

A Recent Cram on Mobile Computing based on Network Applications

Prof. J. Mohana Sundaram^{#1} Prof. V. Rajasekaran^{#2}

^{#1,2} Asst Professor, Department of Computer Science, PSG College of Arts and Science, Cbe-14.

¹ mohanpsgphd@gmail.com ²vrajasekaranpsg@gmail.com

Abstract- The use of Distributed System technology to enable users who are not fixed in a single physical position to communicate with computers which form part of a network; more often than not these computers act like Server. This is one of the upcoming enlargement areas in distributed computing, nowadays many production organization attempts to capture the functionality of normal computer which may embed into portable devices like mobile phones. Mobile computing, which enables real-time isolated access to corporate networks from a mini computer, is now being spotlighted as notebook computers become smaller and more composite, and ISDN, wireless networks, and mobile phones become more popular. Unlike predictable networks, many problems encountered when constructing mobile computing environments affect mobile computing users and Network Analyst. This paper discusses these problems and introduces two connecting software products to help users to overcome them.

Keywords— Mobile computing, wireless network, connecting software, bandwidth.

I. INTRODUCTION

Mobile computing is human-computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad-hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications. The recent trend toward downsizing and great complexity has enhanced the mobility of computers, thus affording convenient use any- where at any time. The significant progress made in communications technology has facilitated the explosive growth of ISDN and wireless networks and cellular phones. Such advanced technologies have thrust mobile computing, which enables the re-mote access of electronic information into the public limelight.

Corporate information systems require a network environment for mobile computing so

that employees can effectively use business information, promote the sharing of information, expand lines of communication, improve work efficiency, and enhance customer confidence and satisfaction. However, unlike conventional networks, many problems and inconveniences imposed by mobility are encountered when companies construct environments for mobile computing. This paper identifies and discusses these problems then introduces communications software with which users can overcome them.

A. Limitations

Insufficient bandwidth: Mobile Internet access is generally slower than direct cable connections, using technologies such as GPRS. These networks are usually available within range of commercial cellular towers. Higher speed wireless LANs has very limited range and the same implementation takes less investment.

Security standards: While works made on mobiles, it is dependent on public networks and need of careful use of Virtual Private Network. Security is a major concern while concerning the mobile computing standards. An easy way of tracking interconnected systems through VPN.

B. Power consumption

When a power outlet or portable generator is not available, portable pc must have the support of power through battery for producing the output.

C. Transmission interferences

Weather, terrain, and the range from the nearest signal point can all interfere with signal reception. Signals which are weak, because they are transferred through different types of objects like tunnels, fully closed buildings and non coverage areas.

D. Potential health hazards

People who use mobile devices while driving are often distracted from driving and are thus assumed more likely to be

involved in traffic accidents.^[3] (There is considerable discussion about whether banning mobile device use while driving reduces accidents or not⁴). Cell phones signals may interrupt medical devices. Mobile phone radiation affects the people's health when compared earlier.

E. Human interface with device

Screens and keyboards tend to be small, which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training.

II. PROBLEMS OF MOBILE COMPUTING

As previously mentioned Mobile Computing requires an environment in which anyone and any necessary information can be accessed at any time from any location. For Mobile computing, "from any location" is the key consideration. Thus, the most pressing problem is how to construct a network environment that enables access from any location in the same way. The use of Mobile computing can be categorized by location as follows:

A. Inside the company

In this case, employees must go to other departments with portable computers to access information servers in the office, the Internet via LAN, or infrared communications environments. Otherwise, company employees must go to other companies to access information servers via LAN or infrared communications environments.

B. Outside the company

In this case, employees access information servers in the corporate networks from outside the company (e.g., while on a train, in a hotel, or at home) using cellular or public phones to obtain information or send reports. This includes accessing corporate or WWW servers on the Internet through an **Internet Service Provider (ISP)**.

Unified administration and automatic distribution of communications environments due to the growing prevalence of the Internet TCP/IP is commonly used in corporate networks. Unfortunately, this protocol is based on access from fixed computers. New protocols like Mobile IP¹⁾ are now being studied to apply TCP/IP to mobile computing in some prominent institutions and corporations, but this will take time to complete.

Even with information outlets provided, mobile users must obtain the following location-de- pendent

information and configure their mobile machines to construct the same access environments as in their departments:

1. Information required to communicate with TCP/IP(e.g., IP address, subnet mask, gateway address)
2. Names of printers and information about printer drivers required to print documents
3. Names and addresses of shared servers required to exchange information
4. Information about the operating environments of application software.

Some basic information described above (e.g., IP address, subnet mask, gateway address) can be automatically obtained from the Dynamic Host Configuration Protocol (DHCP)²⁾ server. The following problems are encountered, however, when applying DHCP to mobile computing.³⁾

5. Difficulty in pooling IP addresses for mobile users due to depleted IP addresses
6. Mobile computer access of multiple IP addresses
7. Unsecured network access due to IP addresses assignment upon request.

