Issues in Internetworking Wireless Data Networks for Mobile Computing

S.T. Vuong, O. Lau, Y.Q. Yu, H. Shi and M. Haahr
Department of Computer Science
The University of British Columbia
Vancouver, BC, Canada V6T 1Z4
vuong@cs.ubc.ca

Abstract — *There are many issues specific to the area of mobile computing which need to be addressed. This paper will discuss the particular issues of mobile hosts, network management and security.*

I. MOBILE HOSTS

One of the most popular protocol suites for network interoperability is TCP/IP. According to the network architecture of the OSI seven-layer model, host-to-host communication is a network layer service. Recently, most of proposals added the functionality pertaining to mobility at the network layer. But confinement to the IP layer is not sufficient to tackle the problem of mobile hosts at the network layer alone, and thus the support at both the higher and lower layers is needed.

Currently, there are several typical proposals extending the functionality to the IP as it exists in an attempt to provide for mobile hosts. These proposals are introduced in the following section.

A. VIP — Sony project

In a proposal made by Sony [17, 18], a MH is assigned to a new temporary address when it is attached to a new network. The mapping between the home address and the temporary address of a MH is kept in an address mapping table (AMT), which is maintained at the routers. Packets transmitted to the home address of the MH are intercepted by some router that holds an AMT entry for the MH. An address conversion is then performed by the router before the packets are forwarded to the physical location of the MH. Unfortunately this method requires modifications to routers and software, and has problems interoperating with the existing hosts unless so-called conversion gateways are used.

B. IBM MHP project

The scheme proposed by IBM [12, 13] is based on the use of an existing IP option, loose source routing. The key idea is that each packet originating from a MH contains enough routing information to be used by the remote host to send a reply back to the source along an optimal path.

This proposal cannot be considered as a possibility in the short term as very few hosts implement loose source routing correctly, resulting in most packets being routed sub-optimally. Additionally, the use of an IP option results in incompatibility with most PCs, and reduces performance from existing routers.

C. Matsushita MHP project

The proposal from Matsushita [21] is based on an encapsulation approach. A MH is assigned a temporary address when it visits a new network. Any packets destined to the home address of the MH are intercepted by a packet-forwarding server (PFS). The PFS then encapsulates the packet and forwards it using the temporary address of the target MH. The problem with this method is that the routing is always suboptimal unless the software on all stationary hosts are modified.

D. Columbia MHP project

The scheme proposed by Columbia University [7] relies on a group of cooperating mobile support routers (MSRs), which advertise reachability to the same (sub)net. Each MH, regardless of its location within a campus, is always reachable via one of the MSRs. When a host sends a packet to a MH, it first gets delivered to the MSR closest to the source host. This MSR encapsulates the packet and delivers it to the target MSR, which strips the encapsulation header and relays the original packet to the MH.

This approach is limited, as it is optimized to work within a campus environment and requires additional features before it can be extended to support wide-area mobility.

The goal of each MHP (Mobile Host Protocol) is to provide optimum, robust routing to and from MHs in such a way that it is practical to implement, and compatible with the existing network infrastructure. It provides close to optimum routing to and from MHs in the local area with a minimum of infrastructure in a manner that is robust and makes minimal demands on the existing network. If the required protocols existed, in a wide area network it offers an unsatisfactory but workable solution that uses sub-optimum routes.

0-7803-2553-2/95/$4.00 © 1995 IEEE

E. MHRP — CMU proposal

CMU is currently developing a proposal to minimize the changes of existing network resources, such as in the host address, routers and protocols, etc. In its MHRP (Mobile Host Routing Protocol) [8], a MH is always identified through the MH's home IP address, regardless of whether the MH is currently connected to its home network or not. The standard internetwork routing mechanisms are adopted and no changes are needed in MH above IP level. The significant feature is to provide better robustness and scalability for large numbers of mobile hosts. Since MHRP is a protocol at this stage, we will have to wait for its future development.

