 2 Mbps respectively. The ADSL lines forward traffic to the end-users via the NS-3 egress points. In our simulation scenario we use 100 ADSL lines. To avoid having 100 Network Interfaces to connect the 100 end- users to the DSLAM, we point each egress socket to the same real Network Interface on the Simulation Host. As such, all ADLS connections are multiplexed over one single 1 Gbps wired ethernet connection.

As a part of the experiment, the metrics of log data/report from both HAN and IPTV delivery network are defined according to the domain expertise. The definition of metric entities is listed below:

Table 5-3 The definition of log report metrics in HAN test-bed

| Resource Type | Entity in Log Report Metrics |
|---|---|
| VoIP Service | Bit Rate |
| | Retrains |
| | Antenna Noise |
| | Signal Strength |
| IPTV Service | Bit Rate |
| | Retrains |
| | Antenna Noise |
| | Signal Strength |
| Data Service | Bit Rate |
| | Retrains |
| | Antenna Noise |
| | Signal Strength |

Table 5-3 defined the metrics for VoIP, IPTV and Data services in log report from HAN test-bed. This report combined the data from both service side and device side. Various managed devices in IPTV networks exchange device specific metrics with the network management system. In our IPTV test-bed, we also described a simplified agent-based IPTV deployment scenario which describes which nodes require monitoring agents, what metrics can be collected from these agents, and what IPTV performance evaluation rules can be inferred from these agents. Metrics are collected from the residential gateway, the DSLAM and the video server. The metrics collected at each of these points of interest are summarized. Table 5-4 details the metrics that are collected from the residential gateway. Table 5-5 details the

metrics collected from the DSLAM. Table 5-6 details the metrics collected from the video server. The terms used in these metrics are described and defined as following:

1) Definition: Residential Gateway: The Residential Gateway is responsible for the distribution of all traffic within the home. It is also responsible for forwarding a customer's traffic to and from the Internet Service Provider's network via the access network (e.g. DSL or Hybrid Fiber Coax). Residential gateways are generally equipped with a single WiFi interface and multiple Ethernet ports. The GW metrics are taken from the underlying system metrics which are part of DD-WRT or have been collected using tshark captures. If a GW has the ability to filter out IPTV flows for independent monitoring of its traffic, it allows for a much more accurate monitoring of the IPTV service. The metrics of Gateway are:

Table 5-4 The definition of Gateway metrics in IPTV delivery network test-bed

| **Name** | **Description** |
|---|---|
| GATEWAY | This identifies the CSV as belonging to a gateway node |
| UniqueID | A unique ID for the GW (gateway-x, $0 \geq x \leq 100$) |
| Codec | This is a string indicating the codec in use (e.g H264 or MPEG2) |
| Bitrate | Fixed value of 1.5 corresponding to 1.5Mb/s SD video |
| Uptime | Records the gateway uptime (OS resource value) |
| IPTVPLR | Records the PLR (iperf stream value) |
| Latency | End-to-end latency between the GW and VServer |
| Jitter | Records jitter (iperf value) |
| iptvMOS | Mean Opinion Score ($1 \geq MOS \leq 5$) This is weighted to have an average of 4.75 |

- GW Uptime: This metric relates to the router itself. Regardless of the conditions of the network interfaces, downtime on a GW will terminate service delivery.

- PLR (Packet Loss Ratio) per Interface: This metric is the primary indicator of IPTV

service quality. Any loss of video data will have an impact on the customer's QoE. Loss events should be kept to a minimum in order to ensure maximum QoE. Any loss events should be noted and reported.

- Latency: This metric records the latency between the GW and the VServer. Latency is very important in the broadcast IPTV scenario; it defines the channel switching delay when a customer selects an new channel.

- Jitter: The inter-arrival times of packets sent from the VServer to the GW must be kept relatively fixed in order to ensure smooth playback. One approach to ensuring this is the application of a jitter buffer; however, this effects the response time of the server.

- Video Mean Opinion Score (MOS): This metric is employed to ascertain the quality of the received video which is presented to the customer. Measurement of video MOS is not always feasible due to the associated monitoring complexity; and yet, if video MOS scores are available they will provide the ISP with a very accurate indication of IPTV service quality. A large number of different metrics are available for selection, but for an operational deployment either non-reference or reduced- reference metrics are typically used. The corresponding scores for each of these metrics can then be converted to a mean opinion score. If direct access to the Set-Top Box (STB) is not available, the STB may calculate and forward the MOS to the GW; the work in this thesis assumes that this is the case.

2) Definition: Digital Subscriber Line Access Multiplexer (DSLAM): The Digital Subscriber Line Access Multiplexer is responsible for the aggregation of individual DSL links onto the ISPs back- haul network. In addition, it performs the forwarding of traffic from the ISPs backhaul network to the appropriate DSL link to the GW in the customer's home. There are a large number of factors which can affect the delivery of traffic to/from the customers GW, such as line attenuation or excessive traffic demands. All parameters related to these must be monitored in order to ensure that the DSL connection between the customer and the ISPs backhaul network is capable of IPTV service delivery with a high-level of QoE. The metrics of DSLAM are:

Table 5-5 The definition of DSLAM metrics in IPTV delivery network test-bed

| Name | Description |
|---|---|
| DSLAM | This identifies the CSV as belonging to a DSLAM node |
| UniqueID | A unique ID for a DSLAM (random variable on 64 bits in ns3) |
| port_id | An int value of the port number used for CSV reporting (typically 48 for current DSLAMs) |
| line_status | A string value representing the current line status (Up/Down/Test, Up = normal, Down = broken, Test = under repair) |
| average_up _line_rate | A value in Mb/s representing the rate of data flow from DSLAM to GW |
| average_down _line_rate | A value in Mb/s representing the rate of data flow from home GW to DSLAM |
| port_severely_ errored_seconds [a] | A value in seconds representing the total amount of time the port has spent experiencing transmission errors (when t = 2 an alert is triggered) |
| port_unavailable _seconds | A value in seconds representing the total amount of time the port was unavailable (line_status = Down/Test) When t = 3 an alert is triggered |
| port_high_ber | A value in seconds representing the total amount of time the port was affected by high bit error rate (when t = 15 an alert is triggered) |
| line_noise _margin | A float value representing the noise margin on the DSL line (triggered if < 10 dB) |
| line_resyncs | A value representing the current number of DSL resyncs performed by the line in the last monitoring interval (when resync = 2 an alert is triggered) |

- Port Status: A value used to represent the current status of the port (Up = ready to transmit, Down = unable to transmit and Testing = testing mode and is unavailable to transmit).

- Line Status: A value used to represent the current status of the connection with the GW. All possible values are enumerated below:

  1) Down: No connection to GW

  2) Downloading: Sending updated firmware to GW.

  3) Data: Connection established, passing data.

  4) Test: In test state.

  5) Unknown: Connection with GW failed due to an unknown error.

- Line Uptime: A value to record how long the connection with the GW has been up.

- DSL Max Attainable Up Line Rate: A value to represent the maximum attainable upstream line rate on a port.

- DSL Max Attainable Down Line Rate: A value to represent the maximum attainable downstream line rate on a port.

- DSL Up Line Rate: A value to represent the current upstream line rate on a port.

- DSL Down Line Rate: A value to represent the current downstream line rate on a port.

- Port In/Out Errors: Values to represent the current number of in or out transmission errors.

- Port Severely Errored Seconds (SES): A value to represent the amount of time in seconds experiencing severe errors on a port.

- Port Unavailable Seconds(UAS): A value to represent the amount of time in seconds that the ADSL line is unavailable for a port.

- Port Loss of Signal Seconds(LOS): A value to represent the amount of time in seconds when a loss of signal has occurred.

- Seconds declared as high bit error rate: A value to represent the amount of time in seconds that have had a high BER for a port.

3) Definition: Broadcast or Video on Demand Server: The video server (VServer) is responsible for the preparation of source content for transmission across the DN and AN. The source content can be either a live broadcast, or stored on- demand content. Regardless of the content's origin, a number of steps must be undertaken in order to prepare the content for transmission. These steps include: codec selection; bitrate shaping; selection of either Constant or Variable Bit Rate (CBR and VBR resp.) video; GOP structure; frame rate; and finally the encoding process. Encoding can be done in either real-time, on the fly, or prior to transmission. Before transmission of video data occurs, it must be packetized for transmission. Video data may be encapsulated in an MPEG Transport Stream which is then further encapsulated within a UDP/IP or RTP/UDP/IP format. The MPEG transport stream lends itself to the creation of CBR video traffic; typically there are 7 MPEG TS packets (188 bytes each) encapsulated inside each IP packet, giving a fixed size of 1,316 bytes in the MPEG TS payload. The server sends these at a fixed rate in the case of CBR video. The VServer may adjust the transmission rate of packets when using VBR traffic (assuming MPEG TS is used since each packet size is fixed). Metrics of Broadcast or Video on Demand Server are:

Table 5-6 The definition of video server metrics in IPTV delivery network test-bed

| **Name** | **Description** |
|---|---|
| VServer | This identifies the CSV as belonging to a VServer node |
| UniqueID | A unique ID for the VServer (server-x,$0 \leq x \geq 100$ ) |
| PLR | The Packet Loss Rate for the VServer's outgoing interface |
| Latency | Records end-to-end latency between the VServer and GW |
| AccSuccRate | Records the access success rate for the VServer (mean of 98%) |
| AvStrmSetup | Average stream setup time, (mean = 150ms) (2PING $\mapsto$ GW + Processing Time) |
| CurResUse | Current resource useage (OS statistics) |

- Video Server Packet Loss: A value to represent the current loss rate on the video server's outgoing link(s) to the DN. A value greater than zero indicates a severe

problem with either the server or its link to the DN; such a scenario must be remedied immediately. Losses further down the path to the customer may be tolerated to some extent, but losses/errors at the server (especially Broadcast TV) will affect a large number of users.

- Video Server Latency: A value to represent the latency between a VServer and a connected customer's STB. Excessive latency will decrease QoE due to excessive wait times for channel change or on-demand transactions.

- Video Access Success Rate: A value to represent the current video access success rate, i.e. what percentage of requests to access a particular video or channel lead to successful transmission of the video/channel.

- Average Stream Setup Time: A value to represent the average time taken to setup an on-demand (or broadcast group join). This is calculated in the present paper as the time taken from the initial setup request to the time taken for the first packets to be transmitted to the customer.

- Video Server Resource Utilisation Rate (%): A value to represent the current resource utilisation rate expressed as a percentage of available resources. Resources can be individually measured in terms of the CPU, memory or disk access. In this work we measure video server resource utilization rate as a combination of all three parameters.

4) End-to-End Metrics:

- Packet Loss Rate PLR (%): Limit Set LIMIT as suggested packet loss rates. Can be either across all traffic or ideally for IPTV traffic only.

## 5.5 *Evaluation for Information Uplift Approach (E1)*

### 5.5.1 Introduction

This section describes the iterative evaluation to validate if the design of information uplift approach and its implementation CASIU is able to uplift meaningful information from real time data by leveraging the domain expert knowledge (**E1**). This evaluation also validated if the design requirement **R1** has been fulfilled to achieve the research objective 2 **(Objective 2)** derived from the research question in Section 1.2. As discussed in the previous section, this

evaluation goal could be divided into five subordinate evaluation goals (**E1.1, E1.2, E1.3, CE, PE**) approached through an evolving experimental process (Chapter 4). The evaluation goal, evaluation setting and evaluation result of each subordinate evaluation goal will be described in the following sections.

### 5.5.2 Evaluation for Heterogeneous Real-time Data Input (E1.1)

#### *5.5.2.1 Evaluation Goal*

The nature of network environment determines this uplift process executed in a real time, which requires that CASIU is capable of processing real-time data input. Therefore, the evaluation goal **E1.1** is to validate to what extent CASIU is able to consume heterogeneous real-time data input. There were two main iterative experiments for achieving this evaluation. The first looked at the approach implemented in the CAISU prototype for HAN and IPTV delivery network monitoring, where the data mapping approach acted as a mediator between the information uplift process and multiple data sources, was appropriate from a technical perspective. The second aim was to get qualitative feedback as to whether CASIU facilitated useful functionality that accepts real-time data input. Specifically this functionality was enabling data mapping to create meaningful connections over multiple separate data sources in order to support information uplifting. By showing this, it would help support the hypothesis that CASIU provided access to data sources without prescribing specific interfaces, or for their developers to know a specific query language and map data entities.

#### *5.5.2.2 Evaluation Setting*

This evaluation involved the use of an early experiment of CASIU that worked exclusively with CSV log sources, as well as a purpose built client application that contained a data source model building. The physical network structure communicated to CASIU by passing log reports in accordance with CASIU's API, and there were no restrictions placed on the design of the log reports. The establishment of a Home Area Network and IPTV delivery network test bed enabled to create consolidated evaluation across the simulated data stream defined by domain expert in order to validate the design and implementation of supporting heterogeneous real-time data inputs. However, the design of the test-bed and log report itself was not evaluated in this experiment, as its role was purely to make a trustable evaluation environment by referencing related research to the test beds adopted in this evaluation.

#### *5.5.2.3 Evaluation Result*

As a part of the experiment, the metrics of log data/report from both HAN and IPTV delivery network are defined according to the domain expertise. After examining the metadata available from the different sources, a domain expert then created four metrics mapping schemas (One for HAN metric, and three for IPTV metrics) and had them integrated into CASIU to load from a pre-defined XML file. As explained in Chapter 3, these mapping schemas enable the mapping between resource models to the entities in log data metrics from different network resources.

After appropriate configuration of the test-bed, CASIU is able to run on the test-bed and receive the real-time log data. A strategy has been adapted to validate if the CASIU could uplift the real-time data from multiple network resources:

a) Generate several stream data sets in two test-beds.

- This data is simulated through our test-beds based on a time interval of 2s. The scalability of the test-bed is set as one router with three devices in HAN; and one video server, two edge routers, four core routers, two DSLAMs and three routers in the IPTV network. The data is also timely updated to the logs, which is fed to CASIU through data input API. Three datasets are generated in each test-bed.
    - Dataset 1 in HAN: 10 minutes data with 103 "0" values
    - Dataset 2 in HAN: 20 minutes data with 145 "0" values
    - Dataset 3 in HAN: 30 minutes data with 302 "0" values
    - Dataset 1 in IPTV: 10 minutes data with 532 "0" values in total
    - Dataset 2 in IPTV: 20 minutes data with 765 "0" values in total
    - Dataset 3 in IPTV: 30 minutes data with 998 "0" values in total

b) Record the timestamp of every piece of data with 0 values.

- The simulated data contains randomly generated 0 values. These 0 values are recorded with their timestamp by using a Java program.

c) Setup CASIU to uplift and visualize the data input.

- CASIU is setup on the top of test-beds and receives the stream data via API with time interval 2s. These data are mapped to resource models and uplifted by a simple rule: if data equals 0, it is in "Bad" condition and show red label in the visual widget (Fig. 5-4).

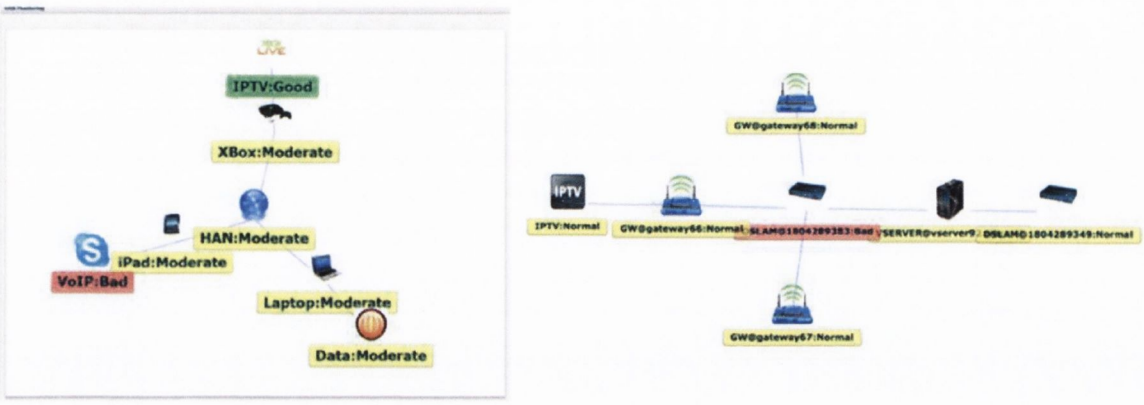



Figure 5-4 Screenshots of Network Topology Widget in Evaluation **E1.1**

d) Monitor and record the timestamp when the node label turns into red.

- A script was embedded in the visual widget to trigger a record when the label of network node turns into red. This record is also marked with timestamp.

e) Examine the network topology and compare the records from data source and visual widget.

- The records from data source and visual widget are firstly used to examine if it is recorded to the correct network node and present the right network topology, which evaluates if the entities in log data are mapped to appropriate resource models. Then the records are compared to see if the 0 values are correctly rendered by CASIU. The evaluation results are listed below.

Table 5-7 Evaluation Result Table of **E1.1**

| **Evaluation E1.1** | **Iterative Experiments** | | | | **Result** |
|---|---|---|---|---|---|
| | **Exp2 with HAN** | | **Exp4 with IPTV** | | |
| Topology Examination | Dataset 1 | Correct | Dataset 1 | Correct | Pass |
| | Dataset 2 | Correct | Dataset 2 | Correct | |
| | Dataset 3 | Correct | Dataset 3 | Correct | |
| Record Comparison | Dataset 1 | Correct | Dataset 1 | Correct | Pass but with timestamp latency |
| | Dataset 2 | Correct | Dataset 2 | Correct | |
| | Dataset 3 | Correct | Dataset 3 | Correct | |

As shown in Table 5-7, this evaluation is approached in two iterative experiments. In each experiment, CAISU was examined with 3 datasets and got correct results. In Exp2, the evaluation validated CASIU is able to uplift the information from single data source and it's further validated with multiple data sources in Exp4. The latency of timestamp in two records reveals the cost of CASIU, which will be further evaluated in the performance evaluation (**PE**). As a conclusion, CASIU is able to uplift multiple real-time data inputs with heterogeneous metrics. The goal of **E1.1** is fulfilled in this evaluation.

### 5.5.3 Evaluation for Uplifting Meaningful Information (E1.2)

#### *5.5.3.1 Evaluation Goal*

As discussed in Chapter 3, CASIU is designed to fulfil the challenges from Chapter 2 by uplifting meaningful information from the real-time data input (**R1.2**). This evaluation **(E1.2)** aims to validate if CASIU is able to uplift meaningful information from a functional point of view. The imported expert knowledge is also crucial to enable this information uplifting process. There were three iterative experiments for achieving this evaluation. The first looked

at the design initially implemented in the CAISU prototype for HAN monitoring, where the one-level (semantic attribute) information uplifting approached for a single data source, and the other two experiments implemented the multi-level uplifting process in different network scenario with multiple data sources, was appropriate from a technical perspective. Followed by a qualitative analysis on the evaluation results as to whether CASIU enables functionality that uplifts meaningful information by leveraging domain knowledge. Specifically this functionality was enabling information uplifting from multiple real-time data input. By showing this, it would help support the hypothesis that CASIU could leverage domain knowledge to support information uplift from multiple data input. However, the performance, feasibility and usability of CASIU was not evaluated in this experiment, as they are further evaluated in following sections.

#### *5.5.3.2 Evaluation Setting*

This evaluation involved the use of test-beds setup in Section 5.4.2.2, which provides a HAN test-bed and also an IPTV delivery network test-bed. The physical network structure communicated to CASIU by passing log reports in accordance with CASIU's API, and there were no restrictions placed on the design of the log reports. The establishment of a Home Area Network and IPTV delivery network test bed enabled a consolidated evaluation across the simulated data stream defined by a domain expert in order to validate the design and implementation of uplifting meaningful information from heterogeneous real-time data inputs. As described in Chapter 3, the domain knowledge model is important for this information uplifting process. The description of domain knowledge applied to two test-beds is introduced in following sections, which also support other evaluations.

