

An era of Mobile computing in networks

By Nishant Lokhande

(MCA II year)

PRMITR

E-mail :nishantlokhande03@gmail.com

Abstract

This paper outlines and put some light on 'Mobile computing in networks'. This paper also represents the advances

in area of mobile computing networks,such as wireless networking. Advances in wireless networking have prompted a new concept of computing , called mobile computing in which users carrying portable devices have access to a shared infrastructure , independent of their physical location. This provides flexible communication between people and (ideally) continuous access to networked services Mobile Computing is a term used to describe technologies that enable people to access network services anyplace, anytime, and anywhere. Mobile computing is a powerful revolution and the way computers are used and in the coming years,this will become even more perceptible although many of the devices themselves will become smaller or even invisible to users to use.

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. Mobile computing provides wireless transmission to access data and information from whatever location.

A] Definitions

1]Mobile computing is "taking a computer and all necessary files and software out into the field."

2]"Mobile computing: being able to use a computing device even when being mobile and therefore changing location. Portability is one aspect of mobile computing."

3]"Mobile computing is the ability to use computing capability without a pre-defined location and/or connection to a network to publish and/or subscribe to information." Uwe Vieille.

II.Mobile data communication with networks

A]Wireless data connections used in mobile computing take three general forms.

1]Cellular data service, uses technologies such as GSM, CDMA or GPRS, and more recently 3G networks such as W-CDMA, EDGE or CDMA2000. These networks are usually available within range of commercial cell towers.

2]Wi-Fi connections ,offer higher performance, may be either on a private business network or accessed through public hotspots, and have a typical range of 100 feet indoors and up to 1000 feet outdoors.

3]Satellite Internet , access covers areas where cellular and Wi-Fi are not available and may be set up anywhere the user has a line of sight to the satellite's location, which for satellites in geostationary orbit means having an unobstructed view of the southern sky. Some enterprise deployments combine networks from multiple cellular networks or use a mix of cellular, Wi-Fi and satellite. When using a mix of networks, a mobile virtual private network (mobile VPN) not only handles the security concerns, but also performs the multiple network logins automatically and keeps the application connections alive to prevent crashes or data loss during network transitions or coverage loss.

III.Wireless communication

Available at: www.researchpublications.org

Wireless communication is the transfer of information between two or more points that are not connected by an electrical conductor. The most common wireless technologies use electromagnetic wireless telecommunications, such as radio. With radio waves distances can be short, such as a few metres for television remote control, or as far as thousands or even millions of kilometres for deep-space radio communications. It encompasses various types of fixed, mobile, and portable applications, including two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking. Other examples of applications of radio wireless technology include GPS units, garage door openers, wireless computer mice, keyboards and headsets, headphones, radio receivers, satellite television, broadcast television and cordless telephones.

A]MOBILE AND WIRELESS DEVICES

Currently, laptops are considered to be the upper end of the mobile device range. Following list gives some examples of mobile and wireless devices graded by increasing performance (CPU , Memory , Display , Input devices etc.,)

1]Sensor: A very simple wireless device is represented by a sensor transmitting state information. An example for such a sensor could be a switch sensing the office door. If the door is closed, the switch transmits this state to the mobile phone inside the office and the mobile phone will not accept incoming calls. Thus, without user interaction the semantics of a closed door is applied to phone calls.

2]Pager: A very simple receiver, a pager can only display short text messages, has a tiny display, and cannot send any messages. Pagers can even be integrated into watches.

3]Mobile Phones: The traditional mobile phone only had a simple black and white text display and could send / receive voice or short messages. Today, however, mobile phones migrate more and more toward PDAs. Mobile phones with full color graphic display, on the internet browser are available.

4]Personal digital assistant: PDAs typically accompany a user and offer very simple versions of office software (calendar, notepad, mail). The typical input device is a pen, with built in character recognition translating hand writing into characters. Web browsers and many other software packages are already available for these devices.

5]Palmtop/pocket computer: The next step toward full computer are pocket computers offering tiny keyboards, color displays, and simple versions of programs found on desktop computers (Text processing, Spread Sheets etc.,).

6]Notebook/Laptop: Finally, laptops offer more or less the same performance as standard desktop computers; use the same software, the only technical difference being size, Weight, and ability to run on a battery.

VI.Cellular networks

A] A cellular network or mobile network is a radio network distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or base station. In a cellular network, each cell uses a different set of frequencies from neighboring cells, to avoid interference and provide guaranteed bandwidth within each cell.

When joined together these cells provide radio coverage over a wide geographic area. This enables a large number of portable transceivers (e.g., mobile phones, pagers, etc.) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission.

B] Cellular networks offer a number of advantages over alternative solutions:flexible enough to use the features and functions of almost all public and private networks

- 1]Increased capacity
- 2]Reduced power use
- 3]Larger coverage area
- 4]Reduced interference from other signals

An example of a simple non-telephone cellular system is an old taxi drivers' radio system, in which a taxi company has several transmitters based around a city that can communicate directly with each other.

V.Wi-Fi network technology

A] Wi-Fi (also spelled Wifi or WiFi) is a popular technology that allows an electronic device to exchange data wirelessly (using radio waves) over a computer network, including high-speed Internet connections. The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards".[1]

Available at: www.researchpublications.org

However, since most modern WLANs are based on these standards, the term "Wi-Fi" is used in general English as a synonym for "WLAN". Only Wi-Fi products that complete Wi-Fi Alliance interoperability certification testing successfully may use the "Wi-Fi CERTIFIED" trademark.