F. IETF proposal

The IETF (Internet Engineering Task Force) is now working on a draft of the IP mobility support protocol. The goal of this project is to develop a standard mobile IP protocol based on existing mobile communication IP and to use it as the future standard. Since there are a number experimental implementations and proposals around, the purpose of this particular proposal is to produce a standard specification based on current work and those previous proposals. Therefore, the group has no intention to specify any details on the configuration of a mobile subnet. The whole work of the project instead tries to focus on an abstract specification level.

The major new entities in the proposal are: the *mobile node*, the *home agent* and the *foreign agent*. The proposal explains these new concepts first, and then discusses the message formats which are used in the mobile environment, and the mechanisms used to forward messages to mobile node. There are also detailed discussions on mobile nodes, foreign agents and home agents. Finally, security problems are considered in the proposal. The details of this proposal can be found in [6].

There are many discussions on the proposal, as the group has now distributed version 8 of the proposal. This version is stable in respect to the basic structure of Mobile IP. Most of the current discussion on the proposal focuses on clarifying confusion and editing.

G. Current and future work

TCP/IP is the most widely used reliable transport protocol and will be used in at least the first generation of mobile computing environment. However, in order to adapt to the mobile environment, some new versions of TCP/IP need to be developed. Although some proposals based on TCP/IP have been put forward in past several years, none of them entirely satisfy all the requirements necessary for a MHP. Thus as a direction for further research, it will be highly desirable to combine the best features of those proposed MHPs into a more sophisticated version of TCP/IP.

Dramatic technological advancements during the past decade in the area of VLSI, high speed packet switching, and fiber optic communications have led to outgrowths from B-ISDN which take advantage of contemporary networking facilities. In the long run, ATM is highly suitable for modern, high-speed telecommunication systems.

ATM (Asynchronous Transfer Mode) has been adopted by CCITT as a universal transfer mode for B-ISDN. With its high-bandwidth uniform switching capability, the application-to-application transfer of graphics, audio, video, and text can be done at much higher speeds than are currently available. ATM promises to be the ultimate on-premise internetworking technology, and it is predicted that ATM may well be the technology that brings the computer and communication industries together.

II. NETWORK MANAGEMENT

With the growing prevalence and complexity of computer networks, network management has become an essential and critical function in the maintenance and use of networks. The increasing complexity of networks creates opportunities for problems to occur where the network or a portion of it could be disabled, or where performance of the network may be deteriorate to a level that is unacceptable to users. [14] Mobile computing introduces its own unique complexities which network management systems must overcome.

Looking at the OSI systems management standard, network management can be broken down in the five general areas of performance management, fault management, accounting management, configuration management, security management. Each of these five areas will be examined below.

A. Performance management

Performance management is one of the areas most greatly impacted by mobile computing. A network management system must be concerned with efficiency issues such as throughput and utilization, and with service-oriented issues such as availability, response time and cost, and accuracy.

Availability is measured by how often a network can be accessed by a user, and how often network failures occur, effectively rendering the network unavailable. Here, mobile computing has a substantial impact, since mobile user access to a network can never be guaranteed. Consequently, the network and the network management system must compensate. [9] Information here needs to be collected on items such as the statistics of "calls blocked" or calls that fail [11] in order to determine the changes needed to the network design or configuration to improve the service offered to the mobile user.

A network's *response time* and the associated cost are also performance factors. The quicker the response time of a network, the better; however, it is almost inevitable that the improved response will result in higher costs. [14] In this area, the nature of radio transmissions has an impact, as the delay in transmitting data is longer on a radio link than on a physical connection (especially if the link is a satellite link); future technological improvements and developments should improve the response time for mobile users. Software should be designed, and a network should be configured to make the most efficient use of the radio link to mobile stations.