1) Home Area Network (HAN) Data Sample and Domain Knowledge

As described in Section 5.4.2.2, our HAN test-bed could generate a log data report, which contains monitoring signal data from clients at the AP and its metrics are associated with a particular IP address and each address is associated with a particular service type – VoIP, Video or other.

| | | VoIP Service | | | | IPTV Service | | | | Data Service | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Time 1 | Time 2 | Bit rate | Retrans | Antenna Noise | Signal Strength | Bit rate | Retrans | Antenna Noise | Signal Strength | Bit rate | Retrans | Antenna Noise | Signal Strength |
| 0 | 1 | | | | | 3.17424 | 0.000779 | -82.8667 | -37.4314 | 8.463056 | 0.002276 | -84.1325 | -23.9588 |
| 1 | 2 | | | | | 2.887936 | 0.000718 | -83.5129 | -37.319 | 7.877248 | 0.00219 | -83.9114 | -23.0902 |
| 2 | 3 | | | | | 2.999968 | 0.000638 | -83.5643 | -37.2863 | 8.03928 | 0.002036 | -82.6884 | -22.1829 |
| 3 | 4 | | | | | 2.066368 | 0.000965 | -81.9819 | -37.5422 | 8.550304 | 0.002135 | -83.6137 | -22.8163 |
| 4 | 5 | | | | | 4.020704 | 0.000536 | -84.0526 | -37.3096 | 8.575232 | 0.002099 | -86.1366 | -22.8547 |
| 5 | 6 | | | | | 3.199136 | 0.000748 | -82.5525 | -37.4553 | 8.28856 | 0.002506 | -84.9203 | -25.0857 |
| 6 | 7 | | | | | 2.999968 | 0.001383 | -82.8257 | -37.444 | 8.587696 | 0.00217 | -85.0929 | -25.7866 |
| 7 | 8 | | | | | 5.439776 | 0.001174 | -86.0984 | -37.7277 | 8.438128 | 0.002641 | -85.127 | -25.9069 |
| 8 | 9 | | | | | 5.502016 | 0.001044 | -85.8032 | -37.5204 | 7.765072 | 0.00227 | -84.3274 | -26.3291 |
| 9 | 10 | | | | | 2.688768 | 0.001246 | -85.4167 | -37.5278 | 2.355696 | 0.00155 | -81.1905 | -22.3968 |
| 10 | 11 | | | | | 2.651424 | 0.001144 | -85.8075 | -37.4883 | 7.316368 | 0.002357 | -83.0187 | -26.2385 |
| 11 | 12 | | | | | 8.140992 | 0.000902 | -85.4954 | -37.4495 | 7.627968 | 0.002311 | -83.8137 | -26.4444 |
| 12 | 13 | | | | | 8.02896 | 0.000994 | -84.5271 | -37.5364 | 7.60304 | 0.002285 | -83.3656 | -25.6574 |
| 13 | 14 | | | | | 8.46464 | 0.000848 | -85.4794 | -37.5824 | 3.714272 | 0.002373 | -67.2886 | -26.8423 |
| 14 | 15 | | | | | 4.991648 | 0.001551 | -85.4813 | -37.5287 | 3.340352 | 0.002525 | -64.1642 | -26.9515 |
| 15 | 16 | | | | | 4.780032 | 0.001603 | -85.8177 | -37.4479 | 4.11312 | 0.002173 | -63.703 | -27.7697 |

Figure 5-5 Sample Log Report from HAN test-bed

Figure 5-5 shows a sample log data report which aggregates log data from clients and services. Table 5-8 demonstrates the domain knowledge applied to this data report.

Table 5-8 Domain Knowledge for Log Report from HAN test-bed

| Metric | Good | Moderate | Bad |
|---|---|---|---|
| Antenna noise | <-90dBm<br>This is the normal operating mode. | -90dBm to -80dBm<br>If a value in this range is consistently measured, it indicates a poor connection to the antenna or a mediocre chipset. A sudden move to this range from "good" indicates an interference problem that the customer should rectify. | >-80dBm<br>Consistent values here show a system failure. Transients indicate strong external interference that must be rectified. |
| Signal Strength | >-74dBm<br>This should yield good throughput for the device. If throughput is bad for this service, then check for congestion | -74dBm to -86dBm | <-86dBm |

| | | | |
|---|---|---|---|
| VoIP throughput. Assuming a duplex G711 call, the limit applies to both uplink and downlink | >63kbps<br>No packet loss, quality should be good, but doesn't take into account delay. | 63kbps to 32kbps<br>High packet loss, but link is maintained | <32kbps<br>Very high packet loss, problems being able to understand words |
| Video throughput change.<br>Assume a CBR UDP stream. Maintain a running average over the past 5 mins and for each 10 seconds, calculate the downlink throughput reduction as a percentage of the average. Any increase is not flagged, but will impact on the average. | <1%<br>Some variation due to window boundary not lining up with frames. | 1% to 10%<br>This level of variation indicates packet loss – quality is dubious. | >10%<br>This level of packet loss would indicate an unusable service. |
| Ratio of retransmissions.<br>If this is not correlated with signal strength, or antenna noise, then it is caused by congestion in the HAN | <1%<br>This is normal mode of operation. | 1% to 10%<br>This may indicate a poor radio channel if it is correlated to a particular service's radio metrics. If it is for all users, then it indicates the onset of congestion | >10%<br>If signal strength is good or moderate and antenna noise is moderate or good, then network is congested |

2) IPTV Delivery Network Data Sample and Domain Knowledge

Various managed devices in IPTV networks exchange device specific metrics with monitoring network systems. We describe a simplified IPTV deployment scenario which describes which nodes require monitoring agents, what metrics can be collected from these agents, and what IPTV performance evaluation rules can be inferred from these agents.

The roles of each major component within the delivery network architecture, including: the VServer, DSLAM and GW are defined in this section. Based on these component definitions, metrics are categorized as End-to-End, access network or distribution network metrics. Definitions are provided for all metrics of interest in each of the network measurement categories, namely; End-to-End, AN and DN. A set of domain knowledge are defined for each category of metric (This set is by no means comprehensive). This knowledge can be used to ascertain the health of the IPTV service. The domain knowledge can be extended to provide a simple root-cause analysis capability.

1) Metric & Rules: Residential Gateway:

- GW Uptime:

  Rule: If GW.UPTIME < Monitoring Interval, GW has rebooted, trigger alarm

- PLR (Packet Loss Ratio) per Interface:

  Rule: If GW.INTERFACE.PLR > 0, trigger warning

- Latency:

  Rule: If AVERAGE (GW.LATENCY) > LATENCY.THRESHOLD, trigger warning. As per TR-126 this threshold should be set at 200ms.

- Jitter:

  Rule: If AVERAGE(GW.JITTER) > JITTER.THRESHOLD, trigger warning. As per TR-126 this threshold should be set at 50ms.

- Video Mean Opinion Score (MOS):

- Rule: If AVERAGE(GW.MOS) < MOS.THRESHOLD, trigger warning. This threshold may be derived based on,subscriber type, content type, etc.

2) Metrics & Rules: Digital Subscriber Line Access Multiplexer: Note the term port is used here to identify a single DSL connection to a customer's residential gateway. The metrics, their names and values are based on a review of DSLAM hardware documentation.

- Port Status:

  Rule: If DSLAM.PORT.PORTSTATUS == DOWN|TESTING, trigger alert.

- Line Status:

  Rule: If DSLAM.PORT.LINESTATUS == DOWN|DOWNLOADING|TEST|UNKNOWN, trigger alert.

- Line Uptime:

  Rule: If DSLAM.PORT.LINEUPTIME < Monitoring Interval, trigger alert.

- DSL Max Attainable Up Line Rate:

  Rule: None.

- DSL Max Attainable Down Line Rate:

  Rule: None.

- DSL Up Line Rate:

  Rule: If DSLAM.PORT.DSLUPLINERATE < DSLAM.PORT.DSLMAXATTAINABLEUPLINERATE, trigger alarm.

- DSL Down Line Rate:

  Rule: If DSLAM.PORT.DSLUPLINERATE < DSLAM.PORT.DSLMAXATTAINABLEUPLINERATE, trigger alarm.

- Port In/Out Errors:

  Rule: If DSLAM.PORT.IN(OUT)ERRORS > Threshold, trigger alarm.

- Port Severely Errored Seconds (SES):

Rule: If DSLAM.PORT.SES > Threshold, trigger alarm.

- Port Unavailable Seconds(UAS):

  Rule: If DSLAM.PORT.SES > Threshold, trigger alarm.

- Port Loss of Signal Seconds(LOS):

  Rule: If DSLAM.PORT.LOS > Threshold, trigger alarm

- Seconds declared as high bit error rate:

  Rule: If DSLAM.PORT.HIGHBER > Threshold, trigger alarm

3) Metrics & Rules: Broadcast or Video on Demand Server:

- Video Server Packet Loss:

  Rule: If VSERVER.LINK.PLR > 0, trigger alarm.

- Video Server Latency:

  Rule: If VSERVER.LINK.LATENCY > threshold, trigger warning.

- Video Access Success Rate:

  Rule: If VSERVER.ACCESSSUCCESSRATE < threshold, trigger warning.

- Average Stream Setup Time:

  Rule: If VSERVER.AVERAGESETUPTIME > threshold, trigger warning

- Video Server Resource Utilisation Rate (%):

  Rule: If VSERVER.RESOURCEUTILISATIONRATE> threshold, trigger warning. The recommended value for 'threshold' will most likely require some experimental analysis to understand the number of sessions that can be concurrently run.

4) End-to-End Metrics and Rules:

- Packet Loss Rate PLR (%): Limit Set LIMIT as suggested packet loss rates in Table 5-

9. Can be either across all traffic or ideally for IPTV traffic only. Appealing to TR126, the recommended values are tabulated in Table 5-9.

Table 5-9 End-to-end Metrics

| Encoding | Limit |
|---|---|
| SD Video MPEG-2 Encoding | 3.0 Mb/s 5.85e-6<br>3.75Mb/s 5.46e-6<br>5.0Mb/s 5.26e-6 |
| SD Video H.264 AVC or VC-1 Encoding | 1.75Mb/s 6.68e-6<br>2.0Mb/s 7.31e-6<br>2.5Mb/s -5.85e-6<br>3.0Mb/s 5.85e-6 |
| HD Video MPEG-2 Encoding | 15Mb/s 1.17e-6<br>17Mb/s - 1.16e-6<br>18.1Mb/s 1.17e-6 |
| HD Video H.264 AVC or VC-1 Encoding | 8Mb/s 1.28e-6<br>10Mb/s -1.24e-6<br>12Mb/s 1.22e-6 |

#### *5.5.3.3 Evaluation Result*

As a part of the experiment, the metrics of log data/report from both HAN and IPTV delivery network and corresponding domain expertise are defined and captured. Focusing on the real-world monitoring challenges, a set of domain knowledge was captured and modelled into Semantic Attributes and Semantic Segments. There were two HAN experts and three IPTV experts, who have solid knowledge in these areas, participated into contributing their knowledge. As explained in Chapter 3, these knowledge models could ensure the information uplifting process.

After appropriate configuration of the test-bed, CASIU is able to run on the test-bed and receive the real-time log data. A strategy has been adapted to validate if the CASIU could uplift meaningful information from multiple input data:

a) Generate several stream data sets in two test-beds.

- This data is simulated through our test-beds based on a time interval of 2s. The scalability of the test-bed is set as one router with three devices in HAN; and one video

server, two edge routers, four core routers, two DSLAMs and three routers in IPTV network. The data is also timely updated to the logs, which is fed to CASIU through data input API. Three datasets are generated in each test-bed.

- Dataset 1 in HAN: 10 minutes data
- Dataset 2 in HAN: 20 minutes data
- Dataset 3 in HAN: 30 minutes data
- Dataset 1 in IPTV: 10 minutes data
- Dataset 2 in IPTV: 20 minutes data
- Dataset 3 in IPTV: 30 minutes data

b) Capture and model expert knowledge

- Domain experts were asked to contribute their domain insights to support network monitoring. In the HAN scenario, domain expertise focuses on aggregating the data from service side and hardware side; and it's more focusing on correlating the logs from different network nodes to the Quality of Experience (QoE) for end-users in the IPTV delivery network.

c) Annotate the log data by using domain knowledge

- Load evaluation data from each dataset into one CSV file. The domain rules are hard coded into a Java program and execute it to annotate all semantic meanings to the dataset. The result is recorded as a benchmark for comparison.

d) Setup CASIU to uplift and visualize the meaningful information.

- CASIU is setup on the top of test-beds and receives the stream data via API with time interval 2s. These real-time data are uplifted by using domain knowledge and the meaningful information is also visualised (Fig. 5-6).

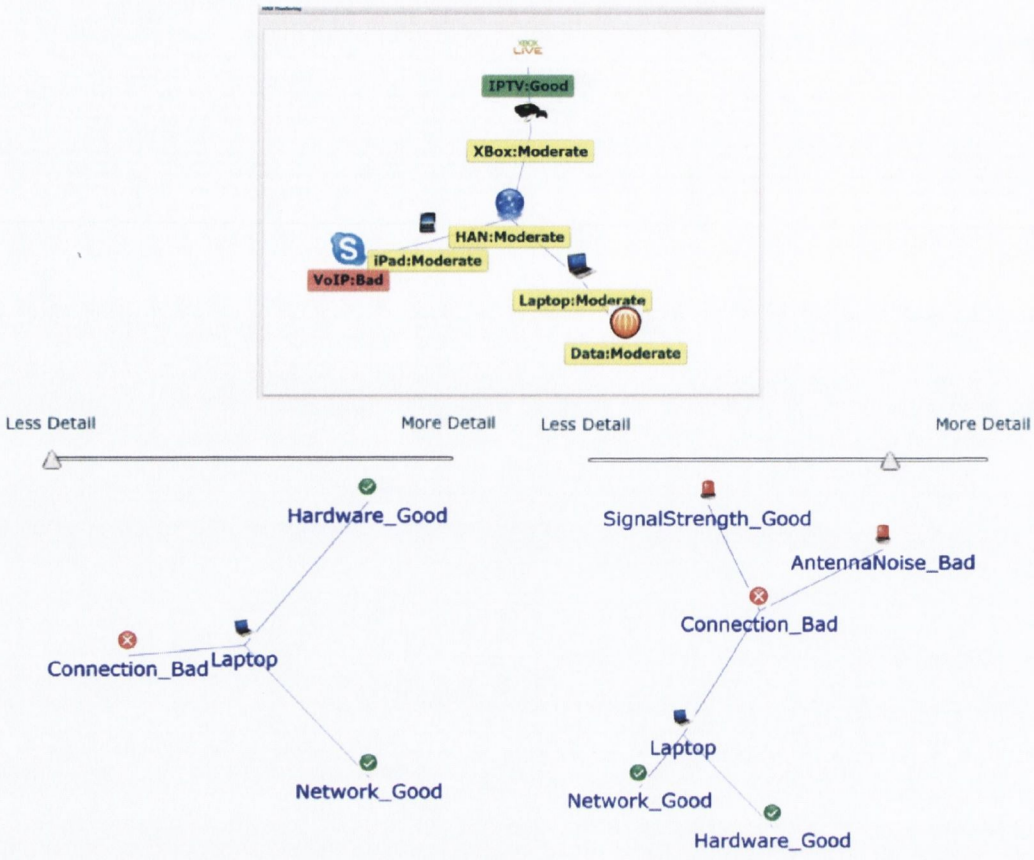



Figure 5-6 Screenshots of Visually Presenting Semantic Information

e) Record the uplifted semantic information.

- A script was embedded in the visual widget to trigger a record of the label of network node. This record is also marked with timestamp.

f) Examine the network topology and compare the records from data source and visual widget.

- The records from data source and visual widget are firstly used to examine if it is recorded to the correct network node and present the corresponding meaningful information, which evaluates if the annotated semantic entities are linked to appropriate resource models. Then the records are compared to see if the semantic meanings are correctly uplifted by CASIU. The evaluation results are listed below.

Table 5-10 Evaluation Result Table of E1.2

| **Evaluation E1.2** | **Iterative Experiments** | | | | | |
|---|---|---|---|---|---|---|
| | **Exp1 with HAN (Single Data Source)** | | **Exp2 with HAN (Multi-Data Source)** | | **Exp4 with IPTV (Multi-Data Source)** | |
| Correction Rate of Links to Network Node | Dataset 1 (4 Nodes) | 100% | Dataset 1 (7 Nodes) | 100% | Dataset 1 (200 Nodes) | 100% |
| | Dataset 2 (4 Nodes) | 100% | Dataset 2 (7 Nodes) | 100% | Dataset 2 (200 Nodes) | 100% |
| | Dataset 3 (4 Nodes) | 100% | Dataset 3 (7 Nodes) | 100% | Dataset 3 (200 Nodes) | 100% |
| Correction Rate of Uplifted Information | Dataset 1 (325 Entities) | 100% | Dataset 1 (802 Entities) | 100% | Dataset 1 (3021 Entities) | 94% |
| | Dataset 2 (634 Entities) | 100% | Dataset 2 (1203 Entities) | 100% | Dataset 2 (7321 Entities) | 89% |
| | Dataset 3 (1198 Entities) | 100% | Dataset 3 (1882 Entities) | 95% | Dataset 3 (9980 Entities) | 67% |

As shown in Table 5-7, this evaluation is approached in three iterative experiments. In each experiment, CAISU was examined with 3 datasets in two different network monitoring scenarios and got a series of results. In Exp1, the evaluation validated CASIU is able to uplift

the information from single data source with 100% correction rate; Exp2 shows the capability of CASIU to uplift information from heterogeneous data sources also with good correction rate and this information uplift approach was further validated with large amount of information from multiple data sources in Exp4, which shows a significant decrease of correction rate. This drawback indicates there is limitation on CASIU engine. These limitations will be further examined and analysed in the feasibility (**FE**) and performance evaluation (**PE**). As a conclusion, CASIU is able to uplift meaningful information from multiple real-time data sets and also there are some limitations on this approach. The goal of **E1.2** is fulfilled in this evaluation.

### 5.5.4 Evaluation for High-level Monitoring Objectives (E1.3)

#### *5.5.4.1 Evaluation Goal*

Based on the uplifted meaningful information, CASIU is also capable to support high-level monitoring objectives. As discussed in Chapter 3, CASIU is designed to leverage domain knowledge to enable information uplifting to support higher-level monitoring objectives Therefore, the evaluation goal **E1.3** is to validate the high-level monitoring tasks in different scenarios which CASIU is able to support. There were three main iterative experiments for achieving this evaluation. The first looked at the approach implemented in the CASIU prototype for HAN network monitoring, where supports for non-expert users to detect and analyse network problems by correlating the information from both physical connection and service qualities. The second aim was to support a network administrator to monitor IPTV delivery network and diagnose connection problems. The third experiment combines the information from delivery network and service itself to enable a Quality of Experience (QoE) based IPTV monitoring (see Chapter 4). By showing this, it would help support the hypothesis that the information uplift CASIU provided is able to support high-level monitoring objectives for non-expert users by leveraging the domain expertise.

#### *5.5.4.2 Evaluation Setting*

This evaluation involved the use of test-beds setup in Section 5.4.2.2, which provides a HAN test-bed and also an IPTV delivery network test-bed. The physical network structure communicated to CASIU by passing log reports in accordance with CASIU's API, and there were no restrictions placed on the design of the log reports. The establishment of a Home Area Network and IPTV delivery network test bed enabled a consolidated evaluation across the

simulated data stream defined by a domain expert in order to validate the design and implementation of uplifting meaningful information from heterogeneous real-time data inputs. As described in Chapter 3, the domain knowledge model is important for this information uplifting process.

#### *5.5.4.3 Evaluation Results*

This evaluation validates the feasibility of the proposed monitoring system using the four problem scenarios. To evaluate the feasibility of the proposed monitoring system, this evaluation proposed four problem scenarios. These monitoring scenarios are designed to expose if the solution can deal with single and multiple points of failure in IPTV delivery and to address a subset of the challenges listed above. In particular, the NM is interested in determining whether or not our integrated solution delivers knowledge of outage in a per user manner and allows the NM to assess the impact of an outage on a per user level. The scenarios are named as follows:

- **Scenario 1**: Excessively high latency at the GW causes poor QoE.
- **Scenario 2**: A high number of severely errored seconds at the DSLAM causes poor QoE.
- **Scenario 3**: A high latency and high number of severely errored seconds contributed to poor QoE.
- **Scenario 4**: The resource utilization rate breaches a threshold at the Video Server which causes poor QoE.

Each scenario is defined in more detail in the following subsections. We continue by describing the experiment emulation environment used to create the test network and network events.

In these experiments, an anomaly or problem has occurred when an IPTV subscriber is experiencing a low QoE, due to fluctuations in the IPTV flow in the network test-bed. The subscriber IPTV flows traverse the simulated network from the video server and are routed to home users through the DSLAMs and the home gateways. We emulate an IPTV delivery network with a video server, two DSLAMs are simulated and three home routers are created using NS-3 models. Each node in the network collects their respective metrics and generates

metric CSV files. The network log data is then reported to the information uplift engine. The uplift engine performs the necessary steps to correctly identify the source(s) of the problem, the particular metric threshold(s) that were breached, and then, the uplift engine uses this information to suggest a solution to the NM. This process is now explained by example.

**Scenario 1**: Excessively high latency at the GW is causing poor QoE: Using a simulation script we cause a single point of failure to occur in the network. Naturally, from the perspective of failure detection and location, we assume the NM is unaware of the time and location of the failure. The uplift engine inspects the CSV entries from the gateway, DSLAM and video server. This procedure examines the metric values in the CSV files to ascertain which metrics have breached their threshold(s). Problem detection, analysis and identification is described below. This process is visualized in the analysis panel of the visual interface with screenshot in Fig.5-7. In order to show clear details, this screen has been illustrated with a mock up figure as in Fig. 5-8, and the same as figures in other scenarios.