Because information about printers, shared servers, and operating environments for application software is unique to each department's network, this information must be obtained from the network administrator of the department concerned. Thus, mobile users wishing to remotely access a conventional network environment must first obtain the information required from the network administrator then manually reconfigure their computers. These tasks impose a large burden on both administrators and Mobile users.

To enhance the convenience of mobile computing environments and relieve the burden on network administrators, a mechanism is needed to enable the unified administration of information needed by mobile users, and to automatically obtain the information when required and recon- figure the mobile computers.

C. Problems When Used Outside the Company

Remotely accessing a corporate server with a portable computer generally requires connection through a wireless network using cellular phones, or through a dial-up network or ISDN using public phones or hotel telephones. Therefore, the problems posed by using a wireless network or accessing a corporate network through ISP should be addressed as follows:

i. Reducing communication costs

The remote access of corporate networks poses accounting problems since most communication is performed through a Wide Area Network (WAN) like a dial-up network. Therefore, a more cost-effective means of communications, such as one that applies mobile agent technology, is urgently needed.

ii. Automatic recovery from line errors

During communication using cellular phones through a wireless network, radio waves may be obstructed and the computer disconnected. In such case, the call must be made again. This takes time and is an inefficient means of communicating.

Countermeasures against wiretapping of data and illegal access of corporate networks There may be other means of accessing a co-operate network via the nearest ISP to reduce communication costs. However, a high-risk factor exists since confidential information may pass through the Internet and be illegally accessed. Therefore, a means to enable cryptographic communications must be devised.

III. MOBILE COMPUTING SOFTWARE

To solve the problems mentioned above, we developed the following products:

- Network Access Control (NAC)

- Mail Transmitter

A. NAC

The proliferation of mobile devices like the iPod, the PC and smart phones have created a challenge for any network manager in today's enterprise environment. Today it's a requirement to securely provide network access to each group of users regardless of who owns the device and where they are accessing the network from. Secure Edge designs **Network**

Access Control systems with application level and device level visibility and control.

Our Solution includes: Role Based Access Control- we integrate our solutions with directory services, and then provide network access to only the resources, applications, and content each user is approved to use. Device Registration Networks can be overrun with employee or guest owned devices. This can create a nightmare for network administrators to try to manage. Secure Edge can build a registration process into your infrastructure to allow guest users to self-register, once approved; they can access the network in a limited role that you define.

Device Fingerprinting it's important to know who is accessing the network; it's just as important to know how they are accessing the network. Security policies can now be applied based upon the Identity of the user as well as what type of device they are using.

Location Aware policies should also be written based upon the users location. Are they on the main campus? Are they working from home? You can and should be able to adjust your security posture by location.

Policy Enforcement a critical part of network access control is limiting the corporate liability as well as protecting users and the network. This can be done by controlling the behaviour of devices connecting to the network. Secure Edge provides ultimate application visibility and control giving you the ability to control the content and risks you'll allow on your network.

B. Mail Transmitter

Mail transmitter works as a POP3 client. It operates as follows:

1) Mobile users e-mail transmission requests to the mail transmitter. The following information must be included: Authentication information, HOME LAN account, destination address and attribute of transmitted mail (e.g., enable/disable file attachment). Transmission requests are encrypted with authentication information attached to protect against intrusion.

2) Upon receiving a transmission request, the mail transmitter decrypts the message, authenticates the client, then reads mail from the account (alternative reception) according to the transmission request.



3) The mail transmitter transfers mail according to the reported conditions.

IV. CONCLUSION

This paper discussed specific problems that should be considered when constructing a mobile computing environment and introduced communications software products developed to overcome these problems. Unfortunately, these products cannot resolve all aspects of these problems. To construct better environments for mobile computing, many remaining problems involving hardware, protocols, application software, and other considerations must be addressed. We should approach these problems not only from a technological standpoint, but also with regard to the prevailing characteristics of mobile computing at a given time.

REFERENCES

- 1) C. Perkins: "IP Mobility Support. RFC 2002, Oct. 1996.
- 2) R. Droms: Dynamic Host Configuration Protocol. RFC 1541, Oct. 1993.
- 3) F. Teraoka: Protocols Providing Seamless Mobility. J. Inst. Elec. Engrs., Jpn., 80, 4, pp.344-349 (1997).
- 4) John D. Raley, David. Dix, David W. Methvin, Martin Heller, Arthur H. Germain III, James E. Powell, Jeffrey Sloman, and Eric Hall: Networking Windows NT. 1st ed., New York, John Wiley & Sons, Inc., 1994, p.538.
- 5) K. Egevang, and P. Francis: "The IP Network Address Translator (NAT)." RFC 1631 May 1994.
- 6) Douglas E. Comer: Internetworking With TCP/IP Volume I: Principles, Protocols, and Architecture 3rd edition, New Jersey, Prentice-Hall, Inc., 1995, p.613.
- 7) Akiyoshi Ochi, Keiji Michine, Toru Atsumi: "Network Applications for Mobile Computing", FUJITSU Sci. Tech. J., 34,1, pp.41-49 (September 1998)