Although recent technological developments for non-mobile networks have provided improved physical transmission media with very low error rates, network *accuracy* for mobile users has posed greater challenges since the physical environment of the transmission medium cannot be controlled. Radio interference (solar storms, magnetic fields and disturbances) can seriously degrade accuracy. A network management system will have to monitor the bit-error rate on radio channels. [11]

Network accuracy affects *throughput*. Since the accuracy for mobile stations is not as high as for non-mobile stations, the protocol overhead required remains substantial. The same problems that affect network accuracy (such as radio interference) also affect throughput, [11] and thus the throughput for mobile computing is comparatively lower. Again, a network management system will need to compensate for these factors in order to provide high-quality service to the mobile user. [9] (For example, where there is a local magnetic disturbance, the signal strength of a radio link may be increased, or perhaps another base station may provide a better connection.)

Utilization is the last measure of performance with which a network manager can determine whether resources are underutilized or over-committed, and consequently reconfigure the network to improve performance. [14] Here, radio channels are most likely to be a highly demanded network resource, which may lead to requests for connections from base stations being queued. [11] A network management system will, like any other resource, make adjustments to base stations to ensure a balance use of resources. (For example, radio channels may be distributed differently among base stations depending on the traffic of mobile stations.)

B. *Fault management*

Faults are abnormal conditions in a network which require attention from a network management system, such as severed communication lines, server crashes or deadlocked processes. Fault management and isolation in itself is very difficult, and are complicated by the presence of mobile stations. Consequently, it is usually the case that mobile stations are left to their own fault isolation. [11]

Testing also becomes more difficult with mobile computing, especially when the tests involve the interactions between a base station and a mobile station, as other factors such as radio interference or whether the mobile station itself has faults cannot be controlled. As with non-mobile network faults, expert systems and fault tolerant processors can greatly assist with fault management. [11, 14]

C. *Accounting management*

Accounting management essentially involves tracking the use of network resources. This may be done for the purposes of billing users, or for other informational purposes such as planning network expansions or service improvements. [11]

Mobile computing creates difficulties because mobile stations may roam between different base stations and networks. Each base station to which a mobile station connects as it roams will have to keep track of all the information that is recorded for accounting purposes. This information will then have to be consolidated, particularly if it is used for billing purposes. If a mobile station roams between different network controlled by different network service providers, not only will the information have to be exchanged and consolidated (as the bill should only come from the mobile user's home service provider) [19, 3], each service provider will have to agree on accounting procedures, how account information is to be exchanged, and what services are accounted for and provided to foreign mobile users.

D. *Configuration management*

Configuration management involves network control, network initialization, and transponder management. [11] With mobile computing, network control and initialization must simply be extended to cover the new areas created, such as the configuration and operation of base stations and satellites, handling mobile stations (especially with roaming), control of radio channels, mobile station traffic patterns and growth, *etc*.

Mobile computing creates the area of transponder management. [11] Transponder management involves the administration of radio and satellite bandwidth. Matters such as the transponder/beam interconnection between satellites, transmission power levels, channel partitioning and service restoration between networks are handled by transponder management. Essentially, it is a special area of configuration management designed to handle matters specialized to mobile computing, particularly with satellite links.

E. *Security management*

Since mobile computing is free of physical restrictions, one of the disadvantages with it is that it is not possible to create physical barriers to protect the security of mobile computing links. Consequently mobile stations are very vulnerable to security threats, and *security management* is the most affected area of network management by mobile computing.

Security is not an issue for a network management system alone, but for the network itself. Consequently, security is covered in its own section later on.

F. Other areas

Mobile computing, especially if a mobile station is linked to a network using wireless means, introduces issues that do not easily fall under the OSI model.

A base station may need to *page* a mobile station, *i.e.* determine the location of the mobile station, and contact it. This may be difficult, as the station may be inactive, broken, out of the service area, or interference may prevent contact.