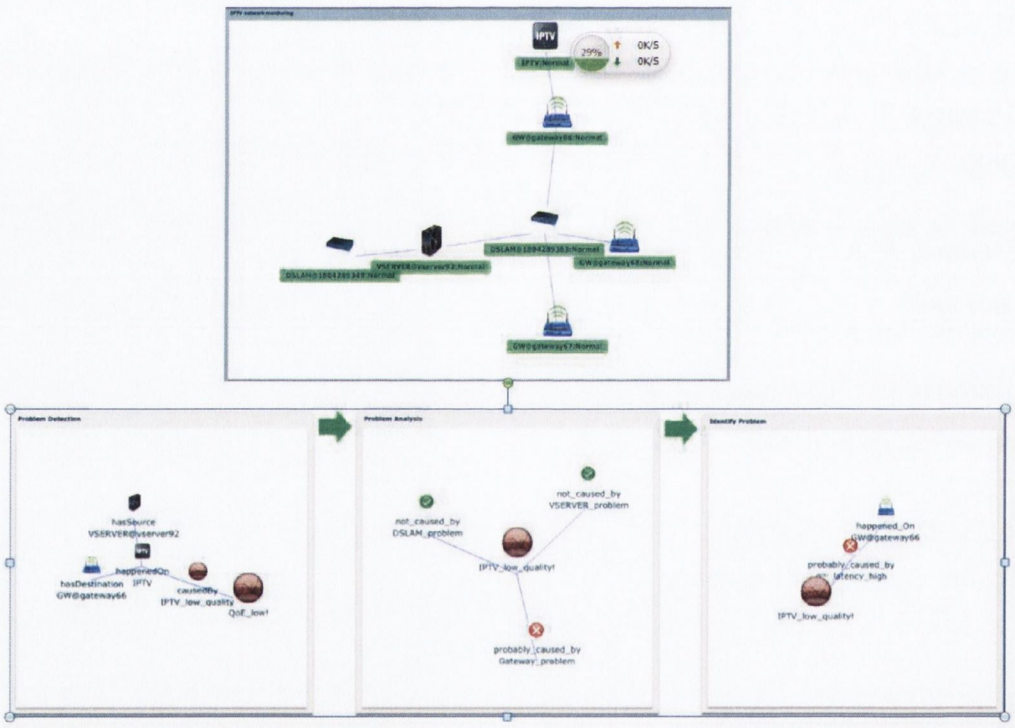



Figure 5-7 Screenshot of Analysis Process in Scenario 1

The topology used to illustrate the problem location and diagnosis process and then the suggested corrective action provided in response to the four scenarios presented here. A

comprehensive analysis of monitored events on a simulated IPTV network is visualized by the NM using the Network Topology, Problem Analysis and Diagnosis, and Real-time Event Monitoring Widgets.

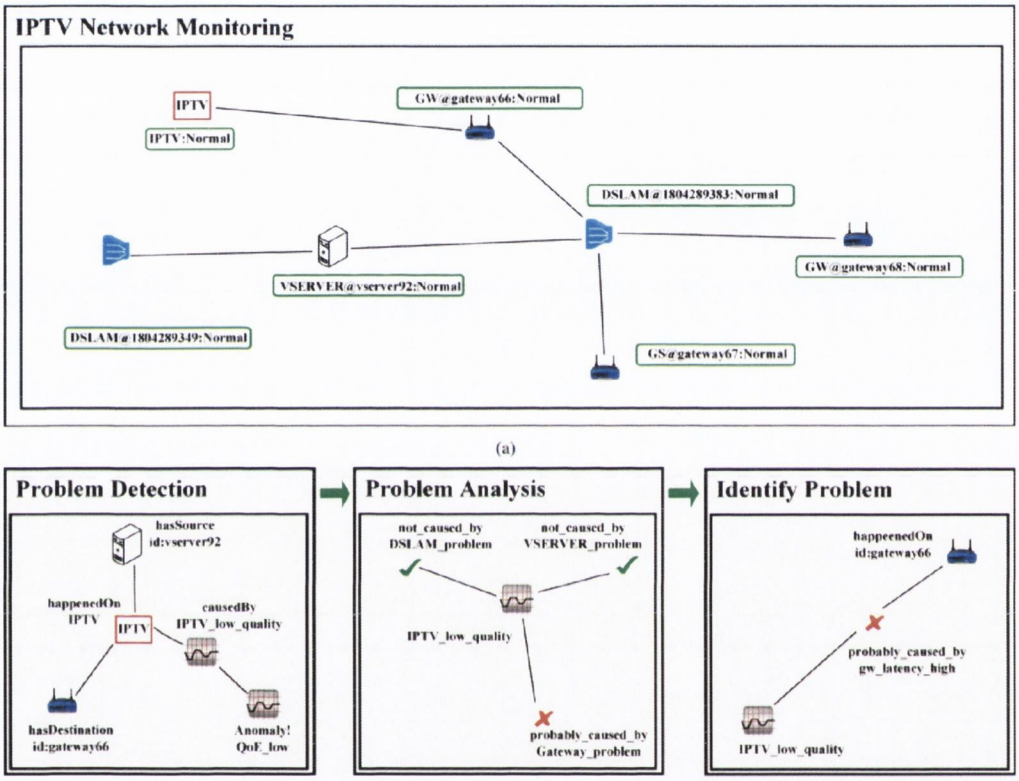



Figure 5-8 Illustration of Analysis Process in Scenario 1

Detection: The uplift engine receives metrics from the network nodes to detect if the customer is receiving poor quality of IPTV service. Poor QoS may be attributed to packet loss, excessive latency, higher jitter, or low video access rates, each of which may affect the QoE of the IPTV consumers. In this particular scenario, a threshold is exceeded and the "IPTV low quality" event is uplifted and triggered as an anomaly event by the uplifted semantic attribute. Problem detection is illustrated in the left-most sub-figure of Fig. 8.

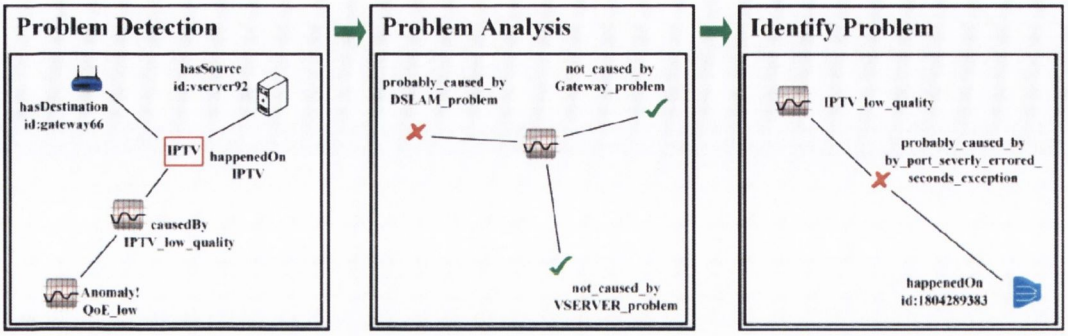
Analysis: Problem analysis is performed by tracing back along the IPTV flow's delivery route and examining the maintained events and semantic attributes in the event pool of the

relevant nodes. It is then determined if the anomaly event was triggered by the uplifted semantic attributes of any of the node in this path. In this scenario the "IPTV low quality" anomaly event was caused by a problem at the subscriber's gateway, which is indicated by a cross in the centre sub-figure of Fig. 8.

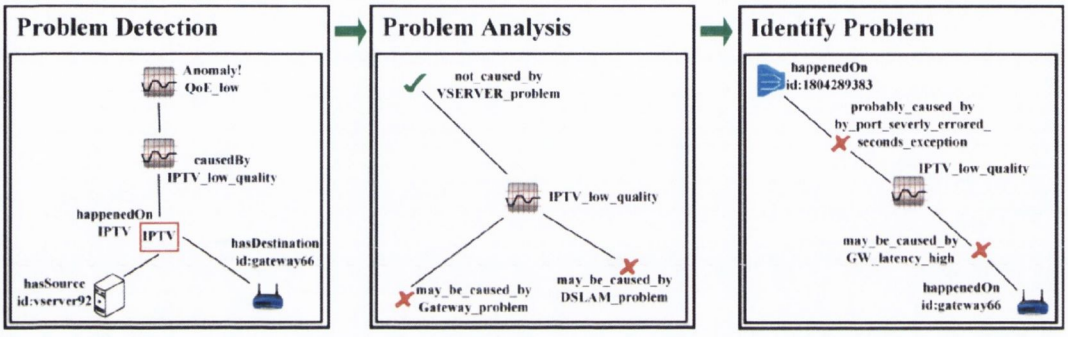
Identification: Examination of the candidate problem network node indicates that the IPTV traffic on "gateway66" is suffering from high latency (right-most sub-figure of Fig. 8). This problem is given as the most likely root-cause for the "IPTV low quality" anomaly detected above. This completes the problem drill-down process for this scenario.

Solution: The recommended ameliorative action is to push configuration changes to the network as per operational guidelines.

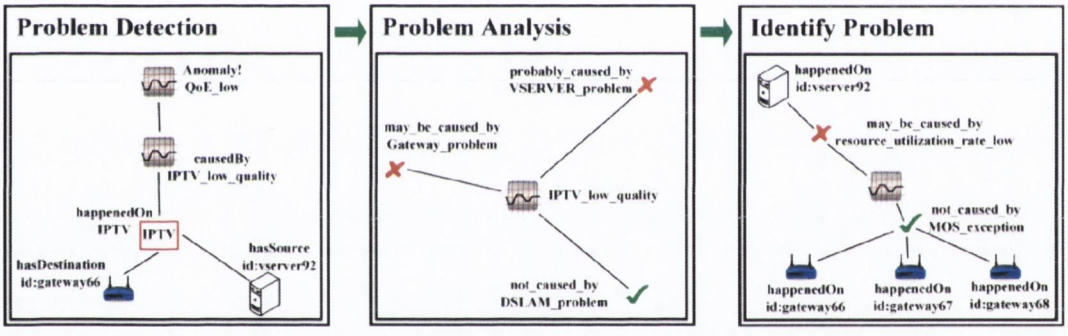
**Scenario 2**: High number of severely errored seconds at the DSLAM: In a similar fashion to Scenario 1, a simulation script is run to generate a single point of failure. The uplift engine performs its inspection procedure for each CSV entry. The problem is detected, analysed and identified and this process is visualized in the analysis panel of the visual interface in Fig. 5-9. Analysis of IPTV topology outage scenarios for single and multiple points of failure: The problem detection, analysis and identification processes are illustrated for each of the scenarios from left to right. This structured approach allows for drill-down which leads to a suggested course of remedial action.




(a) Scenario 2: Anomaly analysis performed when a high number of severely errored seconds at the DSLAM causes poor a QoE.




(b) Scenario 3: Anomaly analysis performed when a high latency and number of severely errored seconds contributes to poor QoE.




(c) Scenario 4: Anomaly analysis performed when the resource utilization rate has breached its threshold value at the Video Server causing poor QoE.

Figure 5-9 Illustration of Analysis Process in Scenario 2, 3, 4

Detection: In this scenario the IPTV flow from the DSLAM to the Gateway experiences a large number of severely errored seconds which causes the end user to experience low QoE.

The threshold associated with the number of errored seconds is exceeded and the "IPTV low quality" event is uplifted and triggered as an anomaly event by the uplifted semantic attribute.

Analysis: The detection process informs the NM that the quality decrease happened on the DSL link between between "DSLAM1804289383" to "gateway66" in the left-most panel of

Fig. 5-9(a). The information uplift engine suggests that the "IPTV low quality" anomaly event may have been caused by a problem on the DSLAM in the right-most panel of Fig. 5-9(a). Identification: Once the uplift engine has identified the source of the problem further analysis – in this case on the customer's connection between the DSLAM and their gateway– indicates that the customer is experiencing a high number of severely errored seconds in the rightmost panel of Fig. 5-9(a).

Solution: The suggested corrective action for this problem scenario is to change the DSL profile in question to a more stable profile, one that has a lower bitrate.

**Scenario 3:** High latency and high number of severely errored seconds: In this scenario, the simulation script causes two nodes to be responsible for the degradation in QoE experienced by the end users –a multi-point of failure scenario. As part of its inspection process the uplift engine notes that there are metrics in two different nodes that are reporting problems. The process of detection, analysis and identification are illustrated in the visual interface depicted in Fig. 5-9(b).

Detection: The left-most graph in Fig. 5-9(b) depicts that the IPTV flow is experiencing an "IPTV low quality" anomaly.

Analysis: We assume a human is tasked with implementing the remedial action suggested by our monitoring system. A natural approach is to present the problem amelioration step in an order which focuses on the node which serves the greatest number of customers: in this case, this is a DSLAM. The reason for this is two-fold. Firstly, the DSLAM serves a greater number of customers (in the range of 24 to 48 customers), whereas the gateway only serves one customer. From a service delivery (and financial) point of view, priority should be given to the problem which has the potential to affect the greatest number of customers. In this case the breached threshold is only localized to one single link, but it is possible to envisage a situation where a problem affects the DSLAM as a whole. Secondly, due to the direction of the flow, it could be the case that the problem in the GW is a symptom of the problem in the DSLAM; therefore solving the DSLAM issue first may in fact solve the problem in the GW without the need for further action.

Identification: Based on the high-level rules described above, our information engine prompts the NM that this problem is probably caused by the "port severely errored seconds

exception" on the DSLAM and may be caused by the "GW latency high on the gateway". The rule for probably has higher priority than may be.

Solution: The remedial action associated with this scenario prompts the NM to reconfigure the GW and DSLAM in line with their operational guidelines. Note however that the configuration for DSLAM has higher priority than the GW.

**Scenario 4**: Resource utilization rate has breached threshold at the Video Server: In this scenario, the simulation script causes one or more of the GWs to report a low QoE. In addition, the video server reports that its resource utilization rate –we think of this as the outgoing bandwidth as a percentage of its outgoing links capacity– has passed its threshold value. The problem detection, analysis and identification are illustrated in Fig. 5-9(c).

Detection: The detection process illustrates that the IPTV flow is experiencing an "IPTV low quality" anomaly.

Analysis: The uplift engine identifies the nodes responsible for this and their corresponding metrics. In this case, the MOS at the GW and resource utilisation rate at the video server are responsible. Based on this indication from the monitoring system, the order of precedence follows the ordering detailed in scenario 3: the problem in the video server is tackled first.

Identification: Even though several gateways are suffering a "MOS exception", they may not have caused the QoE anomaly to send a trigger. The "resource utilization rate low problem" on "videoserver92" may have caused the "IPTV low quality" problem. We define the semantic term "probably" has higher possibility than "maybe". This analysis is presented visually in the right-most panel of Fig. 5-9(c).

Solution: The monitoring system recommends that the NM reduce the bitrate of the videos being transmitted from the video server.

As a conclusion, CASIU is able to uplift meaningful information to support different high-level monitoring tasks. The goal of **E1.2** is fulfilled in this evaluation by four task scenarios.

### 5.5.5 Evaluation for Feasibility of CASIU (E1.4)

#### *5.5.5.1 Evaluation Goal*

The nature of network environment determines this uplift process executed in a real time,

which requires the CASIU is capable to process the real-time data input. Therefore, a trade-off exists on the balance of processing time and load. This trade-off needs to be evaluated and measured as a goal of feasibility evaluation (**FE**) to indicate the factors could affect the processing capability. The evaluation goal E1.4 is to validate to what extent CASIU is able to uplift meaningful information from heterogeneous real-time data inputs. There were two main iterative experiments for achieving this evaluation. The first looked at the approach implemented in the CASIU prototype for HAN monitoring, where the information uplift process through multiple data sources, was appropriate from a technical perspective. The second one aims was to get qualitative measure as to what extent CASIU is able to support real-time data input and the effect from the amount of knowledge models to the information uplift approach. By showing this, the data from experiment 4 (**Exp 4**) was collected to support this evaluation, in which there are more complex data input and sufficient knowledge modelling.

#### *5.5.5.2 Evaluation Settings*

This evaluation involved the use of IPTV delivery network test-bed setup in Section 5.4.2.2. The physical network structure communicated to CASIU by passing log reports in accordance with CASIU's API, and there were no restrictions placed on the design of the log reports. The establishment of a Home Area Network and IPTV delivery network test bed enabled a consolidated evaluation across the emulated data stream defined by domain expert in order to validate the design and implementation of uplifting meaningful information from heterogeneous real-time data inputs. As described in Chapter 3, the domain knowledge model is important for this information uplifting process.

We emulated a network test-bed where an anomaly or problem has occurred when an IPTV subscriber is experiencing a low QoE. Specifically the issue is due to fluctuations in the IPTV flow, which is caused by network traffic overload on one DSLAM. The topology in Section 5.4.2.2 is used to generate the problem scenarios. We emulate an IPTV delivery network with a video server and two DSLAMs, which are created using NS-3 models. The HAN test bed is physically established on three wireless connected laptops, one as a gateway and the other two as home devices. Each node in the network collects their respective metrics and generates metric CSV files. Our information uplift engines are deployed on two servers: one has CPU E8400, 4GB memory for home network processing; the other has CPU i7, 4GB memory for IPTV delivery network processing. The uplifted information is maintained as RDF triples in MySQL databases. The Semantic entity schema is stored in an eXist XML database and domain

ontologies are encoded as discrete OWL files.

#### *5.5.5.3 Evaluation Results*

The semantic attributes in this evaluation are hand-crafted by experts and not automatically extracted from datasets, so it is important to allow them to be efficiently created by non-technical experts. Hence SABer was used directly to support this. From its evaluation it was concluded that SABer (Fig. 5-10) is a tool with good usability and that domain experts without a computer science or information modelling background could use it to create semantic attributes with a minimal amount of training. The significance of this is that it should be possible for experts in metadata rich domains, such as home area networks, to capture domain expertise as semantic attributes if given a sufficient choice of elements. This means that applications get the benefit of accurate human-created semantic attributes without the cost of a lot of manual effort.

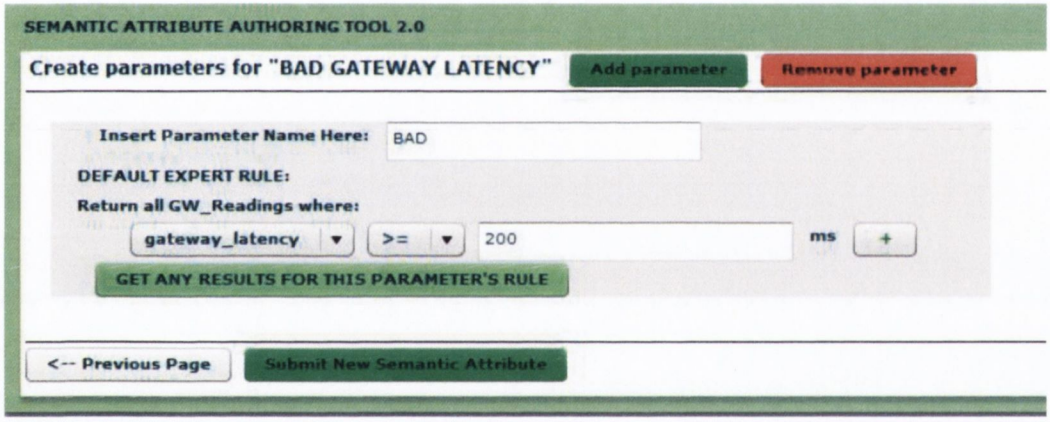



Figure 5-10 SABer: Semantic Attribute Authoring Tool

The design of CASIU has also been prototyped on both HAN and IPTV test-bed. As shown in Table 5-10, the evaluation result in Section 5.4.3 revealed a limitation of CASIU's effectiveness with decreasing correction rate. This evaluation will focus on this issue and validate the feasibility of CASIU to uplift meaningful information from heterogeneous real-time data inputs.

In this evaluation, the uplifted semantic entities are maintained in a MySQL database. This evaluation used around 100 expert defined semantic attributes and semantic segments as described in Section 5.4.3. After 3 hours data collection on the IPTV test-bed, we observed the resource model of each network node has average 20 related semantic entities and the number

of stored semantic entities is mainly affected by three reasons: the scale of domain knowledge models, the length of the historical tracing window, and the amount of network nodes and services.

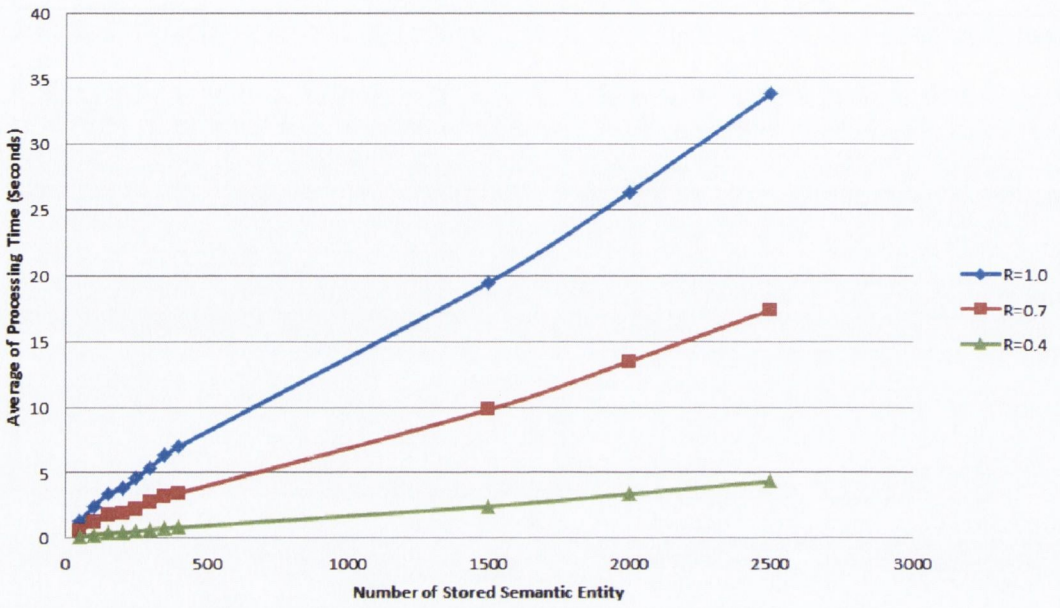



Figure 5-11 Average Processing Time based on Number of Stored Semantic Entities

We intend to establish how the processing time grows with the scale of semantic entities maintained in the entity pool. Moreover, we discovered that the rate ($R=N_{SS}/N_{SA}$) between the number of semantic segments and semantic attributes also affects the processing speed. According to the experiment result (Fig. 5-11), balancing the rate R is an effective way to improve the performance, and we set the time interval for looping the inspection process for the entity pool at 10 seconds, which are sufficient for the network scalability in this test environment. There is also a trade-off between processing speed and the functionality of CASIU, which is discussed in following sections. But in this discussion, we consider the functionality of CASIU remains in the same level.

