Mobile Computing in Past, Present and Future

Ompal Jangir[1], *Navneet*[2], *Neeraj Kumar parashar*[3]
Shekhawati Institute of Technology,Sikar
Email: ompaljangir001sgisikar@gmail.com
gauravmathur21@gmail.com

Sikar-332001, India

Abstract— Mobile Computing defines that a device which permits the flow of transmission of data from one computer to another by never been connected to the Physical link layers. Mobile voice communications which is in demands all over the world is having a great increment of the user subscribers to many networks protocols from last two to three years. This concept is normally called as the Principle of the mobile computing. This has become very interesting in the growth of the technology which allows the users to transmit the information details of data.

The protection attributes of the mobile computing are User Authentication which corrects the identity of the user which has been subscribed to this service. User anonymity which is the international mobile subscriber identity abbreviated as the IMSI which is normally used to the networks to properly use for the identification for the user subscribers. Fraud Prevention is for the prevention of hackers who attack the sites. Protection of user data prevents the data of user which is used to protect the saved information of the end users.

Applications related to this device are for the Estate agents to work on home as well as on the construction sites too. Emergency time to inform the others about the emergency condition that has taken place. In justice courts to take a proper straight decisions against the criminals. In industries for the directors to work on computers using a mobile system. Stock related issues for new latest updates of the shares going on. Card verification to verify the card in banks and other places too.

These increments in the virtual technology, circuits and system speed the mobile computing in the future will be at the developed stage from today. The demand for the mobile computations will be on large scale in the coming future days and these devices will generate a bright flash in future.

Keyword : *Evolution, Wireless, Mobile IP, Figure, Network, Security, Generation.*

I. INTRODUCTION

Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link. The main concept involves –

- Mobile communication
-

are

- Mobile software

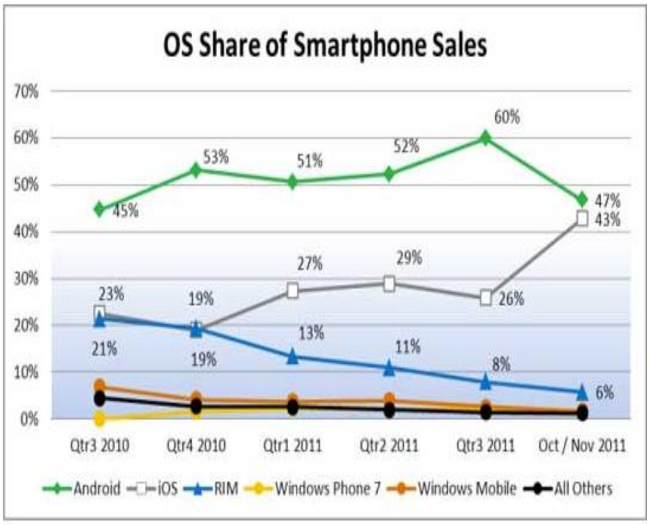
(i) Mobile Communication: The mobile communication in this case, refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. These would include devices such as protocols, services, bandwidth, and portals necessary to facilitate and support the stated services. The data format is also defined at this stage. This ensures that there is no collision with other existing systems which offer the same service.

(ii) Mobile Hardware: Mobile hardware includes mobile devices or device components that receive or access the service of mobility. They would range from portable laptops, smartphones, tablet Pc's, Personal Digital Assistants. These devices will have a receptor medium that is capable of sensing and receiving signals.

(iii) Mobile Software: Mobile software is the actual program that runs on the mobile hardware. It deals with the characteristics and requirements of mobile applications. This is the engine of the mobile device. In other terms, it is the operating system of the appliance. It's the essential component that operates the mobile device.

Mobile Computing Evolution:

In today's computing world, different technologies have emerged. These have grown to support the existing computer networks all over the world. With mobile computing, we find that the need to be confined within one physical location has been eradicated. We hear of terms such as telecommuting, which is being able to work from home or the field but at the same time accessing resources as if one is in the office.