If there are provisions for base stations to move between different base stations while maintaining its link to a network, *handover* is an issue that arises. Mobile stations must be tracked, so that the network management system knows when to hand over a mobile station to another base station, before the mobile station leaves its range and is lost. When a handover is about to occur, the base stations will have to exchange information about the mobile station being handed over. (*e.g.* user's identity, channel being used, *etc.*) [19] If there are differences in the services offered or the abilities of the two base stations, they will need to be resolved by the network management systems. The actual handover should maintain the connection such that the handover is transparent to the user. [9]

A network management may also handle the traffic loads between mobile stations and base stations, balancing the loads between different base stations. This includes managing loads to deal with changes in the concentrations of traffic during various times of the day, such as the shift from the city centre to suburban areas towards the evening. [19]

G. Current network management standards

Two standards have arisen for network management: the Simple Network Management Protocol (SNMP), which was designed for TCP/IP networks, and the OSI systems management standard. SNMP has now evolved into SNMP version 2 (SNMPv2), and the SNMP standard is currently the prevalent one given its quick introduction, its simplicity and the prevalence of TCP/IP networks. On the other hand, OSI system management is more complex than SNMP, and consequently its development is much slower. However, it has more functionality and flexibility than SNMP.
Neither of these standards have developed far enough to cover mobile computing issues comprehensively. Continuing research is needed to incorporate such issues into either these or new network management standards.

III. SECURITY

Traditional computer networks often rely to a great extent on the privacy of the transmission medium for security, but the broadcast techniques necessary to obtain wireless data transfer are inherently non-private. This aspect, combined with mobile computing, raises a number of new problems with regards to security.

A. OSI Threats

In [5], ISO defines eleven threats important to OSI (Open Systems Interconnection) environments. It is generally agreed, for example by Lambert [9] and Varadharajan [20], that six of them are particularly important to mobile computing. This section provides a brief overview of those six threats and some of the related mobility issues.

Impersonation is commonly dealt with by use of an *authentication* mechanism. Much research has been done in this area, and most schemes, as the one described in [1], are based on encryption of data in combination with a *third-party authentication service*, trusted by both the communicating parties.

Unauthorized behaviour and access is a threat with a very wide scope and its theoretical solution *access control* is equally broad. An issue introduced by mobility is that of managing access to wireless network resources, such as transmitters and receivers without sacrificing flexibility.

Information leakage is an important threat. The non-private nature of wireless communication calls for encryption of all data to avoid eavesdropping. The problem of managing encryption keys can be solved by having the previously mentioned authentication service act as a *key server* as well, storing a key for each client and generating new ones on the fly. Another issue where much less research has been done is that of *location privacy*. Obviously, it is necessary to maintain location information for routing purposes, but the user of a mobile computer may not wish to disclose this information to its peers. A responsible routing protocol will have to respect this wish for privacy.

Integrity attacks, such as the *deletion*, *reordering*, *modification* and especially *replay* of data, are threats to which wireless data transmission is particularly prone. Previous experience with transport protocols such as TP4 and TCP may be applied in this area, since the problems of integrity are similar to those of an unreliable network service.

False repudiation problems can to a large extent be solved by the use of authentication services mentioned above. An authentication service based on public key encryption, such as [1], can be used to guarantee both *origin* and *content*, though currently not *receipt.*

Denial of service attacks in the form of channel jamming is an obvious threat to wireless communication. This problem cannot really be resolved by design, but rather by detection mechanisms combined with an effective police force.

C. *Future Issues*

It is not yet clear where in the OSI Protocol Stack security in mobile computing should go; Aziz [1] suggests the link-layer, but another possibility is the transport layer. Clearly, encryption introduces communication overhead, and limiting it to one layer seems sensible.

If current trends continue, authentication services will play a major role in future wireless networks. This raises a number of issues, most of which have to do with the trust placed in these services and the people responsible for them. For example, authentication services will need to be very failure- and tamper-proof, while at the same time being extremely prone to criticism from users.

IV. CONCLUSION

Whereas TCP/IP was adequate and suitable for internetworking heterogeneous networks with diverse properties, there are special properties of WMDNs and special service requirements of the users of these networks, that have not been taken into account in the design of TCP/IP. For examples, the highly variable and unpredictable data link delays in WMDMs could result in redundant retransmissions at the transport (TCP) layer. It is thus important to harmonize the services and protocols of the transport and data link layers to improve the utilization of the valuable wireless channel bandwidth and realize cost savings by the operators and users of WMDNs.