### 5.5.6 Evaluation for Performance of CASIU (E1.5)

#### *5.5.6.1 Evaluation Goal*

CASIU was implemented as a prototype system that embodied the *knowledge-driven information uplift approach* that was outlined in chapter 3. As has already been highlighted in this chapter, this prototype has been successfully used with different applications in

different network monitoring scenarios. However, as a data processing engine it was necessary to quantify how much overhead CASIU added in terms of overall query latencies in network monitoring systems. A data processing engine should be as efficient as is possible, thus by quantifying its overhead it helps show under what circumstances the current prototype of CASIU is a usable system. By detailing such overheads it also makes clear whether these costs are outweighed by the benefits that CASIU's features network monitoring systems. One common concern for semantic-based approach CASIU adapted is its performance. Thus, this evaluation aims to satisfy the Goal of **PE** outlined in Section 5.2. It must be stressed that the particular implementation of CASIU evaluated is only a prototype system, hence this performance evaluation focussed on its core feature (information uplifting). The three main aims of this experiment were thus:

- Demonstrate that the speed in generating semantic information representations of the same size with dependencies of the formatting, type and size of source being accessed.

- Show that semantic processing time within CASIU, apart from that taken to generate uplifted information, is flexible depending on the size of information model and semantic processing approaches.

#### *5.5.6.2 Evaluation Settings*

CASIU is an information uplift engine and so does not store data directly, but rather consume individual data sources and uplifts the results. Hence the length of time for an uplift process to be returned to a network monitoring system is very dependent on the location and type of data being accessed. For instance, issues such as the network quality between CASIU and the different data sources, the load on these repositories when the queries are being sent, and the size and optimisation of these individual sources, will have a huge effect on query latencies. As these factors vary hugely and are independent of CASIU itself, this experiment focuses on measuring the overhead of the processing that can be attributed to operations within CASIU. The length of time that data sources spend processing is unaffected whether they are queried directly by a client application without using CASIU, so it is the overhead added by CASIU that is of most relevance to this thesis.

Three different data sources for this experiment were selected as representative instances of the types of data sources that CASIU can access. The three sources were generated and collected from respectively, as well as having a similar (or larger size) than the datasets previously accessed by CASIU.

- A local log report generated from the HAN test bed contains 30 minutes log data from 4 devices (one router and three laptops) and 3 services. Data is collected and wrote into the log report every 2s in a CSV format.

- The stream log collected remotely from the IPTV test bed contains 30 minutes log data from 13 devices (one video server, four core routers, two DSLAMs and six routers) and one IPTV services called from one of six routers randomly. Data is directly received through API every 2s and logged to a CSV file at the meantime.

- The big stream log collected remotely from the IPTV test bed contains 30 minutes log data from 125 devices (five video server, forty core routers with edge routers, twenty DSLAMs and sixty routers) and 20 IPTV services randomly. Data is directly received through API every 2s and logged to a CSV file in the meantime.

The CASIU engine was deployed on a PC with CPU i7 2.5GHz, 4GB memory. The uplifted information is maintained as RDF triples in MySQL databases. The Semantic entity schema is stored in an eXist XML database and domain ontologies are encoded as discrete OWL files. The Operating System installed was a 32 Bit version of Windows 7, and the log data was sent to CASIU with all times for each process logged to a millisecond precision. The times associated with CASIU's processing would of course decrease considerably if a more powerful computer or sophisticated parallel processing techniques were used. However, this experiment aimed to highlight the prototype's speed on a modest machine not optimised for performance.

#### *5.5.6.3 Evaluation Results*

According to the evaluation goal, this experiment was divided into three parts: *Speed Measurement of Information Uplift Process in CASIU, Speed Measurement of Semantic Processing in CASIU* and *Speed Measurement with Large-scale Data.*

1) *Speed Measurement of Information Uplift Process in CASIU*

In this part, a data fragment within a time period (10s equals 5 time intervals) is collected and uplifted by CASIU. The uplifted information encapsulated with semantic entities is sent to the MySQL database, in order to demonstrate that the speed in generating uplifted information was independent/dependent of some factors being accessed. Four data entities were chosen for this experiment. Because these uplifting returned result sets of a comparable size with information from 10s which is 5 time intervals, it helped to determine if results sets from data sources of a particular format took longer to process by CASIU than others. Each of these queries was sent ten times and an average length of time to generate the uplifted information was stored for each one. This allowed comparisons to be made regarding the time spent generating uplifted information of a similar size. Table 5-11 shows the specific details of each data entity.

Table 5-11 Detail of Data Entities for Speed Measurement

| **Data Entity** | **Formatting** | **Size of Data Source** | **Number of Associated Semantic Entities** | **Information Uplifting Algorithms** |
|---|---|---|---|---|
| a) Latency in Gateway Log from HAN test-bed | CSV | 216 other entities | 20 | Status Aggregation Algorithms |
| b) Latency in Gateway Log from IPTV test-bed | Streaming | 580 other entities | 20 | Status Aggregation Algorithms |
| c) Latency in Gateway Log from IPTV test-bed | CSV | 580 other entities | 20 | Status Aggregation Algorithms |
| d) Throughput in IPTV service Log from IPTV test-bed | Streaming | 580 other entities | 20 | Status Aggregation Algorithms |

| | | | | |
|---|---|---|---|---|
| e) Throughput in IPTV service Log from IPTV test-bed | Streaming | 580 other entities | 20 | Status Aggregation Algorithms & CP Detection Algorithms |
| f) Throughput in IPTV service Log from IPTV test-bed | Streaming | 580 other entities | 40 | Status Aggregation Algorithms & CP Detection Algorithms |

These data entities were processed 100 times and average results of processing time were calculated to demonstrate the differences. In order to compare these results, these entities were loaded and uplifted by the same CASIU engine deployed on the machine in Section 5.4.6.2. The speed measurement is shown in Fig 5-12.

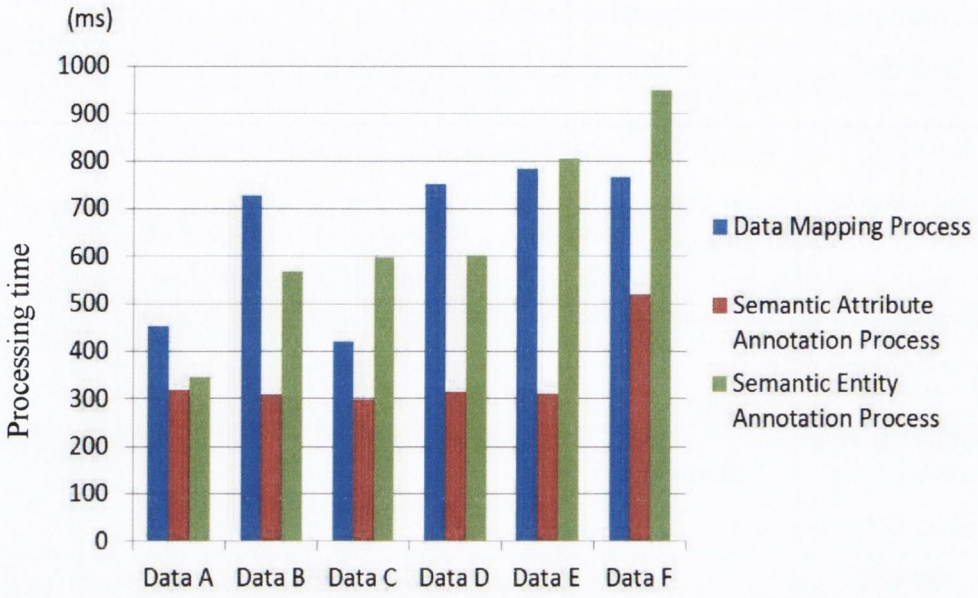



Figure 5-12 Evaluation Result of Speed Measure of Information Uplift Process

According to the evaluation result, we could get following conclusions in Table 5-12:

Table 5-12 Conclusions from Evaluation **PE**(1)

| Process | Formatting | Size of Data Source | Number of Associated Semantic Entities | Information Uplifting Algorithms |
|---|---|---|---|---|
| Data Mapping Process | Relevant | Irrelevant | Irrelevant | Irrelevant |
| Semantic Attribute Annotation Process | Irrelevant | Irrelevant | Relevant | Relevant |
| Semantic Entity Annotation Process | Irrelevant | Relevant | Relevant | Relevant |

By comparing Data A, C in CSV format and Data B, D, E, F as streaming input, we can conclude that the time of processing is relevant to the formatting of data entity for Data Mapping Process. The stream input may have extra connection cost than loading data from local log. The difference between Data F and Data A, B, C, D, E shows the number of associated semantic entities could affect the processing time of Semantic Attribute Annotation Process. Compared to Data A, the extra cost of Data B, Data C and Data D shows the size of the data source is relevant to the Semantic Entity Annotation Process. And due to the correlation event between different entities, it also related to the number of associated semantic entities. The

Data E and Data F show the difference of applied information uplifting algorithms affects both the Semantic Attribute Annotation Process and the Semantic Entity Annotation Process.

2) *Speed Measurement of Semantic Processing in CASIU*

In this part, a data fragment within one time period (1 minute equals 30 time intevials) is collected and uplifted by CASIU. The uplifted information encapsulated with semantic entities is sent to the MySQL database and then processed according to detect and analyse anomalies, in order to demonstrate that the speed in semantic processing was independent/dependent of some factors being accessed. Four data entities were chosen for this experiment. Because the semantic processing is closely relevant to the type of anomaly and its knowledge, this evaluation was not aiming to measure all types of anomalies but helped to determine what factors may affect the processing time from data sources by CASIU. Each of these queries was sent ten times and an average length of time to generate the uplifted information was stored for each one. This allowed comparisons to be made regarding the time spent generating uplifted information of a similar size. Table 5-13 shows the specific details of each anomaly.

Table 5-13 Detail of Anomalies for Speed Measurement

| Type of Anomaly | Size of Uplifted Semantic Entities | Size of Data Source | Number of Associated Semantic Segments |
|---|---|---|---|
| a)Bad Connection in HAN test bed | 352 | 216 other entities | 5 |
| b)Bad Connection in HAN test bed | 634 | 216 other entities | 5 |
| c)Bad Connection in HAN test bed | 634 | 453 other entities | 5 |
| d)Bad QoE from IPTV test-bed | 2045 | 580 other entities | 20 |
| e) Bad QoE from IPTV test-bed | 2045 | 580 other entities | 40 |

These data entities were processed 10 times and average results of processing time were calculated to demonstrate the differences. In order to compare these results, these entities were loaded and uplifted by the same CASIU engine deployed on the machine in Section 5.4.6.2. The speed measurement is showed in Fig 5-13.

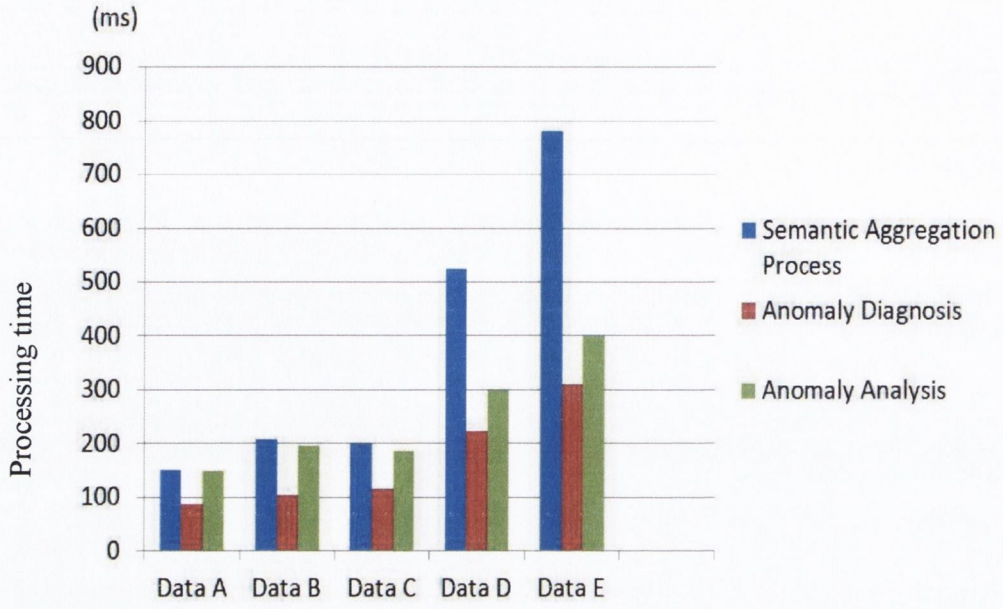



Figure 5-13 Evaluation Result of Speed Measure of Semantic Processing

According to the evaluation result, we could get following conclusions in Table 5-14:

Table 5-14 Conclusions from Evaluation **PE**(2)

| **Process** | **Size of Uplifted Semantic Entities** | **Size of Data Source** | **Number of Associated Semantic Segments** |
|---|---|---|---|
| Semantic Aggregation Process | Relevant | Irrelevant | Relevant |
| Anomaly Diagnosis | Relevant | Irrelevant | Relevant |
| Anomaly Analysis | Relevant | Irrelevant | Relevant |

By comparing Data A and Data B, C we can conclude that the time of processing is relevant to the size of uplifted semantic entities. And the difference between Data A, B, C and D, E also show us the size of associated semantic segments also affects the processing time. But the size of data source is not directly relevant to the speed of semantic processing. Due the variety of domain knowledge and the complexity of anomaly, the speed measurement for semantic processing is not stable for every circumstance, which is also limited by the result from feasibility evaluation (**FE**). So in this section, the measurement is roughly showing the relevancy with different factors, which could be used to optimize or adjust the

performance in real-world implementation.

*3) Speed Measurement with Large-scale Data*

In network systems, the performance for large-scale data set is an important factor in the evaluation of a monitoring approach. This evaluation is used to evaluate the capability of CASIU to process large amount of data with a limited hardware configuration. The evaluation uses the big stream log collected remotely from the IPTV test bed, which contains 30 minutes log data from 125 devices (five video servers, forty core routers with edge routers, twenty DSLAMs and sixty routers) and 20 IPTV services randomly. Data is directly received through the API every 10s and logged to a CSV file in the meantime. The data fragment is collected and uplifted by CASIU. The uplifted information encapsulated with semantic entities is sent to the MySQL database and then processed according to detect and analyse anomalies, in order to demonstrate that the trend of speed decreasing with the increasing amount of network resources. Because the speed itself is also closely relevant to a variety of knowledge and network topology, this evaluation was not aiming to precisely measure the speed but helped to determine what factors may be optimised to support the large scale data processing by CASIU. This evaluation is divided into two parts: the measure of speed with different network scalability and the measure of speed with different processes.

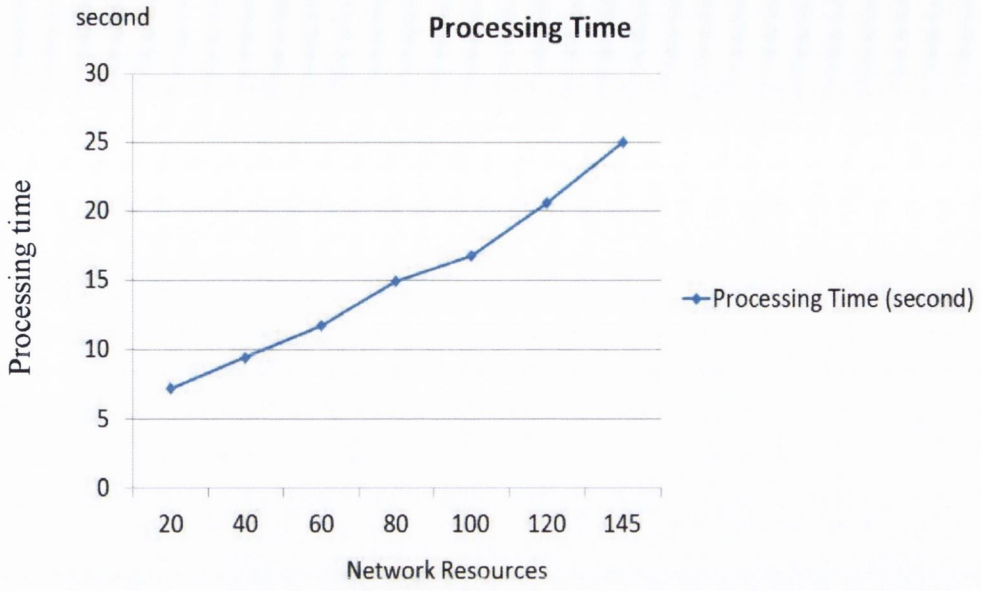



Figure 5-14 Evaluation Result of Speed Measure of Large Scale Data

As shown in Figure 5-14, the time cost for processing Large Scale Data is increasing with expanding amount of network resources. This processing time reached 24.96s for the data from 145 network resources in one time interval (10s), which may cause the decrease of process accuracy as discussed in Section 5.4.5 as the time interval is less than the processing time. This evaluation result is based on current hardware configuration, a PC with CPU i7 2.5GHz, 4GB memory. This performance could be improved by increasing the hardware configuration.

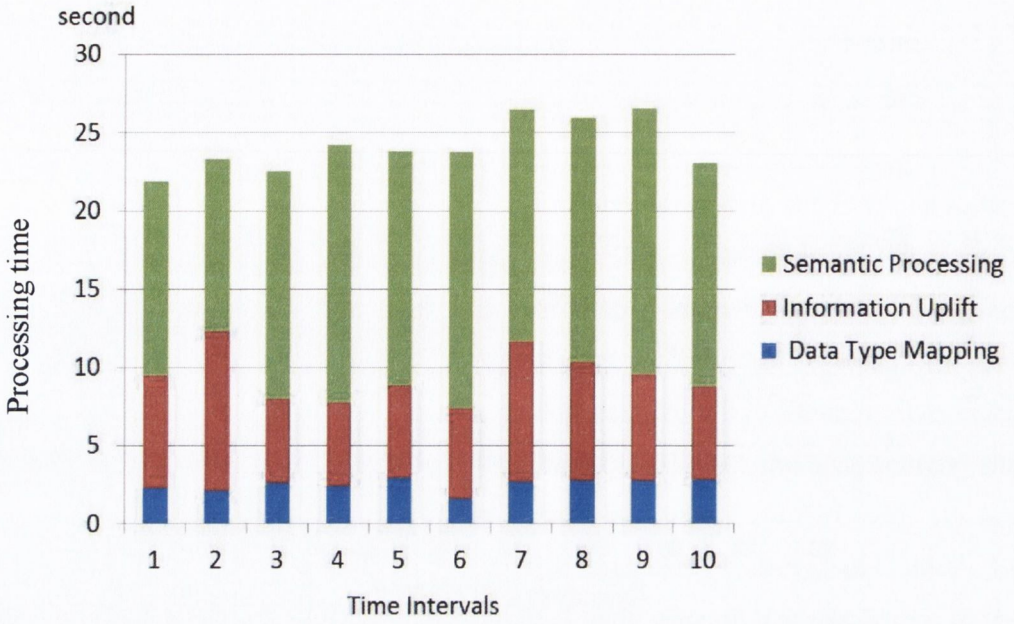



Figure 5-15 Evaluation Result of Speed Measure of Different Processes

With 145 network resources, the data in 10 time intervals were processed and the processing time (second) for each process is listed in Figure 5-15. Although the processing time is in a variety of different time interval, the cost of semantic processing is still more than information uplift and data type mapping process. By analyzing the log details, the major reason is the frequent interaction with MySQL database to retrieve temporal maintained events, which cost 76% of processing time in semantic processing and 56.7% in information uplift process. This could be improved by optimizing database or using in-memory database instead.

This section concludes the correlation and affection of different factors to influent the performance. Several new solutions could be considered to apply them here.

- Use parallel processing with distributed infrastructure.
- .Choose faster algorithms in particular business domain

- Optimize the reasoner of the system

However, the investigation on these topics is out of the scope if this research. CASIU also demonstrates how the semantic information could benefit the network monitoring with different data setups and also different applications.s

## 5.6 *Evaluation for Network Monitoring Framework (E3)*

### 5.6.1 Introduction

This section describes the iterative evaluation to validate if the design and implementation of CasiuVis is able to support non-expert users in understanding and monitoring network systems in different scenarios (**E3**). This evaluation also validates if the design requirement **R3** has been fulfilled to achieve the research objective 4 **(Objective 4)** derived from the research question in Section 1.2. As discussed in Section 5.2, this evaluation goal could be divided into two subordinate evaluation goals (**E3.1** and **E3.2**) approached through an evolving experimental process (Chapter 4). **E3.1** is a functionality evaluation to validate if CasiuVis is able to support non-expert users in both HAN and IPTV scenarios. **E3.2** is focusing on usability evaluation with a series of user trails and questionnaires for different user groups. The evaluation goal, evaluation setting and evaluation result of each subordinate evaluation goal will be detailed described in following sections.