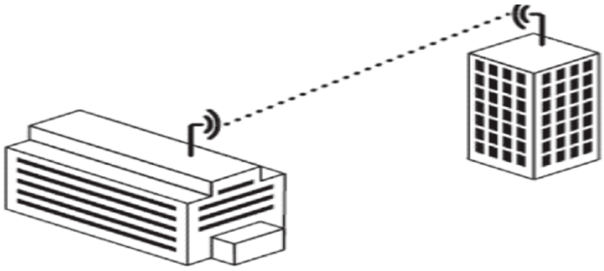
The constant and ever increasing demand for superior and robust smart devices has been a catalyst for market share. Each manufacturer is trying to carve a niche for himself in the market. These devices are invented and innovated to provide state-of-the-art applications and services. For instance, different manufacturers of cellular phones have come up with unique smartphones that are capable of performing the same task as computers and at the same processing speed.

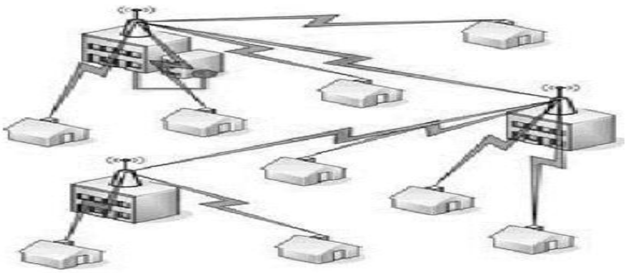
Wireless Network Introduction:

Wireless means transmitting signals using radio waves as the medium instead of wires. Wireless technologies are used for tasks as simple as switching off the television or as complex as supplying the sales force with information from an automated enterprise application while in the field.

Some of the inherent characteristics of wireless communications systems which make it attractive for users, are given below −

- **Mobility** − A wireless communications system allows users to access information beyond their desk and conduct business from anywhere without having a wire connectivity.
- **Reachability** − Wireless communication systems enable people to be stay connected and be reachable, regardless of the location they are operating from.
- **Simplicity** − Wireless communication system are easy and fast to deploy in comparison of cabled network. Initial setup cost could be a bit high but other advantages overcome that high cost.
- **Maintainability** − In a wireless system, you do not have to spend too much cost and time to maintain the network setup.
- **Roaming Services** − Using a wireless network system, you can provide service any where any time including train, buses, aeroplanes etc.
- **New Services** − Wireless communication systems provide various smart services like SMS and MMS.



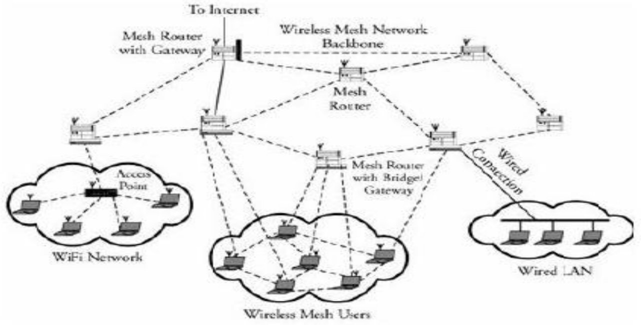


Wireless Network Topologies:

(i) point-to-point bridge: As you know, a bridge is used to connect two networks. A *point-to-point bridge* interconnects two buildings having different networks. For example, a wireless LAN bridge can interface with an Ethernet network directly to a particular access point.

(ii) point-to-multipoint bridge: This topology is used to connect three or more LANs that may be located on different floors in a building or across buildings(as shown in the following image).

(iii) Mesh or ad hoc network: This network is an independent local area network that is not connected to a wired infrastructure and in which all stations are connected directly to one another(as shown in the following image).



Wireless Technologies:

Wireless technologies can be classified in different ways depending on their range. Each wireless technology is designed to serve a specific usage segment. The requirements for each usage segment are based on a variety of variables, including Bandwidth needs, Distance needs and Power.

(i) Wireless Wide Area Network (WWAN): This network enables you to access the Internet via a wireless wide area network (WWAN) access card and a PDA or laptop.These networks provide a very fast data speed compared with the data rates of mobile telecommunications technology, and their range is also extensive. Cellular and mobile networks based on CDMA and GSM are good examples of WWAN.

(ii) Wireless Personal Area Network (WPAN): These networks are very similar to WWAN except their range is very limited.