Those important current research issues in mobile computing which are examined and presented in this paper represent the preliminary results of a concerted effort to implement a testbed interconnecting a Motorola/ARRC WMDN and wireline networks in the initial phase of a collaborative project between UBC, SFU and Motorola Advanced Radiodata Research Center (ARRC).

REFERENCES

1. Aziz, Ashar and Diffie, Whitfield. "Privacy and Authentication for Wireless Local Area Networks." *IEEE Personal Communications Magazine*, First Quarter 1994.
2. BarNoy, A. and Kessler, I. "Tracking Mobile Users in Wireless Communications Networks", *IEEE Trans. Information Theory*, vol. 39, No. 6, pp. 1877–1886, November, 1993.
3. Chum, Stanley. "Network Management For Wireless Communication." Wireless Communications, Selected Topics, International Conference 1992.
4. Cohen, D., Postel, J.B. and Rom, R. "IP Addressing and Routing in a Local Wireless Network", *IEEE INFOCOM*, vol. 6, pp. 626–632, 1992.
5. ISO/IEC 7498–2 Information Processing Systems — Open Systems Interconnection Reference Model — Part 2: Security Architecture. February, 1989.
6. IETF Internet draft. "IP Mobility Support: Draft–IETF–MobileIp–Protocol–0.8", January, 1995.
7. Ioannidis, J., Duchamp D. and Maguire, G. Q. "IP-based Protocols for Mobile Internetworking", *ACM*, pp. 235–245, August, 1991.
8. Johnson, D.B. "Scalable and Robust Internet Routing for Mobile Hosts", IEEE Proceedings, 14th International Conference on Distributed Computing Systems, pp. 2–11, June 1994.
9. Kenward, Gary W. "Mobile Data Communications: The Future Is In Networks." Wireless Communications, Selected Topics, International Conference 1992.
10. Lambert, Paul A. Security for Universal Personal Communications. 1st International Conference on Universal Personal Communications '92 Proceedings. IEEE, 1992.
11. Leung, Victor C.M. and Spolsky, Andrew I. "Network Management for Mobile Satellite Systems." Vehicular Technology, 1991 Conference.
12. Perkins, C. E. "Simplified Routing for Mobile Computers Using TCP/IP", *IEEE*, September, 1992.
13. Perkins, C. E. and Bhagwat, P. "A Mobile Networking System Based on Internet Protocol", *IEEE Personal Communications*, vol. 1, pp. 32–41, 1994.
14. Stallings, William. *SNMP, SNMPv2, and CMIP: The Practical Guide to Network-Management Standards*. Reading, Massachusetts: Addison-Wesley Publishing Company, 1993.
15. Su, Z. and Mathis, J. "Internetwork Accommodation of Network Dynamics: Naming and Addressing", *Proc. International Conf. Comp. Communications*, pp. 681–685, October 1984.
16. Sunshine, C. and Postel, J. "Addressing Mobile Hosts in the ARPA Internet Environment", IEN 138, USC Information Science Institute, March, 1980.
17. Teraoka, F., Yokote, Y. and Tokoro, M. "A Network Architecture Providing Host Migration Transparency", ACM SIGGCOMM , pp. 209–220, August, 1991.
18. Teraoka, F. *et. al.*, "VIP: A Protocol Providing Host Mobility", ACM Communications, vol. 37, No. 8, pp. 67–76, August 1994.
19. Tracey, D. "Telecommunications Management and Mobility." *Telecommunications, 1993* (IEE Conference Publication 371).
20. Varadharajan, V. Authentication in Mobile Distributed Environment. Mobile and Personal Communications, 1993 (IEE Conference Publication 387).
21. Wada, H., *et. al.*, "Mobile Computing Environment Based on Internet Packet Forwarding", Proc. Winter USENIX, January 1993.