### 5.6.2 Evaluation for Different Monitoring Scenario

#### *5.6.2.1 Evaluation Goal*

By the influences of state of the art, the information uplift approach needs to support non-expert users to leverage accurate and complete conceptual network information to achieve the monitoring purposes in diverse network environments. Due to this requirement, CasiuVis framework needs to be validated to support the information uplift approach with corresponding information representations to fit into diverse network environments (**E3.1**). The evaluation results in previous sections are to

validate to what extent CASIU is able to uplift the meaningful information in real-time, which is grounding to support non-expert users in understanding and monitoring complex network systems. As a key finding for non-expert network users, the visual representation of network information is required to improve visibility of network systems, which is still challenged by the usability and representations for high-level monitoring objectives. The first goal of evaluating the design and implementation in the CasiuVis prototypes within two evolving experiments for HAN and IPTV delivery network monitoring was appropriate from a functionality perspective. Specifically this functionality was enabling users to get involved in approaching real-world monitoring tasks. By showing this, it would support the hypothesis that CasiuVis could assist non-expert users to achieve monitoring tasks without help from providers.

#### *5.6.2.2 Evaluation Setting*

This evaluation involved the use of test-beds setup in Section 5.4.2.2, which provides a HAN test-bed and also an IPTV delivery network test-bed. The CasiuVis is integrated with these test-beds and deployed on a PC with CPU i7 2.5GHz, 4GB memory.

As shown in Figure 5-16, two groups of participants each were assembled (one group expert user and the other non-expert), with each person engaging in the experiment separately and in isolation from other participants. In the HAN experiment (**Exp2**), nineteen of the participants were non-expert users with no or basic HAN usage experience and five were experts with at least five years' experience on network monitoring/management. In the IPTV experiment (**Exp3**), ten of the participants were non-expert users who are network administrators or engineers with less than 5 years' experience and the other five were considered as expert users who are senior architects or researchers with expertise on different network monitoring/management areas. An entire session including the demonstration, performance of tasks and filling in of questionnaires typically took

around forty minutes to complete. The first step of the experiment consisted of a demonstration of how to use CasiuVis to monitor a network with a sample task. This demonstration was done by the evaluator who uses CasiuVis to explore, diagnose, and analyse a network anomaly happening in real time. Then three tasks in HAN and four tasks in IPTV delivery network involved an identical process to that which the participants would undertake in the experiment. Each of these tasks demonstrated to the participants involved a combination of a different real-world monitoring scenario.

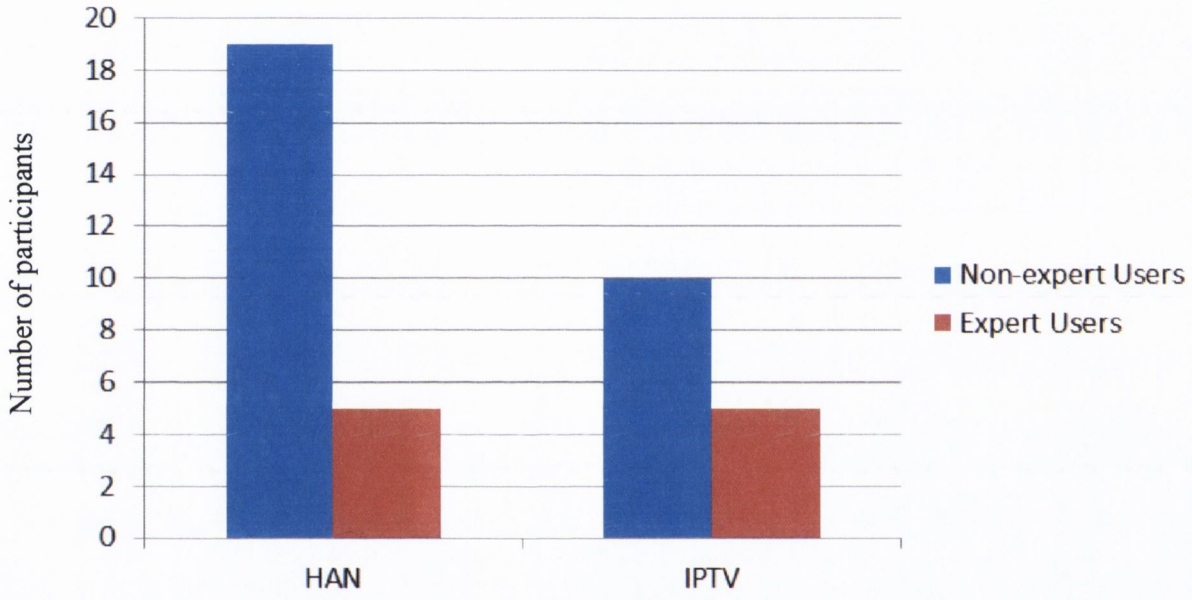



Figure 5-16 User Groups in Two Monitoring Scenarios

These tasks were presented to the participants in a random order. This is because users tend to get quicker with later tasks when they are more familiar with the application interface. After these tasks, participants are asked to finish a questionnaire which will be analysed in next section as a part of usability evaluation. The tasks presented to the user are listed as follows:

In Experiment 2 (**Exp2**), these tasks were designed based on different types of event in HAN use case:

Table 5-15 Event Table for Evaluation

| **Type of Network Event** | **Encoding Type** | **Example** |
|---|---|---|
| Composed Event on One Domain | Semantic Segment | "GW_Status_Bad" |
| Composed Event on Multi-domain | Semantic Segment | "QoE_Low" |
| Composed Temporal Event on One Domain | Semantic Segment with Temporal Operator | "Connection_Congestion" |
| Composed Temporal Event on Multi-domain | Semantic Segment with Temporal Operator | "Network_Congestion" |

- **Scenario 1**: Laptop connection bad caused by antenna interference (Single event on one domain)
- **Scenario 2**: VoIP service low quality caused by antenna interference (Single event on multi-domain)
- **Scenario 3**: VoIP service and IPTV service low quality caused by heavy uploading on another machine at the same time (Multi-event on multi-domain with temporal reasoning)

In Experiment 3 (**Exp3**), these tasks were also designed based on different types of event. Details of these scenarios were introduced in Section 5.4.4.2:

- **Scenario 1**: Excessively high latency at the GW causes poor QoE (Single event on multi-domain at end-point of this network)

- **Scenario 2**: A high number of severely errored seconds at the DSLAM causes poor QoE.(Single event on multi-domain with temporal reasoning)

- **Scenario 3**: A high latency and high number of severely errored seconds are contributed to poor QoE (Multi- event on multi-domain with temporal reasoning)

- **Scenario 4**: The resource utilization rate breaches a threshold at the Video Server which causes poor QoE (Single event on multi-domain at start-point of this network)

#### *5.6.2.3 Evaluation Result*

In the thesis, the human factors involved are every bit as important as traditional software engineering measures. As part of the evaluation of the CasiuVis framework, a prototype was developed and deployed and a detailed user study undertaken in two different real-world monitoring scenarios. During the evaluation procedure, participants were divided into two groups:

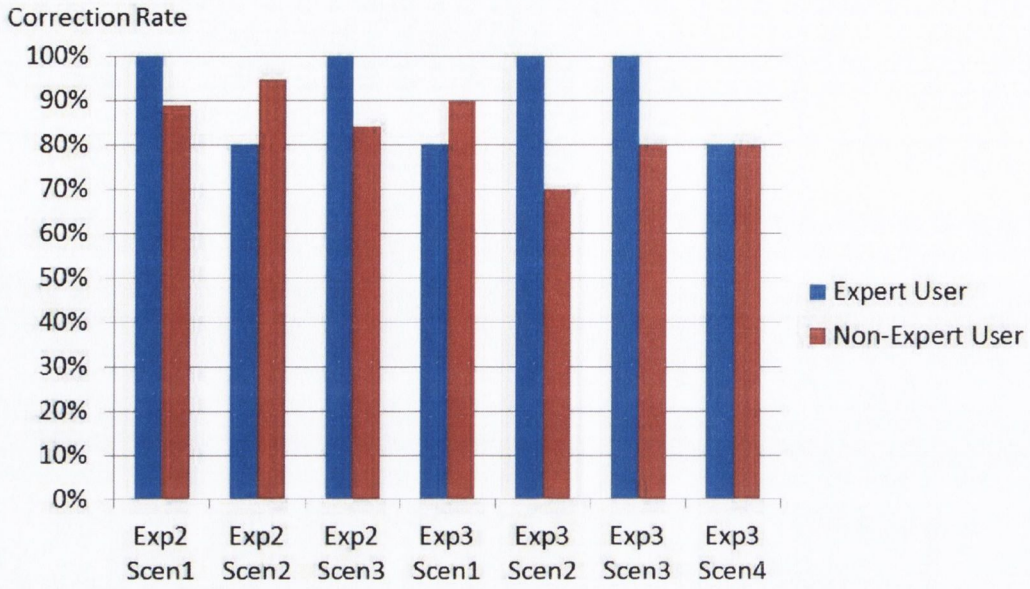



Figure 5-17 Evaluation result on **E3.1**

Overall the results indicate that in its current prototype state our system is suitable for varied monitoring tasks in several different scenarios. All tasks even with different complexities were well-performed in both expert user and non-expert user groups. Most tasks have more than 80% correction rate. Moreover, nearly all participants agree that this network monitoring tool is usable and easy to learn with information visualization techniques we adopted. This result also indicates non-expert users are able to monitor their network without support from domain expert by using our system and they could achieve similar correction rate with domain experts. This evaluation could validate our CaisuVis is able to support non-expert users to perform monitoring tasks in different network scenarios.

### 5.6.3 Evaluation for Usability

#### *5.6.3.1 Evaluation Goal*

For CasiuVis to be applicable to many domains it needs to be shown that non-expert users can successfully achieve monitoring tasks in different domains without

usability boundaries. As stated previously, for the purposes of this thesis 'non-expert' people refers to computer literate participants with basic skills such as operating Internet browsers, but with no network monitoring experience. Likewise, this experiment considered those participants with decent network expertise to be expert users. Section 5.5.2 described both expert and non-expert users can use CasiuVis to achieve monitoring tasks, which demonstrates the effectiveness of our system. The goal of this evaluation more focuses on measuring and validating the usability of CasiuVis. Furthermore, this evaluation helps explore whether CasiuVis with embedded information representations is sufficiently abstract to distance the user from the differences in the various monitoring tasks and their underlying information. By the influences of state of the art, non-expert users can understand complex network information with appropriate usability (**E3.2**). As a key finding for non-expert network users, the visual representation of network information is required to improve visibility of network systems, which is still challenged by the usability and representations for high-level monitoring information. From the usability perspective, this evaluation addresses the requirement for the monitoring framework to visually represent high-level monitoring information for non-expert users.

#### *5.6.3.2 Evaluation Setting*

During the procedure of this evaluation, participants were divided into two groups, non-expert user and expert, based on different network knowledge background, and they will be invited to use this system for three different tasks in HAN experiment (**Exp2**) and four tasks in IPTV experiment (**Exp3**) as described in Section 5.5.2. These participants were also asked to complete a questionnaire on the functionality, effectiveness, efficiency, usability, user-interface, and limitations of CasiuVis (Appendix I, II, and III).

Some questions were presented in a SUS based questionnaire, followed by statements which participants can rate on a Likert scale: Strongly Agree, Agree,

Disagree, Strongly Disagree, for qualitative analysis. Participants were also encouraged to provide qualitative feedback on the different tasks, to enable the gathering of data for analysis which has not been collected for quantitative analysis.

Table 5-16 Experiment Target Group for Usability Evaluation **E3.2**

| **Experiment Target Group** | **Participants** | **Exclusion/inclusion criteria** |
|---|---|---|
| Non-expert User Group in HAN (19 participants) | 12 Students in Trinity College Dublin (5 female, 7 male)<br>7 Residents in Dublin (2 female, 5 male) | The opinions of all members of this group were encouraged and appreciated as part of this study. |
| Expert Group in HAN (5 participants) | 2 Academics in Trinity College Dublin (2 male)<br>3 Academics in University College Dublin (1 female, 2 male) | The opinions of academics were appreciated for two reasons:<br>a) possible experience of using network monitoring systems<br>b) background in home area network and familiar with the network monitoring data |

| | | |
|---|---|---|
| Non-expert User Group in IPTV (10 participants) | 2 Ph.D. Students in Trinity College Dublin (2 male)<br>5 students in University College Dublin (2 female, 3 male)<br>1 network engineer in IBM Tivoli (1 male)<br>2 network engineer in Ericson (2 male) | The opinions of all members of this group were encouraged and appreciated as they have some background knowledge about IPTV network but not sufficient to perform QoE-based monitoring on large scale network. |
| Expert Group in IPTV (5 participants) | 1 System Architect in IBM Tivoli (1 male)<br>1 professor in University College Dublin (1 male)<br>1 senior researcher in University College Dublin (1 male)<br>1 senior researcher in Waterford Institute of Technology (1 male)<br>1 professor in Trinity College Dublin (1 male) | The opinions of senior academics and architect were appreciated for three reasons:<br>a) experience of using network monitoring systems<br>b) expertise in IPTV delivery network and familiar with the network monitoring data |

#### *5.6.3.3 Evaluation Result*

During the evaluation procedure, users were invited to use CasiuVis to perform monitoring tasks and then gave feedback on the system using a standardized usability scale (SUS) questionnaire, detailed subjective feedback and monitoring of the effectiveness of their performance of the tasks.

The evaluation results are calculated based on satisfaction rate and classified according to the following aspects: ease of use is evaluated by the standard SUS-based usability questionnaire; UI design is based on the mean user-specified subjective marks; the functionality metric is based on the mean subjective feedback from non-expert users on whether they are satisfied with the current functions; finally expertise support is based on the mean subjective evaluation by provided domain knowledge support within CasiuVis.

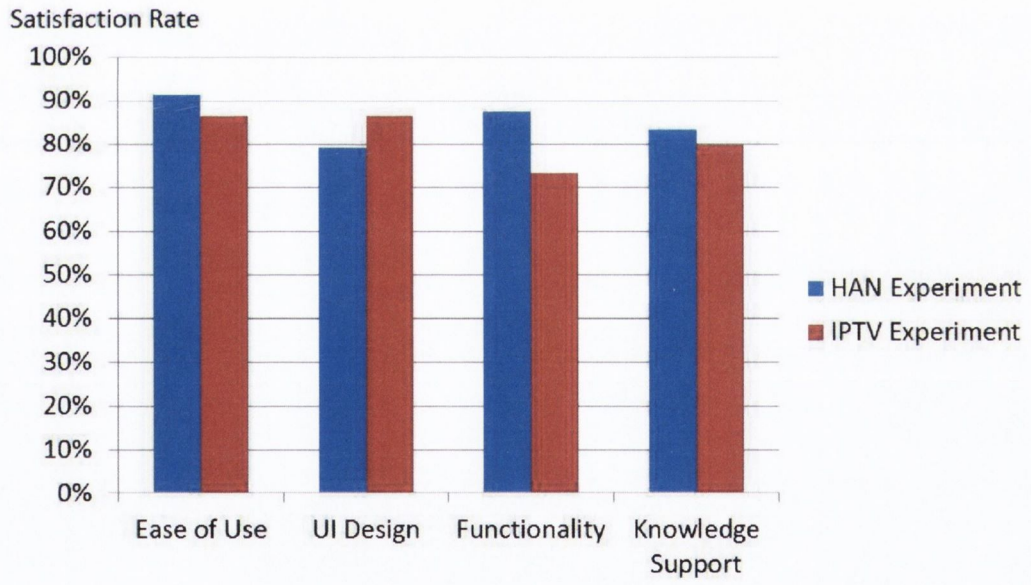



Figure 5-18 Statisfaction Rate of Usability Evaluation

According to the evaluation results, it can be seen that the system scored highly in evaluated aspects. However the weakest area, at 73%, was the IPTV functional satisfaction rate. Two users in IPTV experiments stated that the UI of our prototype needs more explanations in the manual as too many technical terms in the chart. Nonetheless this is respectable and overall the results indicate that in its current prototype state our system is suitable for varied monitoring tasks in several different scenarios. Moreover, nearly all participants agree that this network monitoring tool is easy to learn and easy to use with novel semantic visualization widgets and especially for the large scale network. There were some complaints about the confusion of text annotation on the visual widgets, but they are still acceptable for most users. More than 80% of users agree the domain knowledge embedded in CasiuVis is able to help them understand complex network issues and even for expert users, it is still useful to correlate information from different domains.

## 5.7 *Comparison with Existing Systems*

This analysis is performed according to a comparison of selected five innovative network monitoring systems for non-expert users to partly fulfil the remaining challenges addressed in Section 2.4 for non-expert users. Then an analysis is performed after the comparison table to point out the key findings and compare to CASIU and CasiuVis.

Table 5-17 Comparison of existing Tools with CASIU and CasiuVis

| | **Network Magic** | **ISI Framework** | **Eden** | **Homework Project** | **Netcool** | **CASIU with CasiuVis** |
|---|---|---|---|---|---|---|
| Complete Conceptual Model (C1) | Limited Support with network traffics | Well Support with comprehensive data model | Well Support with Spatial + Logical models | Well Support with comprehensive data model | Well Support with traffic protocols and services | Well Support with comprehensive data model |
| Difficulties for Creating and Updating Information Representations (C2) | No Support | Limited Support with independent semantic models | Limited Support with independent models | Limited Support with independent models | Limited Support with independent models | Well Support to model domain expertise from knowledge capturing tools |
| High-level Monitoring Information Representation (C3) | Little Support with network status | Well Support with higher level abstraction | Little Support with network status | Little Support with network status | Little Support with network status | Well Support with higher level insights |

| | | | | | | |
|---|---|---|---|---|---|---|
| Cross-domain Monitoring Information Representation (C4) | No Support | No Support | No Support | No Support | Limited Support with indenpended models | Well Support information from different network/knowledge domain |
| Degree of Autonomy (C5) | Little Support with embedded logic | Well Support with expert knowledge input but hard to capture | Little Support without knowledge input | Well Support with expert knowledge input but hard to capture | Well Support with expert knowledge input but hard to capture | Well Support |
| Drill-down Analysis (C6) | Little Support with pre-defined suggestion | Little Support with human judgement | No Support | No Support | Little Support with human judgement | Well Support |

| | | | | | | |
|---|---|---|---|---|---|---|
| Visual Representation to Improve Usability (C7) | Average Support to the non-expert users | Little Support to the non-expert users | Average Support to the non-expert users | Well Support to the non-expert users | Little Support to the non-expert users | Well support for non-expert users |
| Visual Representation of High-level Monitoring Information (C8) | Little Support with only network status | Average Support with some degree of knowledge required | Little Support with only network status | Little Support with only network status | Average Support with some degree of knowledge required | Well support for non-expert users |

Although the tools introduced above have different academic and commercial focuses, their work showed that information modelling, information visualisation, and knowledge-driven analytic approaches can be effective when used together to assist non-expert users in coping with diverse network monitoring tasks. CASIU and CasiuVis addressed all these challenges.

From this comparison, it is obvious that the common information model is a common solution for modelling heterogeneous network components. The information plane in Eden and Homework project and the novel semantic model in ISI framework all support a comprehensive description of heterogeneous network resources and they are also extensible to support new protocols, metrics and other network resources. From the comparison, the knowledge input is necessary to ensure

the system flexibility for the network environments. Even these modelling approaches all provide a formal syntax, but network domain experts normally are not policy/semantic experts, which brings encoding difficulties for network domain experts to create and update these models. CASIU provides comprehensive information representations as a common model to enable the description of knowledge and information to understand each other, share meaning and support knowledge-based reasoning.

As discussed in Section 2.4, high-level information is important for non-expert to monitor network status and understand the networking problems. Most current systems still focus on presenting the network status, which is no longer sufficient to establish enough understanding for non-experts. ISI framework presents an effective semantic approach to model the higher-level meaning of network behaviour from low-level network resources models. This high-level abstraction modelling is not well-supported by current common information models [CIM 2004] [SID 2005] [Strassner 2002]. And most systems lack the support to cross-domain modelling for network resources. Only Netcool provides the models for the cross-domain network resources, like revenue, geo-location, user experience, etc., but these models still indented to each other, which is hard to be correlated to expose the inherent relationships from these network resources. The comprehensive representation CASIU provided is able to bridge the mode model from network resources in different domains as demonstrated in Section 5.4.3.

Expert knowledge is often required for diagnosis, analysis, and overcoming network problems. From the comparison of these systems, all tools can utilise and model some degree of domain knowledge and it is proven effective for the network troubleshooting. It is obvious that the degree of imported domain knowledge is crucial to promise the level of intelligence and autonomy of the monitoring process, which is especially important for non-expert users. The knowledge models in ISI framework, Homework, and Netcool provide a more flexible way to ensure the

intelligence and autonomy. And some of them support the drill-down analysis, but it still need the user to analyse the root-cause reason by themselves, which is not appropriate for non-expert users. By using the information representations, CASIU supports a knowledge-driven way to diagnose and analyse root-causes by approaching semantic processing.

These systems show the existing visual dashboard can improve the understanding of non-experts users with low learning barrier. In addition, Homework provides comic style interfaces for non-experts to define their own rules, which expose the usability that is crucial for non-expert users. How to visually present the high-level monitoring information to non-expert user is still a challenge. The ISI project and Netcool system made some attempts from different ways: ISI project provides a multi-resolution display to the information in different abstraction level and Netcool supports different visual views for the information in different domain. CasiuVis is adaptable for a range of meaningful and user-friendly visual widgets to enable non-expert users in understanding and monitoring network systems, as shown in our user trails in Section 5.4.7.This section compared the five high impact systems analysed in Chapter 2 with CASIU and CasiuVis to clarify how our information uplift approach fulfil the challenges for non-expert users exposed in Chapter 2. These findings highlight the remaining challenges for non-experts and expose some technical findings, which are all addressed in this research. This close coupling of design and implementation means that the successful evaluation described in this chapter also helps to validate the usefulness of the underlying approach and its framework and models.