A device that can use Wi-Fi (such as a personal computer, video-game console, smartphone, tablet, or digital audio player) can connect to a network resource such as the Internet via a wireless network access point. Such an access point (or hotspot) has a range of about 20 meters (65 feet) indoors and a greater range outdoors. Hotspot coverage can comprise an area as small as a single room with walls that block radio waves or as large as many square miles — this is achieved by using multiple overlapping access points.

B] Wi-Fi can be less secure than wired connections (such as Ethernet) because an intruder does not need a physical connection. Web pages that use SSL are secure but unencrypted internet access can easily be detected by intruders. Because of this, Wi-Fi has adopted various encryption technologies. The early encryption WEP, proved easy to break. Higher quality protocols (WPA, WPA2) were added later. An optional feature added in 2007, called Wi-Fi Protected Setup (WPS), had a serious flaw that allowed an attacker to recover the router's password. The Wi-Fi Alliance has since updated its test plan and certification program to ensure all newly certified devices resist attacks. The use of WPS greatly reduces the time required to gain access by the use of so called "brute force" attacks.

VI.Limitations with networking

1] Range & Bandwidth: Mobile Internet access is generally slower than direct cable connections, using technologies such as GPRS and EDGE, and more recently HSDPA and HSUPA 3G and 4G networks. These networks are usually available within range of commercial cell phone towers. Higher speed wireless LANs are inexpensive but have very limited range.

2] Security standards: When working mobile, one is dependent on public networks, requiring careful use of VPN. Security is a major concern while concerning the mobile computing standards on the fleet. One can easily attack the VPN through a huge number of networks interconnected through the line.

3] Power consumption: When a power outlet or portable generator is not available, mobile computers

must rely entirely on battery power. Combined with the compact size of many mobile devices, this often means unusually expensive batteries must be used to obtain the necessary battery life.

4] Transmission interferences: Weather, terrain, and the range from the nearest signal point can all interfere with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.

5] 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] (While this may seem obvious, there is considerable discussion about whether banning mobile device use while driving reduces accidents or not.[4][5]) Cell phones may interfere with sensitive medical devices. Questions concerning mobile phone radiation and health have been raised.

6] 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.

VII.In-vehicle computing and fleet computing with mobile networks

A] Another use of mobile coping in networks as ; Many commercial and government field forces deploy a ruggedized portable computer with their fleet of vehicles. This requires the units to be anchored to the vehicle for driver safety, device security, and ergonomics. Rugged computers are rated for severe vibration associated with large service vehicles and off-road driving and the harsh environmental conditions of constant professional use such as in emergency medical services, fire, and public safety.

B] Operating temperature: A vehicle cabin can often experience temperature swings from -20F to +140F. Computers typically must be able to withstand these temperatures while operating. Typical fan-based cooling has stated limits of 95F-100F of ambient temperature, and temperatures below freezing require localized heaters to bring components up to operating temperature (based on independent studies by the SRI Group and by Panasonic R&D).

Vibration can decrease the life expectancy of computer components, notably rotational storage such as HDDs.

Visibility of standard screens becomes an issue in bright sunlight.

Touchscreen users easily interact with the units in the field without removing gloves.

C] High-temperature battery settings: Lithium ion batteries are sensitive to high temperature conditions

Available at: www.researchpublications.org

for charging. A computer designed for the mobile environment should be designed with a high-temperature charging function that limits the charge to 85% or less of capacity.

External antenna connections go through the typical metal cabins of vehicles which would block wireless reception, and take advantage of much more capable external communication and navigation equipment. Several specialized manufacturers such as First Mobile Technologies, National Products Inc (Ram Mounts), Gamber Johnson and LedCo build mounts for vehicle mounting of computer equipment for a wide range of vehicles. The mounts are built to withstand the harsh conditions and maintain ergonomics.

Specialized installation companies design the mount design, assembling the parts, and installing them in a safe and consistent manner away from airbags, vehicle HVAC controls, and driver controls. Frequently installations will include a WWAN modem, power conditioning equipment, transceiver antennae mounted external to the vehicle, and WWAN/WLAN/GPS/etc.

VIII. Security issues involved in mobile computing referred with network

A] Mobile security or mobile phone security has become increasingly important in mobile computing. It is of particular concern as it relates to the security of personal information now stored on the smartphone.

B] More and more users and businesses use smartphones as communication tools but also as a means of planning and organizing their work and private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks. Indeed, smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company.

C] All smartphones, as computers, are preferred targets of attacks. These attacks exploit weaknesses related to smartphones that can come from means of communication like SMS, MMS, wifi networks, and GSM. There are also attacks that exploit software vulnerabilities from both the web browser and operating system. Finally, there are forms of malicious software that rely on the weak knowledge of average users.

D] Different security counter-measures are being developed and applied to smartphones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps.

XI. Conclusion

In this era of mobile computing there are limitations which are solved by many techniques. Mobile computing has severe limitations however, it is far from impossible, and technology improves all the time. It has evolved many advances with networking. The user uses a portable device that shares the abilities of computers. Mobile Computing is an umbrella term used to describe technologies that enable people to access network services anytime, anywhere.

Mobile computing is revolutionizing the way computers are used and in the coming years this will become even more perceptible although many of the devices themselves will become smaller or even invisible to users.

X. References

- [1] Gier, Jim. "Wireless Network Industry Report".
- [2] Mitchell, Bradley. "Satellite Interne".
- [3] Lachu Aravamudhan, Stefano Faccin, Risto Mononen, Basavaraj Patil, Yousuf Saifullah, Sarvesh Sharma.
- [4] Srinivas Sreemanthula. "Getting to Know Wireless Networks and Technology", InformIT.
- [5] PPT on mobile computing.