## 5.8 *Evaluation Analysis*

The aims of this chapter were to show how the research question is fulfilled from evaluations on the design and implementations of both CASIU and CasiuVis, as well as to provide further evidence that the research objectives were being supported by evaluations in Table 5-1. It depicts the relationships that exist from this

thesis' research question down to the individual evaluation goal. It shows how the evaluation that was looked for in the various experiments stemmed directly from research objectives, and ultimately the research question. This section aims to analyse these evaluation results from previous sections to illustrate how the research question is fulfilled and expose existing limitations.

### 5.8.1 Analysis of Evaluation Results

The main aim of our research is to support non-expert users in understanding and monitoring network systems. Hence, CASIU with its monitoring framework CasiuVis and corresponding information representations was evaluated to validate if the design requirements have been fulfilled in an iterative prototyping process. The evidence of this hypothesis is supported by a series of evaluation results.

This evaluation (**E1**) fulfills the design **Requirement R1** which states that CASIU must be designed to uplift meaningful information from real time data by leveraging domain expert knowledge. **E1** consists of a series of evaluations to validate if the design and implementation of CASIU is able to fulfil **Objective 2**. Therefore, the goal of functional evaluation **E1.1** is to validate to what extent CASIU is able to consume heterogeneous real-time data input. From the evaluation result in Section 5.4.2, most events were correctly uplifted and correlated to network resources. The goal of **E1.1** is fulfilled by examining the topology structure of uplifted information and comparing the result sets in both HAN and IPTV monitoring scenario. Hence, the design requirement is also fulfilled by the prototypes in **Exp2** & **Exp4**. CASIU is also designed to uplift meaningful information from the real-time data input (**R1.2**). **E1.2** aims to validate if CASIU is able to extract meaningful information from real-time data input from a functional point of view. This goal is fulfilled by the evaluation result in Section 5.4.3, which validated CASIU is able to uplift the information from single data source with 100% correction rate in **Exp1** and the result in **Exp2** also showed good correction rate and CASIU was further validated with large amount of information from multiple data

sources in **Exp4**, which showed a significant decrease of correction rate. This drawback indicates there is limitation on CASIU engine. These limitations will be further examined and analysed in the feasibility **(FE)** and performance evaluation (**PE**). CAISU is designed to leverage domain knowledge to enable information uplifting to support higher-level monitoring objectives (**R1.3**). The goal of evaluation goal **E1.3** is to validate to what extent CASIU is able to fulfil this requirement. As the result shown in Section 5.4.4, four complex monitoring tasks were performed in IPTV experiment to demonstrate the capability of CASIU to support higher-level monitoring objectives, especially the drill-down analysis and automatic analysis capability, which meets the research challenges in Chapter 2. CASIU is designed for real time processing. Therefore, a trade-off exists on the balance of processing time and load. This trade-off needs to be evaluated and measured as a goal of feasibility evaluation (**FE**). The evaluation result in Section 5.4.5 indicates the boundary and factors that could affect or limit the processing capabilities, which could be reduced by better hardware performance. It is also prudent to evaluate the performance of CASIU in order to help quantify to what extent it increases process latencies. This procedure can be summarised as a performance evaluation (**PE**) to measure its performance in three aspects. As the result exposed in Section 5.4.6, the performance of each process in CASIU was analysed and it is also acceptable to process large-scale real time data set. This analysis indicates how to adjust its performance to fit into different network monitoring scenarios. As a conclusion, the design requirement **R1** and research objective 2 is validated through evaluation **E1**.

Design requirement **R2** is evaluated by **E2**, which is based on the evaluation result from other evaluations, which validate the information representation could support multi-data input, diverse domain expertise, and also enable the information uplift approach. The information representation for **R2.1** was used in **E1.1**, which correctly represented the information from heterogeneous data input resources. The cross-domain knowledge representation **R2.2** has been adopted in **E1.2**, **E1.3** and

**E3.1**, which supports monitoring tasks in different domain. The representation of high-level information was validated in **E1.3** and has been validated to fulfill **R2.3** with comprehensive representations of network information from low-level to high-level. A comprehensive encoding for the domain expert's insights **R2.4** was applied in **E3.1** to demonstrate how this captured and modeled expertise could help non-expert users solve complex monitoring tasks. As a conclusion, the design requirement **R2** and research objective 3 is validated through evaluation **E2**.

Due to the requirement **R3.1**, CasiuVis framework needs to be validated to support the information uplift approach with corresponding information representations to fit into diverse network environments (**E3.1**). With the result in Section 5.5.2, CasiuVIs could help both expert users and non-expert users to perform network monitoring tasks. The non-expert users are able to achieve the similar results by using CasiuVis in different networks, which fulfilled the requirement **R3.1**. As a key finding for non-expert network users, the visual representation of network information is required to improve visibility of network systems. From the usability perspective, this evaluation result in Section 5.5.3 addresses the requirement for the monitoring framework to visually represent high-level monitoring information for non-expert users (**R3.2**). As a conclusion, the design requirement **R3** and research objective 3 is validated through evaluation **E3**.

### 5.8.2 Analysis of Limitations

The evaluation goals were put into practise in this chapter, and the evaluation findings validated the research objectives of this thesis. Meantime, the successful evaluation also helped figure out the limitations of this approach and its associated framework from different perspectives.

These experiments showed that non-expert users can benefit from leveraging expertise, but as some users indicated there is still a space to improve the usability of UI design and text annotation on the visual widgets, which was especially vital in

HAN. As the design of visual widget is beyond the scope of the research in this thesis, this limitation could be addressed by using better visual design and more user research on more detailed target user groups.

From the domain expert's perspective it was possible to see the contribution of expertise encoding throughout the various experiments. This research showed that SABer [Hampson et al 2010] was a tool with good usability, and that domain experts without a computer science background could use it to create semantic attributes with a minimal amount of training and this research also extended the knowledge representation to render more types of expertise by using SABer. Some expert users also suggested better integration with SABer to provide a one-site solution for monitoring tasks, which could be addressed in further work.

From a real-world perspective it was shown how CASIU and CasiuVis evolved over the various experiments with user feedback resulting in additional features being added over time to face the real world problems. However, as analysed in **FE** and **PE**, the performance of this approach may bring extra engineering challenges in some scenarios. Our study also indicated the factors may affect performance, which provides a way to adjust our current solution to fit into different network scenarios. The low performance of database or network connection may also result in the overall performance not being sufficient for particular scenario.

As a conclusion, the evaluations in this chapter proved the design and implementation of CASIU and CasiuVis answered the research question and fulfilled all research objectives with acceptable limitations.

## 5.9 *Conclusion*

This chapter described the overall evaluation strategy employed in this thesis, as well as detailing the various experiments involved. These evaluation studies

incorporated a variety of techniques, such as user trials, performance tests, questionnaires and scenario case study, and included experiments with CASIU and CasiuVis. An analysis of the evaluation results highlighted how the design and implementation of CASIU and CasiuVis were successful, that these systems fulfilled the research objectives outlined in Section 1.3 and that they contained a set of features that advanced the state of the art. Furthermore, their successful evaluation also helped to validate the *knowledge-driven information uplift approach* itself. The following chapter concludes this thesis by outlining the specific contributions that have been made, and by highlighting some future work that can extend this research.

# Chapter 6
# Conclusion

This chapter presents the conclusion of this thesis. Initially it states an assessment of the extent to which research objectives derived from research question in Chapter 1 have been fulfilled and then discusses the contributions that this research has made. The work in this thesis has been undertaken and evaluated in different areas, thus this chapter discusses the limitations identified by this work as well as possible future work.

## 6.1 *Achievements*

### 6.1.1 Achievements for Research Question

This thesis hypothesized that an expert knowledge-driven information uplift approach could be used to bridge the understanding gap between non-expert users and raw data for monitoring network systems. To pursue this, a research question was set out for this thesis as:

"This research asks how and to what extent domain expert knowledge may be leveraged to enable the real time uplift of meaningful information from raw data to support non-expert users in understanding and monitoring network systems?"

Five objectives were derived from this question:

- **Objective 1**: survey the state of the art of network monitoring and identify related approaches and techniques to support non-expert users and categorize them. Find out the existing similar approaches, analyze and compare them to indicate the research challenges.

- **Objective 2**: design and implement representations for domain expertise to support the knowledge-driven network monitoring.

- **Objective 3**: design and implement a knowledge-driven approach to uplift meaningful information from real time log data to support non-expert users.

- **Objective 4**: design and implement a general framework to support non-expert user to perform monitoring tasks in different network scenarios.

- **Objective 5**: follow an iterative approach to prototype, evaluate, and validate the design and implementation in different network monitoring use cases.

The design in Chapter 3 contributed an information uplift approach (CASIU) with accompanying domain knowledge models and framework to support non-expert users in understanding and monitoring network systems. This approach was implemented and embedded into a visualization framework (CasiuVis) to consume network log data from heterogeneous types of interconnected nodes and visually represent the domain knowledge driven uplifting of information to non-expert users to face the high-level network monitoring challenges from Quality of Service (QoS) and Quality of Experience (QoE) aspects. Followed by a series of experiments, this approach with its framework and knowledge models was well evaluated to fit the research challenges systematically studied from a state of the art in network monitoring and information extraction.

### 6.1.2 Achievements for Research Objectives

A state of the art in network monitoring for non-expert users and a study of information extraction approaches for stream network log data were conducted to fulfil the research ***Objective 1***. The state of the art in network monitoring was performed by surveys of traditional network monitoring systems. These surveys informed the common and diverse features of traditional network systems from a variety of functional aspects. Then a study was addressed about the information representation and visualization approaches and techniques used in network monitoring systems. The requirements for non-expert users were stated and followed by a discussion of why not traditional network monitoring tools, which are not suitable for non-expert users. This discussion also states the research challenge with a functional comparison of five monitoring systems with high impact in both academic and industrial areas. According to the research challenges addressed in the network monitoring for non-expert users, a study of mainstream information extraction approaches for stream data was performed. This study was addressed into three more focused surveys undertaken in the areas of information extraction on network stream data and knowledge-driven information extraction for high-level meanings for network information to benefit non-expert network users. The survey of information extraction on network stream data informed the design of our information uplift approach. By analysing information extraction, we investigated the benefits of domain knowledge to information extraction approach, which inspired the design of semantic information representative encoding and models. Moreover, the study of network information visualisation contributed to the design of the visual representation layer in CasiuVis framework, which proved the value of our information uplift approach for non-expert users in understanding and monitoring network systems. The surveys and studies for research ***Objective 1*** stated the related research about network monitoring and information extraction for non-expert users, which figured out the remaining research challenges and inspired the design in following research objectives.

To address the research ***Objective 2***, the semantic encodings and knowledge models were defined for domain expertise. In order to capture the domain expert's insights for network monitoring, three appropriate semantic encodings were concluded and designed: a) **Basic Semantic Attribute** is used to encode the basic concept in network domain; b) **Semantic Segment** is designed to combine several basic semantic attributes with corresponding logic to express high-level meanings; c) **Temporal Semantic Attribute** is proposed to enable the temporal reasoning capability on our information uplift approach, which is crucial for the real-time data stream. These encodings were able to be automatically captured through a visual authoring tool, which enables the knowledge capturing from network domain experts who normally lack semantic encoding capability. In addition, a cross-domain knowledge model was achieved to formally combine and model the knowledge from different network experts and then leverage this knowledge model to support network diagnosis and root-cause analysis for the network anomalies from both Quality of Service (QoS) and Quality of Experience (QoE) aspects. These semantic encodings and models enable a knowledge-based reasoning, which provides fundamental logic for the information uplift approach addressed in next research objective.

The primary objective of this thesis was to achieve the research Objective 3 to design and implement an approach to uplift meaningful information from real time raw data by leveraging the domain expert knowledge. This underlying semantic approach defined with its accompanying knowledge models, which allows the domain knowledge driven information uplifting from real-time data stream. This was achieved through the well-defined domain encoding and knowledge model in ***Objective 2***. The close coupling of the design outlined in Chapter 3 with its implementation (described in Chapter 4), meant that the successful evaluations of the Semantic Information Uplift (CASIU) engine (detailed in Chapter 5) also validated the usefulness of our approach and its accompanying domain knowledge models. The design specification outlined in Chapter 3 was influenced by Objective

1 of this thesis, which was to examine the state of the art in how knowledge driven information uplift is performed for stream network data, as well as the state of the art in both HAN and IPTV network monitoring for non-expert users.

From the analysis of deficiencies within the state of art that took place in Chapter 2, the research ***Objective 4***: design and implement a framework to generalize the knowledge driven information uplift approach for non-expert users in different network monitoring scenarios was derived for the framework which embodies the expert-supported approach to information uplifting in different network scenarios. This framework was designed in a layered structure to capsule CASIU engine and domain knowledge models in order to generally support the knowledge-driven information uplift in different network plug-ins. According to these research challenges, the CasiuVis framework was designed with a layered structure to support information uplift approach suitable for different network log inputs; knowledge-driven semantic processing to uplift meaningful information from low-level to high-level; representations and models for domain knowledge; and a set of visual widgets in visual representation layer to assist non-expert users in understanding semantic meaningful information for the network problem diagnosis, analysis, and overcoming common problems

All of these features were successfully implemented into the framework design described in Chapter 3, and the seven steps that constitute the knowledge-driven approach to data exploration were also detailed within that chapter.

The information uplift approach and its accompanying framework and models were used to underpin the technical implementations of a Semantic Information Uplift engine (CASIU) and the network monitoring framework (CasiuVis). As described in this thesis, CasiuVis was successfully deployed in two different domains (HAN and IPTV delivery network), supporting various expert knowledge domains.

Both CASIU and CasiuVis were successfully evaluated (as described in Chapter 5), which fulfilled the final **Objective 5**: define an iterative implementation and test process for the information uplift approach and its framework which supports a feedback loop to assist design refinement and perform evaluation studies of usability, feasibility and performance. The evaluation in this research was performed in three major aspects: usability, feasibility, and performance. The usability is mainly based on user-based evaluation, which was performed through questionnaires and feedback from both non-expert and expert users. This evaluation was applied on CasiuVis framework in both HAN and IPTV delivery network scenario. The feasibility is evaluated by functional comparison with existing similar systems and also the user performance through a series of functional tests. This evaluation was approached as an iterative process during four experiments, and the iterated prototype was examined against initial objectives. The performance evaluation was combined by tests from both performance and accuracy aspects on different dataset. These evaluations concluded that our information approach with CASIU engine and CasiuVis framework has good usability for non-expert users and its functionality and performance satisfy different network environments.

## 6.2 *Contributions to SoA*

The major contribution of this thesis is an information uplift approach driven by domain expert knowledge. This approach contributes to the state of the art by offering non-expert users better understanding of network systems via a knowledge driven information uplifting, which adapts heterogeneous network and stream data from network components. The information uplift approach contributed a design of semantic encodings for domain expert's insights, a cross-domain knowledge model, and an information uplift process. Importantly, this approach specifies a novel and general information uplift engine, which serves as a useful intermediary to extract, aggregate and uplift the meaningful information for the real-time awkward network log data. Specifically it contributes to the state of the art through its semantic

encoding to establishing the logical relationship between captured domain expertise and existing domain knowledge models, and this formal knowledge representation enables a semantic information uplift, which could automatically invoke related knowledge model to uplift semantic meanings from low-level to high-level and maintain them structurally based on the network component and service.

This research further developed Hampson's research [Hampson et al 2011]by extending his semantic attribute encoding into three types: basic semantic attribute, semantic segment, and temporal semantic attribute. These new encodings provides a combination of atom concepts and endows them temporal stamp, which enables a layered structure for semantic meanings from low-level to high-level and also the temporal reasoning capability to better fit the dynamic nature of network scenario. Compared to most existing semantic uplift approaches, our approach has a high compatibility for heterogeneous network environments. The uplift approach performs flexibly on different data set input by dynamically invoking corresponding domain knowledge model. By using standard semantic techniques, our knowledge model could interoperate with other semantic knowledge models on the web and the flexibility of our information uplift approach promises the potential to address different network scenario and improve the understanding of non-expert users.

The minor contribution of this thesis is the design and implementation of an information uplift framework and a prototypical implementation to support non-expert users in understanding and monitoring different network systems, termed the *Semantic Information Uplift engine (CASIU) and* its *network monitoring framework (CasiuVis)*, to fit our knowledge-driven information uplift approach into different network scenarios and promise the visual representation for non-expert users. The implementation of the Semantic Information Uplift engine (CASIU) is the instrument of this framework which was used to showcase its features. And the framework (CasiuVis) has been implemented into four iterative experiments and its details have appeared in several peer-reviewed publications. CasiuVis was deployed

in the Science Foundation Ireland funded FAME project, Scenario E, as the novel HAN monitoring tool and our framework is recently deployed in FAME-IBM Tivoli work plan as central technologies, which is aiming to investigate a novel IPTV delivery network monitoring solution. In summary, the successful deployment and evaluation of CasiuVis validates the framework we designed, and reinforces the value of our knowledge-driven information uplift approach.

Six papers were published in relation to research carried out in this thesis:

"Integration of QoS Metrics, Rules and Semantic Uplift for Advanced IPTV monitoring", co-author, *Journal of Network and Systems Management* (accepted)

This paper describes the CasiuVis framework with extended semantic encoding and knowledge model to show how it fits into IBM Tivoli IPTV delivery network monitoring scenario.

"Secure Federated Monitoring of Heterogeneous Networks", IEEE Communications Magazine 2013

This paper proposes a novel approach by combining CASIU and federated network monitoring to give the flexibility to deal with the dynamism and diversity of realistic multi-domain monitoring deployments.

"A framework to leverage domain expertise to support novice users in the visual exploration of Home Area Networks", in Proceeding of *the IEEE Network Operations and Management Symposium (NOMS 2012)*, Maui, HI, USA, April, 2012.

This paper concentrates on the design, implementation and evaluation of CasiuVis framework. The design of information uplift approach and the knowledge model is given in detail. The implementation of them in CasiuVis as well as the evaluation are also described and discussed in this paper.

"An ontology-driven approach to support wireless network monitoring for home area networks", in Proceedings of *International Conference on Network and Service Management* (CNSM 2011) Paris, France, October 24-28, 2011.

This paper designs, implements and evaluates the CASIU engine with functionality and usability evaluation in the HAN environment.

"Towards a framework to support novice users in understanding and monitoring of Home Area Networks", in Proceedings of the *IEEE Workshop on Managing Ubiquitous Communications and Services* (PerCom 2012 workshop), March 19-23, 2012, Lugano, Switzerland

This paper describes the CasiuVis framework and how it fits into SFI FAME HAN monitoring scenario.

"A Novel Approach to Support the Visual Exploration and Management of Heterogeneous Home Area Network Devices and Services", in Proceedings of *International Conference on Autonomous Infrastructure, Management, and Security* (AIMS 2011) Nancy, France, June 13-17, 2011

This paper investigates a potential use of information uplift approach and a visual interface to perform HAN monitoring with usability evaluation.

## 6.3 *Future work*

There are a number of practical and research issues in which there is potential for extensions and advances to this work. The performance of our approach could be improved by more efficient engineering work or better hardware and database systems (SAP HANA). This could be improved by choosing a more efficient reasoner and optimizing the reasoning approach. This section focuses on some proposed approaches to extend our research and overcome current limitations.

### 6.3.1 Personalised Network Monitoring Framework

Our information uplift approach provides an important step in enabling end-users to consume large volumes of fine-grained data from heterogeneous sources. As described in this thesis it does this by performing a semantic uplift based on knowledge and expertise encoded by subject domain experts. This offers end-users the ability to capitalize on this expertise when interrogating and examining information that would otherwise be inscrutable. While an important step forward, there are a number of future challenges that need to be addressed. The first of these is to overcome the "one-size-fits-all" issue, where the visualization techniques and underlying data upon which the visualizations are based are the same for every end-user regardless of the task they wish to perform or their prior experience of examining such data.

As such tailoring the information selected and the visualization techniques employed to meet the needs of a specific user, i.e. personalization, is an appropriate and essential next step in furthering human-centric monitoring tools. This personalization challenge may be viewed at two parts; the personalized selection of data and semantic uplift approach that is pertinent to the user's task and then selecting a visualization technique that is most appropriate for displaying that information. In order to personalize the selection of data, and subsequent semantic uplift, it is necessary to characterize the task the user is performing and be able to conceptually relate it to the type of data that may be used to fulfill that task. As a user scrutinizes and explores the data offered, their task may change, so this task definition should facilitate an evolution between task types. This flow between task types is analogous to narrative-based Adaptive Hypermedia personalization [Conlan02], though in the case of human-centric monitoring visualization there is a need to correlate the evolving task, and the data used, with appropriate visualization techniques. This is a second part of the personalization challenge – the automatic selection and threading of visualization techniques to support users in exploring the

data further.

There are a wide range of visualization techniques available and they each support interaction paradigms and data types differently. As a user's exploration takes them from task to task and across different heterogeneous data sources (with varying degrees of semantic uplift) it will become necessary to identify visualizations that best suit their needs. This may be achieved by first characterizing and understanding the nature of the data. For example, if the data is a graph of relationships does it have locally deep hierarchies? If so, a visualization technique that will both display relationships and give information on the nature of collapsed nodes may be appropriate. Closely related to the selection of visualizations is the challenge of offering an appropriate exploration paradigm to the end user so that they do not become lost as they explore across visualizations.

### 6.3.2 Utilization of Linked Data and On-line Domain Knowledge

Linked data provides an approach to interlink and publish data, information or knowledge on the web so that they are machine processable. The DBpedia [Bizer et al 2009] project extracts structured data from Wikipedia and re-publishes it on the web with a public API to enable queries and interlinking with other datasets and applications. This provides a general purpose knowledge base with a very large number of instances (3.64 million things in version 3.7). Many network devices are included in this data-set and it can be used as a source of further context for them. In addition more abstract network concepts such as "router", "wireless networking" and so on are also described, enabling the presentation of introductory material on relevant concepts to home users in the context of a particular network event.

However this knowledge is not strongly structured and suffers from inconsistencies so significant effort is required in performing mappings to our local knowledge base. For example, it may be necessary to process DBpedia's SKOS [SKOS 2004] category tree in addition to the class inheritance hierarchy to correctly

classify an instance and instance values must have some checking to guard against erroneous values present due to human input error in Wikipedia itself. It is also necessary to carefully handle incompleteness since some information though present in Wikipedia is not amenable to the automatic extraction techniques of DBpedia and is thus either not present or very weakly classified and hence hard to extract with standard queries.

By extending our framework, we harvest the structured linked data from DBpedia and map them to corresponding local domain ontology concepts to gather relevant information about connected network components. This information is used to identify the type of detected device/service and provide rich and easy-to-understand introductory text for technical concepts in the network environment. This enables us to partially automate the generation of Linked Data Entity instances in our local knowledge base.

As a reasonable solution, our framework gathers information of active devices and services, for example using UPnP device detection, classify those devices as specific network component or device types in our local knowledge base and then retrieve the related concepts from the linked data on the web to get extra information, such as device/service type, manufacturer, model, introduction text, etc.. This could also be useful for the information uplifting process itself but that is to be studied in future work. The information harvest from the web is also potentially of great benefit for novice users to understand the details of detected problems, expert-supplied reasons and solutions. However ensuring information quality and user overload are critical concerns when presenting this additional information. Given the characteristics of sources like DBpedia it means that runtime dynamic queries of these sources are unlikely to be productive in the short term and instead they provide a way to quickly seed explanatory information that must be pre-checked by domain experts for its validity and utility.

### 6.3.3 Improve the efficiency of semantic reasoning

Another way to improve the performance of this research is to improve the approach to semantic reasoning. As the evaluation result in Figure 5-15 suggests, the semantic processing time is the major cost of the information uplift approach. This could be improved by choosing a more efficient reasoner and optimizing the reasoning approach. In the current implementation, the embedded reasoner from Jena is used to perform this reasoning. From some research [Bock et al. 2008], a benchmark of reasoners was created and the cutting-edge reasoners could be evaluated and selected based upon this benchmark. This work could be extended to the research in this thesis by comparing and evaluating appropriate reasoners for real-time reasoning with streaming data. The reasoning approach adopted in this research could also be optimized by using better in-memory and real-time reasoning approaches.

# Reference


[Abello et al. 1999] Abello, J., Koutsofios, E., Gansner, E. R., and North, S. C., "Large network present visualization challenges," SIGGRAPH Computer Graphics, 33(3), 13-15. 1999

[Accenture 2008] Accenture, "Big trouble with no trouble found: How consumer electronics firms confront the high cost of customer returns," 2008.

[Agrawal et al. 2005] Agrawal, D., Lobo, J., "Policy-based management of networked computing systems," IEEE Communications Magazine, vol. 43, Oct. 2005, pp. 69-75.

[AlertFox 2011] AlertFox, "AlertFox: Website Transaction Monitoring", http://alertfox.com/

[AlchemyAPI 2011] AlchemyAPI, http://www.alchemyapi.com/

[AllegroGraph 2008] AllegroGraph, http://www.franz.com/agraph/allegrograph/.

[Allen 1983] Allen , J ., "Maintaining Knowledge about T emporal Intervals," Communications of the ACM 26, 11 (Nov. 1983), 832–843.

[Andersen et al. 1992] Andersen, Peggy M., Hayes, Philip J., Huettner, Alison K., Schmandt, Linda M., Nirenburg, Irene B., Weinstein,

Steven P., "Automatic Extraction of Facts from Press Releases to Generate News Stories," Processing of the Third Conference on Applied Natural Language Processing, 1992

[Aib et al. 2003] Aib, I., Agoulmine, N., Fonseca, M. S., and Pujolle, G., "Analysis of policy management models and specification languages," Second International Conference on Network Control and Engineering for QoS, Security, and Mobility (Net-Con 2003), October 13-15, 2003, Muscat, Oman, Springer Netherlands, 2003, p. 26.

[Athanasopoulos et al. 2008] Athanasopoulos, E., et al. "Homemaestro: Order from chaos in home networks," in Proceedings of ACM SIGCOMM (demo), August 2008, also see Microsoft Research Technical Report MSR-TR-2008-84.

[Asghar et al. 2009] Asghar, J., Le Faucheur, F., & Hood, I., "Preserving Video Quality in IPTV Networks," IEEE Transactions on Broadcasting, 55(2), 386–395. 2009

[AURORA 2007] "AURORA: Traffic analysis and visualization", IBM research, http://www.zurich.ibm.com/aurora/

[Bock et al. 2008] Jurgen Bock, Peter Haase, Qiu Ji, Raphael Volz,. "Benchmarking OWL Reasoners". In ARea2008 - Workshop on Advancing Reasoning on the Web: Scalability and Commonsense (June 2008)

[Balasubramaniam et al. 2011a] Balasubramaniam, S., Mineraud, J., Perry, P., Jennings, B., Murphy, L., Donnelly, W., and Botvich, D., "Coordinating allocation of resources for multiple virtual IPTV providers to maximize revenue," Broad., IEEE Trans., vol. 57, no. 4, pp. 826 – 39, Dec. 2011.

[Balasubramaniam et al. 2011b] Balasubramaniam, S., Mineraud, J., McDonagh, P., Perry, P., Murphy, L., Donnelly, W., and Botvich, D., "An evaluation of parameterized gradient based routing with QoE monitoring for multiple IPTV providers," Broad., IEEE Trans., vol. 57, no. 2, pp. 183 – 94, Jun. 2011.

[Ball et al. 2004] Ball, R., Fink, G. A., and North, C., "Home-centric visualization of network traffic for security administration," In Proceedings of the 2004 ACM Workshop on Visualization and Data Mining For Computer Security (VizSEC/DMSEC '04), 55- 64, 2004

[Barford et al. 2002] Barford, P., Kline, J., Plonka, D., and Ron, A., "A Signal Analysis of Network Traffic Anomalies," in Proc. of ACM SIGCOMM Internet Measurement Workshop (IMW) 2002, Marseille, France, November, 2002. pp. 71-82.

[Barrett et al. 2004] Barrett, R., Maglio, P. P., Kandogan, E., and Bailey, J., "Usable autonomic computing systems: the administrator's perspective", In Proceedings of the First International Conference on Autonomic Computing, pages 18–25. IEEE Computer Society, 2004

[Barrett et al. 2007] Barrett, K., Davy, S., Strassner, J., Jennings, B., van der Meer, S., and Donnelly, W., "A Model Based Approach for Policy Tool Generation and Policy Analysis," 2007 First International Global Information Infrastructure Symposium, 2007, pp. 99-105.

[Becker et al. 1995] Becker, R.A., Eick, S.G., Wilks, A. R., "Visualizing network data," IEEE Transactions on Visualization and Computer Graphics, 1995.

[Berners-Lee et al. 2001] Berners-Lee, T., Hendler, J., Lassila, O., "The Semantic

Web," Scientific American, p. 34-43., 2001.

[Bly et al. 2006] Bly, S., Schilit, B., McDonald, D. W., Rosario, B., and Saint-Hilaire, Y., "Broken expectations in the digital home," In CHI '06 Extended Abstracts on Human Factors in Computing Systems (CHI '06), 568-573.

[Breitgand et al. 2005] Breitgand, D., Hennis, E., and Shehory, O., "Automated and adaptive threshold setting: Enabling technology for autonomy and self-management," In Proceedings of the Second International Conference on Autonomic Computing. IEEE Computer Society, 2005.

[Brutlag 2000] Brutlag, J., "Aberrant behavior detection in time series for network monitoring," In Proceedings of the 14th System Administration Conference, 2000.

[Brown et al. 2007] Brown, A. S., et al. "Household Technology Use: Integrating Household Life Cycle and the Model of Adoption of Technology in Households", The Information Society, Special Issue: ICT in Everyday Life: Home and Personal Environments, 2007.

[Brown et al. 2013] Brown, A., Mortier, R., Rodden, T., "MultiNet: Reducing Interaction Overhead in Domestic Wireless Networks", Proceedings of ACM SIGCHI Conference on Human Factors in Computing Systems (CHI). 2013.

[Brownlee 1999] Brownlee, N.,"SRL: A Language for Describing Traffic Flows and Specifying Actions for Flow Groups", IETF, 1999, http://www.watersprings.org/pub/id/draft-ietf-rtfm-ruleset-language-07.txt.

[Boley et al. 2001] Boley, H., Tabet, S., and Wagner, G., "Design rationale of

RuleML: A markup language for semantic web rules," International Semantic Web Working Symposium (SWWS), Citeseer, 2001, p. 381–402.

[Camden et al. 2004] Camden, C.,et al, "A Scalable Framework for Wireless Network Monitoring", In Proceedings of ACM WMASH, 2004.

[Card et al. 1999] Card, S., Mackinlay, J., Shneiderman, B.(Eds.)," Readings in Information Visualization: Using Vision to Think", Morgan Kaufmann, 1999.

[Change et al. 2005] Chang, N., and Liu, M., "Optimal controlled flooding search in a large network," In Proceedings of Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), pages 229-237, April 2005.

[Chen et al. 2009] Chen, K. T., Tu, C. C., and Xiao, W. C., "Oneclick: A framework for measuring network quality of experience," in Proceedings of IEEE INFOCOM 2009, 2009.

[Chetty et al. 2007] Chetty, M., Sung, J., and Grinter, R. E.; "How Smart Homes Learn: The Evolution of the Networked Home and Household," Ubicomp, 27-144, 2007

[Chetty et al. 2010] Chetty, M., et al.., "Who's Hogging The Bandwidth: The Consequences Of Revealing The Invisible In The Home," 28th International Conference on Human factors in computing systems, New York. 2010.

[Chetty et al. 2012] M. Chetty et al. "You're Capped: Understanding the Effects of Bandwidth Caps on Broadband Use in the Home," Proc. 2012 ACM Annual Conf. Human Factors in Computing Systems, CHI '12, New York, NY, 2012, pp.

3021–30.

[Chu et al. 2006] Chu, D., Deshpande, A., Hellerstein, J. M., and Hong, W., "Approximate data collection in sensor networks using probabilistic models," Proceedings of IEEE International Conference on Data Engineering (ICDE), April 2006.

[CIM 2004] "CIM Policy Model, v. 2.8," Distributed Management Task Force, http://www.dmtf.org/standards/cim/cim_schema_v281/CIM_Policy28-Final.pdf, Jan. 25, 2004.

[CISCO 1990] CISCO Systems, "Cisco Systems NetFlow Services", http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html

[CISCO 2008] CISCO, "Network Monitoring Tools", http://cisco-network.com/hands-on/network-monitoring-tools/

[Crabtree et al. 2012] Crabtree, A., et al., "Unremarkable Networking: The Home Network as a Part of Everyday Life", Proceedings of ACM Conference on Designing Interactive Systems (DIS). June 2012.

[Comer 2007] Comer, D., "Automated Network Management Systems", Pearson Prentice Hall, Pearson Education, Inc., New Jersey, 2007.

[Chu et al. 2004] Chu, F., and Zaniolo, C., "Fast and light boosting for adaptive mining of data streams," In PAKDD, volume 3056, 2004.

[Dabler et al. 1998] Dabler, R., Palm, H., "Virtuelle Informationsraume mit VRML: Informationen recherchieren und prasentieren in 3D," Heidelberg: dpunkt-Verlag.1998

[Damianou et al. 2000] Damianou, N., Dulay, N., Lupu, E., Sloman, M., "PONDER: A Language for specifying Security and Management Policies for Distributed Systems", The Language Specification, v2.3, 2000.

[Dean et al. 2004] Dean, M., and Schreiber, G., "OWL web ontology language reference", http://www.w3.org/TR/owel-ref, 2004.

[Demers et al. 2003] Demers, A., Gehrke, J., and Rajaraman, R., "Energy-efficient data management for sensor networks: A work-in-progress report," In Proceedings of 2nd IEEE Upstate New York Workshop on Sensor Networks, October 2003.

[Deshpande et al. 2004] Deshpande, A., Guestrin, C., and Madden, S., "Model-driven data acquisition in sensor networks," In Proceedings of International Conference on Very Large Data Bases (VLDB), pages 588-599, August 2004.

[Drools 2007] Drools - The Business Logic integration Platform, http://www.jboss.org/drools.

[DMTF 1992] DMTF member only site, http://www.dmtf.org/apps/org/workgroup/policy/.

[Emma 2010] Emma, D., "Broadband Access", Key Issues for the New Parliament 2010, UK Parliament, http://www.parliament.uk/documents/commons/lib/research/key%20issues/Key%20Issues%20Broadband%20access.pdf

[ENVI 2012] ENVI, http://www.openflow.org/wp/gui/

[Etherpeek 2002] Etherpeek, http://www.wildpackets.com/products

[FaraDian et al. 2002] FaraDian, A., Gehrke, J., and Bonnet, P., "GADT: A

probability space ADT for representing and querying the physical world," In Proceedings of IEEE International Conference on Data Engineering (ICDE), pages 201-211,February 2002.

[Few 2006] Few, S., "Information Dashboard Design", O'Reilly Media, 2006.

[FlowMon 2008] FlowMon, http://www.invea-tech.com/products/flowmon

[Frasincar et al. 2003] Frasincar, F., Telea, A., and Houben, G., "Adapting graph visualization techniques for the visualization of RDF data," Museum, 2003.

[Geroimenko et al 2006] Geroimenko, V., Chen, C., "Visualizing the Semantic Web," Springer, 2006.

[GNetWatch 2008] GNetWatch, http://gnetwatch.sourceforge.net/

[Grinter and Edwards 2005] Grinter, R. E. and Edwards, W. K., "The Work to Make a Home Network Work," Proceedings of the Ninth European Conference on Computer-Supported Cooperative Work (ECSCW' 05), September, 2005.

[Guerrero et al. 2006] Guerrero, A., Villagrá, V. A., Vergara, J. E. L. D., Berrocal, J., "Ontology-based integration of management behaviour and information definitions using SWRL and OWL", Lecture Notes in Computer Science, 2006, Volume 4269/2006, 227-232.

[Gupta et al. 2004] Gupta, A., et al. "Measuring and understanding user comfort with resource borrowing," 13th IEEE International Symposium on High Performance Distributed Computing (HPDC 2004)

[Gupta et al. 2011] Gupta, P., Londhe, P., Bhosale A., "IPTV End-to-End

Performance Monitoring", Communications in Computer and Information Science, 2011, Volume 193, Part 5, 512-523

[Hampson et al. 2011] Hampson, C., Conlan, O., "Facilitating Casual Users in Exploring Linked Data through Domain Expertise," DEXA 2011, Toulouse, France, 2011, pp319-333

[Handschuh et al. 2002] Handschuh, S., Staab, S., and Ciravegna, S., "S-CREAM — Semi-automatic CREAtion of Metadata," Knowledge Engineering and Knowledge Management: Ontologies and the Semantic Web, 2002

[Handschuh et al. 2003] Handschuh, S., Staab, S., "Annotation for the semantic web," IOS Press, 2003.

[Herman et al. 2000] Herman, I., Melanccon, G., Marshall, M. S., "Graph Visualization and Navigation in Information Visualization: A Survey," IEEE Transactions on Visualization and Computer Graphics, Vol. 6, No. 1, 2000, pp. 24-43.

[Hildebrand 2009] Hildebrand, M., "Configuring Semantic Web Interfaces by Data Mapping," Interface, 2009, pp. 1-9.

[Hirsch et al. 2008] Hirsch, C., Grundy, J., and Hosking, J., "Thinkbase: A Visual Semantic Wiki," 7th International Semantic Web Conference (ISWC'08), 2008

[Hoag et al. 2006] Hoag, J. C., and Hayes-Roth, F. A., "Semantic Reasoning for Adaptive Management of Telecommunications Networks," IEEE International Conference on Systems, Man and Cybernetics, SMC'06, Taipei, Taiwan 2006, p. 127–131.

[Homework 2011] Homework Project, http://www.homenetworks.ac.uk

[Horrigan 2008] Horrigan, J. B., "Home Broadband Adoption 2008," Pew Internet and American Life Project, 2008.

[Huebscher et al. 2008] Huebscher, M. C., & McCann, J. A., "A survey of autonomic computing—degrees, models, and applications," ACM Computing Surveys (CSUR), 40(3), 1–28. doi:10.1145/1380584.1380585

[Hussain et al. 2011] Hussain, A., & Viswanathan, A. (2011). "Multiresolution Semantic Visualization of Network Traffic," 2011 Fifth IEEE International Conference on Semantic Computing (ICSC), 2011, p.p. 364–367

[IBM 2001] IBM, "Autonomic computing: IBM's perspective on the state of information technology", 2001 Available at http://www.research.ibm.com/ autonomic/manifesto/autonomic computing.pdf.

[ISO 9595] International Organization for Standards. Common Management Information Service (CMIS) Definition, ISO DIS 9595 (Draft International Standard).

[ISO 9596] International Organization for Standards, Common Management Information Protocol (CMIP) Specification, ISO DIS 9596 (Draft International Standard).

[Jena 2006] Jena, http://openjena.org/.

[Jennings et al. 2007] Jennings, B., Svan der Meer, S., Balasubramaniam, S., Botvich, D., O'Foghlu, M., Donnelly, W., Strassner, J., "Towards autonomic management of communications networks," Communications Magazine, IEEE, vol.45, no.10, pp.112-121, October 2007

[Karagiannis et al. 2008] Karagiannis, T., Gkantsidis, C., Key, P., Athanasopoulos,

E., and Raftopoulos, E., "HomeMaestro: Distributed monitoring and diagnosis of performance anomalies in home networks," no. MSR-TR-2008-161, 29 October 2008

[Keim et al 2006] Keim, D.A., Mansmann, F., Schneidewind, J., Schreck, T., "Monitoring Network Traffic with Radial Traffic Analyzer," IEEE Symposium On Visual Analytics Science And Technology, 2006

[Keller et al. 2005] Keller, T., Tergan, S. O., "Visualizing Knowledge and Information: An Introduction," In Knowledge and Information Visualization: Searching for Synergies. Springer 2005.p.1-23.

[Kephart 2005] Kephart, J.O., "Research challenges of autonomic computing," Proceedings. 27th International Conference on Software Engineering, 2005. ICSE 2005., 2005, pp. 15-22.

[Kharbili et al. 2008a] Kharbili, M. E., and Stein, S., "Policy-Based Semantic Compliance Checking for Business Process Management", in Proc. MobIS Workshops, 2008, pp.178-192.

[Kharbili et al. 2008b] Kharbili, et al. "Towards a Framework for Semantic Business Process Compliance Management ", GRCIS'08 Workshop at CAiSE'08, 2008.

[Kiesler et al. 2000] Kiesler, S., Lundmark, V., Zdaniuk, B., Kraut, R. E., "Troubles with the Internet: The dynamics of help at home," Human Computer Interaction, 15, 323-351, 2000.

[Kim et al., 2013] Kim, H., Feamster, N., "Improving network management

with software defined networking", Communications Magazine, IEEE (Volume:51 , Issue: 2 ), 2013.

[King 2009] P. King, "Wi-Fi Connected Home & Portable Devices: Global Market Forecast and Outlook", Strategy Analytics, Sep 2009, http://www.strategyanalytics.net/default.aspx?mod=ReportAbstractViewer&a0=3083

[Kikuchi et al. 2007] Kikuchi, M., Takayuki, I., Takakura, H., Yoshoda-Honmachi, S., and Kyoto, J., "A Visualization Technique for Monitoring of Network Flow Data," 1st Internationanl Symposium of Information and Computer Elements, 2007, p. 291–296.

[Kosiur 1999] Kosiur, D., "Policy-based Network Management: what is it and who needs it?", The Burton Group, 1999.

[Lan-Secure 2011] Lan-Secure, http://www.lan-secure.com/company.htm

[Lamport 1994] Lamport, L., "The Temporal Logic of Actions," ACM Trans. Program. Lang. Syst. 16, 3 (1994), 872–923.

[Latham 1995] Latham, R., "The dictionary of computer graphics and virtual reality", Springer-Verlag, New York, 1995.

[Lemon 2012] Lemon, http://lemon.web.cern.ch/lemon/index.shtml

[Liboftrace 2012] Liboftrace, http://www.openflow.org/wk/index.php/Liboftrace

[Liotta et al. 2002] Liotta, A., Pavlou, G., & Knight, G., "Exploiting agent mobility for large-scale network monitoring", IEEE Network Magzine, 7–15, 2002.

[Lo et al. 2009] Lo, J.E., Berrocal, Æ.J., and Villagra, A., "Ontology-

Based Network Management : Study Cases and Lessons Learned," Manage, 2009, pp. 234-254.

[Lobo et al. 1999] Lobo, J., Batia, R., Naqvi, S., (Bell Labs), "A Policy Description Language", American Association for Artificial Intelligence (www.aaai.org), 1999.

[Maedche et al. 2001] Maedche, A., Staab, S., "Ontology learning for the Semantic Web," Intelligent Systems, IEEE, 2001.

[Madden et al. 2002a] Madden, S., and Franklin, M. J., "Fjording the stream: An architecture for queries over streaming sensor data," In Proceedings of IEEE International Conference on Data Engineering (ICDE), pages 555-566, February 2002.

[Madden et al. 2002b] Madden, S., Franklin, M. J., Hellerstein, J. M., and Hong, W., "TAG: A tiny agregation service for adhoc sensor networks," In Proceedings of USENIX Symposium on Operating Systems Design and Implementation (OSDI), pages 131-146, December 2002.

[Mathonet et al. 1987] Mathonet, R., Cotthem, H. V., Vanrycheghem, L., "DANTES: an expert system for real-time network troubleshooting", Proceedings of the 10th international joint conference on Artificial intelligence (IJCAI'87), pp 527-530, 1987.

[Maynard 2003] Maynard, D., "Multi-source and multilingual information extraction", Natural Language Processing Group. University of Sheffield, UK. BCS-SIGAI Workshop, 2003

[Miller et al. 2009] Miller, J. S., Lange, J. R. and Dinda, P. A., "EmNet: Satisfying the individual user through empathic home networks," Department of Electrical Engineering and

Computer Science, Northwestern University, Tech. Rep. NWU-EECS-09-05, April 2009.

[Mortier et al., 2012] Mortier, R., et al., "Homework: Putting Interaction into the Infrastructure", Proceedings of 25th ACM UIST Symposium. 2012.

[Moore et al. 2001] Moore, B., Ellesson, E., Strassner, J., Westerinen, A., "Policy Core Information Model -- Version 1 Specification", RFC 3060, 2001.

[Nakamura et al 2013] Nakamura, M., et al., "Considering impacts and requirements for better understanding of environment interactions in home network services", Computer Networks, Volume 57, Issue 12, 20 August 2013, Pages 2442–2453

[Netcool 2006] Netcool, http://www-01.ibm.com/software/tivoli/

[Netflow Analyzer 2011] Netflow Analyzer, http://www.manageengine.com/products/netflow/netflow-traffic-analysis.html

[NetPrefect 2009] NetPrefect, http://www.netprefect.com/

[NetQoS 2005] NetQoS, http://www.ca.com/us/content/Integration/netqos.aspx

[Netrounds 2011] Netrounds, http://www.netrounds.com/

[Network Magic 2005] Network Magic, http://homestore.cisco.com/en-us/software/cisco-software-network-magic_stcVVcatId553232VVviewcat.htm

[Network Probe 2003] Network Probe, http://www.objectplanet.com/probe/

[Nsauditor 2006] Nsauditor, http://www.nsauditor.com/

[OpenFlow 2008] OpenFlow, http://www.openflow.org/wk/index.php/OpenFlow_Wiki

[OpenNMS 1999] OpenNMS, http://www.opennms.org/

[OWL 2004] Web Ontology Language (OWL), http://www.w3.org/2004/OWL/

[Papadopoulo et al. 2004] Papadopoulos, C., Kyriakakis, C., Sawchuk, A., and He, X., "CyberSeer: 3D audiovisual immersion for network security and management," In Proceedings of the 2004 ACM Workshop on Visualization and Data Mining For Computer Security (VizSEC/DMSEC '04), 90-98.2004.

[Patarin et al. 1999] Patarin, S., Makpangou, M., "Pandora : A Flexible Network Monitoring Platform", INRIA report, RR-3834, 1999, http://hal.inria.fr/inria-00072823/PDF/RR-3834.pdf

[PAX-PDL 2002] "PAX Pattern Description Language Reference Guide", Solidum, http://www.solidum.com/products/pax_pdl.cfm, April 2002.

[Pediaditakis et al. 2012a] Pediaditakis, D., Gopalan, A., Dulay, N., Sloman, M., Lodge, T., "Home network management policies: Putting the user in the loop", Proceedings of IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY). July 2012.

[Pediaditakis et al. 2012b] Pediaditakis, D., Gopalan, A., Dulay, N., Sloman, M., "A configuration service for home networks", Proceedings of IEEE Network Operations and Management Symposium (NOMS). April 2012.

[Pras et al. 2007] Pras, A.; Schonwalder, J.; Burgess, M.; Festor, O.; Perez, G.M.; Stadler, R.; Stiller, B.; "Key research challenges in

network management," Communications Magazine, IEEE , vol.45, no.10, pp.104-110, October 2007

[PRTG 2004] PRTG Traffic Grapher, http://www.paessler.com/prtg

[Protégé 2004] Protégé Document, http://protege.stanford.edu/doc/sparql/

[Popov et al. 2003] Popov, B., et el., "KIM–semantic annotation platform," The SemanticWeb-ISWC 2003, 2003, p. 834–849.

[Rajagopalan et al. 2006] Rajagopalan, R., & Varshney, P., "Data-aggregation techniques in sensor networks: a survey," IEEE Communications Surveys & Tutorials, 8(4), 48–63. doi:10.1109/COMST.2006.283821

[RDF 2004] RDF Primer, W3C Recommendation, http://www.w3.org/TR/2004/REC-rdf-primer-20040210/, 2004.

[Rose 1996] Rose, M.T., "The Simple Book: An Introduction to Management of TCP/IP - based internets", Prentice Hall, 1996.

[Rumelhart & Ortony 1977] Rumelhart, D.E., & Ortony, A., "The representation of knowledge in memory," In R.C. Anderson, R.J. Spiro, & W.E. Montague (Eds.), Schooling and the acquisition of knowledge (pp. 99-133). Hillsdale, NJ: Lawrence Erlbaum Associates.

[Russell et al. 2008] Russell, A., and Smart, P., "NITELIGHT: a graphical editor for SPARQL queries," International Semantic Web Conference (Posters \& Demos), Citeseer, 2008, pp. 2-3.

[Saif et al. 2002] Saif, U., Gordon, D., and Greaves, D.; "Internet access to a home area network," Internet Computing, IEEE, vol. 5,

2002, p. 54–63.

[Savoia et al. 2006] Savoia, R., "Custom tailoring," CIO, 9 (17) (1996), p. 112

[SevOne VoIP 2010] SevOne VoIP, http://www.sevone.com/technologies/voip

[SID 2005] "Shared Information/Data model (SID) Model Suite (Phase 5)", TeleManagement Forum, NGOSS Release 4.5, www.tmforum.org, Available 24th May 2005.

[McGillicuddy et al. 2009] McGillicuddy, S.; "Network management and monitoring market remains crowded," SearchNetworking.com, April, 2009.

[Shehan and Edwards 2007] Shehan, E. and Edwards, W. K., "Home Networking and HCI: What Hath God Wrought?" In Proc. of the ACM Conference on Human Factors in Computing Systems (CHI'07), 2007

[Sheridan-Smith et al. 2003] Sheridan-Smith, N., Colquitt, D., and Wootton, J., "Moving from Next-Generation Networks to Enriched-Experience Networks," University of Technology, Sydney, Australia, Confidential deliverable 1A, 2003

[Shneiderman 2005] Shneiderman, B., "The eyes have it: A task by data type taxonomy for information visualizations," In Proceedings IEEE Visual Languages (pp. 336-343). Available online March 16, 2005: http://citeseer.nj.nec.com/shneiderman96eyes.html.

[Sloman 1994] Sloman, M., "Policy Driven Management for Distributed Systems," Network, vol. 2, 1994, pp. 1-24.

[Sloman& Lupu 2002] Sloman, M., and Lupu, E., "Security and Management Policy Specification," IEEE Network, pp. 10-19, 2002.

[SPARQL 2008] SPARQL Query Language for RDF, W3C Recommendation, http://www.w3.org/TR/rdf-sparql-query/, 2008

[Strassner 1999] Strassner, J., "Directory Enabled Networks", Chapter 10, Macmillan Technical Publishing, 1999.

[Strassner 2002] Strassner, J., "DEN-ng: achieving business-driven network management," NOMS 2002. IEEE/IFIP Network Operations and Management Symposium. " Management Solutions for the New Communications World"(Cat. No.02CH37327), Ieee, 2002, pp. 753-766.

[Strassner 2004] Strassner, J., "Policy-Based Network Management", Morgan Kaufmann Publishers, 2004.

[Strassner et al. 2006] Strassner, J., Agoulmine, N., and Lehtihet, E., "Focale: A novel autonomic networking architecture," Multimedia Systems, 2006, pp. 48-60.

[Stone et al. 2001] Stone, G. N., et al. "Network Policy Languages: A Survey and a New Approach", IEEE Network, January/February 2001.

[Soliman et al. 2008] Soliman, J., Colquitt, D., Leaney, J., and Hunter, M., "Policy-based Network Management for Enriched-Experience Networks," Service Management, 2008.

[Sundaresan et al. 2013] Sundaresan, S., et al., "Web performance bottlenecks in broadband access networks", Proceedings of the ACM SIGMETRICS/international conference on Measurement and modeling of computer systems, 2013.

[Sventek et al. 2011] Sventek, J., et al."An information plane architecture supporting home network management," 2011 IFIP/IEEE

International Symposium on Integrated Network Management (IM), 2011

[Tallis 2003] Tallis, M., "Semantic Word Processing for Content Authors", Second International Conference on Konwledge Capture, 2003, Florida.

[tcpdump 1999] tcpdump, http://www.tcpdump.org/

[Teger et al. 2002] Teger, S.; Waks, D.J.; "End-user perspectives on home networking," Communications Magazine, IEEE, vol.40, no.4, pp.114-119, Apr 2002

[Telchemy 2003] Telchemy, http://www.telchemy.com/index.php

[Tolmie et al. 2007] Tolmie, P., Crabtree, A., Rodden, T., Greenhalgh, C., and Benford, S., "Making the home network at home: Digital housekeeping," Proceedings of the 10th European Conference on Computer-Supported Cooperative Work (ECSCW), 331-350. 2007.

[Toutain et al. 2011] Toutain, F., Bouabdallah, A., Zemek, R., and Daloz, C., "Interpersonal Context-Aware Communication Services," Communications Magazine, IEEE, vol. 49, no. 1, pp. 68 – 74, January 2011.

[Tshark 2013] Wireshark Foundation, "Tshark." www.wireshark.org/docs/man-pages/tshark.html.

[Vergara et al. 2008] Vergara, J. E. L. D., Aracil, J., Martínez, J., Salvador, A., "Application of ontologies for the integration of network monitoring platforms", Proceedings of 1st European Workshop on Mechanisms for Mastering Future Internet, Salzburg, Austria,10-11 July, 2008.

[Vergara et al. 2009] Vergara, J. E. L. D., et al. "Ontology-Based Network Management: Study Cases and Lessons Learned", Journal of Network and Systems Management, 17(3), p.234-254, 2009.

[Viswanathan et al. 2011] Viswanathan, A., Hussain, A., Mirkovic, J., Schwab, S., & Wroclawski, J., "A Semantic Framework for Data Analysis in Networked Systems," Proceedings of the 8th USENIX conference on Networked Systems Design and Implementation, Berkeley, USA, 2011

[Wagner et al. 2009] Wagner, E.J., and Birnbaum, L., "Rich Interfaces for Browsing News in Blog Posts," Computational Linguistics, 2009.

[Wallin et al. 2009] Wallin, S., Leijon, V., "Telecom network and service management: An operator survey," Wired-Wireless Multimedia Networks and Services Management, 2009, p. 15–26.

[Wang and Lu 2007] Wang, W. and Lu, A., "Interactive wormhole detection and evaluation", Information Visualization 6(1), Mar. 2007, 3-17.

[Wansink 2013] Wansink, K., "Global Broadband and FttH, Key Statistics and Insights", http://www.budde.com.au/Research/Global-Broadband-and-FttH-Key-Statistics-and-Insights.html?r=51, 2013

[Ware 2004] Ware, C., "Information Visualization - Perception for Design", Morgan Kaufmann, 2004

[Wienhofen 2004] Wienhofen, L. W. "Using Graphically Represented Ontologies for Searching Content on the Semantic Web".

In Proceedings of the information Visualisation, Eighth international Conference (July 14 - 16, 2004).

[Wilson 2000] Wilson, E., "Network Monitoring and Analysis: A Protocol Approach to Troubleshooting", Prentice Hall PTR, New Jersey, 2000.

[Yang et al. 2010] Yang, J., Edwards, W. K., and Haslem, D., "Eden: supporting home network management through interactive visual tools," Proceedings of the 23nd annual ACM symposium on User interface software and technology, ACM, 2010, p. 109–118.

[Yao et al. 2002] Yao, I., and Gehrke, J., "The Cougar approach to in-network query processing in sensor networks," In Proceedings of ACM International Conference on Management of Data (SIGMOD), pages 9-18, June 2002.

[Uren et al. 2006] Uren, V., Cimiano, P., Iria, J., Handschuh, S., Vargasvera, M., Motta, E., Ciravegna, F., "Semantic annotation for knowledge management: Requirements and a survey of the state of the art",Services and Agents on the World Wide Web, Vol. 4, No. 1. (January 2006), pp. 14-28

[Zhang et al. 2005] Zhang, S., Cohen, I., Goldszmidt, M., Symons, J., and Fox, A., "Ensembles of models for automated diagnosis of system performance problems," Technical Report HPL-2005-3, Hewlett-Packard, January 2005.

# Appendix I

**Survey**: Evaluation of a wireless network monitoring system for network experts.

***Please do not participate if you are under 18 years of age.***

| HANMS (Home Area Network Management System) | For each of the statements below, please indicate the extent of your agreement or disagreement by placing a tick in the appropriate column. | Strongly Agree | Agree | Disagree | Strongly Disagree |
|---|---|---|---|---|---|
| **1** | I want to use this system to monitor my home network. | | | | |
| **2** | I do not think this system could be used by the user with limited network knowledge background. | | | | |
| **3** | It was easy for me to learn how to use HANMS to monitor the home network. | | | | |
| **4** | The HANMS monitoring system lacks proper annotation for visual components. | | | | |
| **5** | The HANMS monitoring system could allow me to understand how the current network works. | | | | |
| **6** | The events could not be found and highlight in time. | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 7 | I found it was easy to find out when and where the event occurred. | | | | |
| 8 | The reasons for events were not correctly inferred. | | | | |
| 9 | The probability for each reason was not suitable. | | | | |
| 10 | With the corresponding data and visual widgets, it was hard for me to understand why the reasons were inferred. | | | | |
| 11 | I found the Time Machine was helpful. | | | | |
| 12 | I think the HANMS monitoring system was not sufficient to support different kinds of tasks. | | | | |
| 13 | Compared to non-semantic based network monitoring systems, I feel more comfortable to monitor the home network with HANMS. | | | | |
| 14 | The semantic attributes were not appropriately defined to annotate the raw data. | | | | |
| 15 | The reasoning result could correctly express the meaning of raw data. | | | | |
| 16 | The event was not accurately defined and detected. | | | | |
| 17 | The logical relationships of network components were correctly presented. | | | | |

| | **Question:** | **Please select one of the options below:** | | | |
|---|---|---|---|---|---|
| 14 | Have you configured the home network before? | No experience at all | Some experience | Advanced experience | Expert experience |
| 15 | Do you have any wireless network knowledge background? | No experience at all | Some experience | Advanced experience | Expert experience |

| 16 | Do you have network monitoring experience? | No experience at all | Some experience | Advanced experience | Expert experience |
|---|---|---|---|---|---|

17. In task one, was the event that happened in HAN1 and its inferred reasons presented correctly and accurately? If not, please indicate the problem.

_____

_____

_____

18. In task two, was the event that happened in HAN3 and its inferred reasons presented correctly and accurately? If not, please indicate the problem.

_____

_____

_____

19. In task three, was the event happened in HAN2 and its inferred reasons presented correctly and accurately? If not, please indicate the problem.

_____

_____

_____

20. What additional functions or widgets do you think would be useful for monitoring the home area network?

_____

_____

21. Any comments do you want to leave for this experiment and HANMS?

The time taken to complete this survey is much appreciated.

# Appendix II

**Survey**: Evaluation of a wireless network monitoring system for normal home network users.

***Please do not participate if you are under 18 years of age.***

| | **HANMS (Home Area Network Management System)** | **For each of the statements below, please indicate the extent of your agreement or disagreement by placing a tick in the appropriate column.** | Strongly Agree | Agree | Disagree | Strongly Disagree |
|---|---|---|---|---|---|---|
| **1** | I want to use this system to monitor my home network. | | | | | |
| **2** | I do not think this system could be used by the user with limited network knowledge background. | | | | | |
| **3** | It is easy for me to learn how to use HANMS to monitor the home network. | | | | | |
| **4** | The HANMS monitoring system lacks proper annotation for visual components. | | | | | |
| **5** | The HANMS monitoring system could allow me to understand how the current network works. | | | | | |
| **6** | The events could not be found and highlight in time. | | | | | |
| **7** | I found it was easy to find out when and where the event occurred. | | | | | |
| **8** | The reasons for events were not correctly inferred. | | | | | |
| **9** | The probability for each reason was not suitable. | | | | | |
| **10** | With the corresponding data and visual widgets, it | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | was hard for me to understand why the reasons were inferred. | | | | |
| **11** | I found the Time Machine was easy to use. | | | | |
| **12** | I think the HANMS monitoring system was not sufficient to support different kinds of tasks. | | | | |
| **13** | Compared to non-semantic based network monitoring systems, I feel more comfortable to monitor the home network with HANMS. | | | | |

| | **Question:** | **Please select one of the options below:** | | | |
|---|---|---|---|---|---|
| **14** | Have you configured the home network before? | No experience at all | Some experience | Advanced experience | Expert experience |
| **15** | Do you have any wireless network knowledge background? | No experience at all | Some experience | Advanced experience | Expert experience |
| **16** | Do you have network monitoring experience? | No experience at all | Some experience | Advanced experience | Expert experience |

17. In task one, what happened in HAN1 and what caused this event?

_____

_____

_____

18. In task two, what happened in HAN3 and what caused this event?

19. In task three, what happened in HAN2 and what caused this event(s)?

20. What additional functions or widgets do you think would be useful for monitoring the home area network?

21. Any comments do you want to leave for this experiment and HANMS?

The time taken to complete this survey is much appreciated.

# Appendix III

**Survey**: Evaluation of an IPTV network monitoring system for network administrators.

*Please do not participate if you are under 18 years of age.*

| FAME-IBM IPTV Network Monitoring Tool | For each of the statements below, please indicate the extent of your agreement or disagreement by placing a tick in the appropriate column. | Strongly Agree | Agree | Disagree | Strongly Disagree |
|---|---|---|---|---|---|
| 1 | I want to use this system to monitor IPTV networks. | | | | |
| 2 | I do not think this system could be used by a user with limited network knowledge. | | | | |
| 3 | It was easy for me to learn how to use this system to monitor the IPTV network. | | | | |
| 4 | This IPTV network monitoring system lacks proper annotation for visual components. | | | | |
| 5 | This IPTV network monitoring system allows me to understand how the current network functions. | | | | |
| 6 | These anomalies in monitoring scenario could not be found and highlighted in real time. | | | | |
| 7 | I found it was easy to find out when and where anomalies occurred. | | | | |
| 8 | The root-cause reasons for anomalies were not clearly inferred step by step. | | | | |
| 9 | The result of the reasoning in each step was not clear. | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 10 | With the corresponding network context, it was hard for me to understand why the reasons were inferred. | | | | |
| 11 | I found the network context panel was helpful. | | | | |
| 12 | I think the IPTV network monitoring system was not sufficient to support the QoE-based monitoring. | | | | |
| 13 | The status of QoE is well associated with the user group and network context. | | | | |
| 14 | The semantic concepts (e.g. IPTV_Qulity_Low) were not easy to understand by the people without appropriate network knowledge. | | | | |
| 15 | Compared to network performance based IPTV network monitoring systems, I feel more comfortable to monitor the IPTV network with this system. | | | | |
| 16 | The root-cause anomaly analysis is not sufficient to support daily network problem diagnosis and analysis | | | | |
| 17 | The domain expert knowledge is effectively leveraged to improve IPTV network monitoring in this system. | | | | |

| | **Question:** | **Please select one of the options below:** | | | |
|---|---|---|---|---|---|
| 14 | Do you have any network configuration and troubleshooting experience? | No experience at all | Some experience | Advanced experience | Expert experience |
| 15 | Do you have sufficient network knowledge on QoE, QoS, and | No experience at all | Some experience | Advanced experience | Expert experience |

| | | | | | |
|---|---|---|---|---|---|
| | Network Logs from different network components? | | | | |
| **16** | Do you have any IPTV network knowledge background? | No experience at all | Some experience | Advanced experience | Expert experience |

17. In task scenario2, was the QoE anomaly that happened in IPTV network and its inferred reasons presented correctly and accurately? If not, please indicate the problem.

_____

_____

_____

18. What additional functions or widgets do you think would be useful for monitoring the IPTV network?

_____

_____

_____

19. Any comments do you want to leave for our IPTV network monitoring system?

_____

_____

_____

The time taken to complete this survey is much appreciated.