(iii) Wireless Local Area Network (WLAN): This network enables you to access the Internet in localized hotspots via a wireless local area network (WLAN) access card and a PDA or laptop. It is a type of local area network that uses high-frequency radio waves rather than wires to communicate between nodes.

These networks provide a very fast data speed compared with the data rates of mobile telecommunications technology, and their range is very limited. Wi-Fi is the most widespread and popular example of WLAN technology.

(iv) Wireless Metropolitan Area Network (WMAN): This network enables you to access the Internet and multimedia streaming services via a wireless region area network (WRAN). These networks provide a very fast data speed compared with the data rates of mobile telecommunication technology as well as other wireless network, and their range is also extensive.

Issues with wireless network:

There are following three major issues with Wireless Networks.

- **Quality of Service (QoS)** − One of the primary concerns about wireless data delivery is that, unlike the Internet through wired services, QoS is inadequate. Lost packets and atmospheric interference are recurring problems of the wireless protocols.
- **Security Risk** − This is another major issue with a data transfer over a wireless network. Basic network security mechanisms like the *service set identifier (SSID) and Wireless Equivalency Privacy (WEP);*these measures may be adequate for residences and small businesses, but they are inadequate for the entities that require stronger security.
- **Reachable Range** − Normally, wireless network offers a range of about 100 meters or less. Range is a function of antenna design and power. Now a days the range of wireless is extended to tens of miles so this should not be an issue any more.

Mobile Computing Future Trends:

(i) 3G: 3G or third generation mobile telecommunications is a generation of standards for mobile phones and mobile telecommunication services fulfilling the International Mobile Telecommunications-2000 (IMT-2000) specifications by the International Telecommunication Union. Application services include wide-area wireless voice telephone, mobile Internet access, video calls and mobile TV, all in a mobile environment.

(ii) Global Positioning System (GPS): The Global Positioning System (GPS) is a space-based satellite navigation system that provides location and time information in all weather, anywhere on or near the Earth, where there is an unobstructed line of sight to four or more GPS satellites. The

GPS program provides critical capabilities to military, civil and commercial users around the world. In addition, GPS is the backbone for modernizing the global air traffic system, weather, and location services.

(iii) Long Term Evolution (LTE): LTE is a standard for wireless communication of high-speed data for mobile phones and data terminals. It is based on the GSM/EDGE and UMTS/HSPA network technologies, increasing the capacity and speed using new modulation techniques. It is related with the implementation of fourth Generation (4G) technology.

(iv) WiMAX: WiMAX (Worldwide Interoperability for Microwave Access) is a wireless communications standard designed to provide 30 to 40 megabit-per-second data rates, with the latest update providing up to 1 Gbit/s for fixed stations. It is a part of a fourth generation or 4G wireless-communication technology. WiMAX far surpasses the 30-metre wireless range of a conventional Wi-Fi Local Area Network (LAN), offering a metropolitan area network with a signal radius of about 50 km.

(v) Near Field Communication: Near Field Communication (NFC) is a set of standards for smartphones and similar devices to establish radio communication with each other by touching them together or bringing them into close proximity, usually no more than a few centimeters. Present and anticipated applications include contactless transactions, data exchange, and simplified setup of more complex communications such as Wi-Fi.

REFERENCES

[1] R. F. Nogueira, R. de Alencar Lotufo and R. Campos Machado, "Fingerprint Liveness Detection Using Convolutional Neural Networks," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1206-1213, June 2016.

[2] M. Hildebrandt and J. Dittmann, "StirTraceV2.0: Enhanced Benchmarking and Tuning of Printed Fingerprint Detection," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 833-848, April 2015.

[3] X. Yu et al., "Contrast Enhanced Subsurface Fingerprint Detection Using High-Speed Optical Coherence Tomography," in IEEE Photonics Technology Letters, vol. 29, no. 1, pp. 70-73, Jan.1, 1 2017.

[4] A. Das, M. P. Dutta and S. Banerjee, "VOT-EL: Three tier secured state-of-the-art EVM design using pragmatic fingerprint detection annexed with NFC enabled voter-ID card," 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), Pudukkottai, 2016, pp. 1-6.

[5] F. Pérez-González, M. Masciopinto, I. González-Iglesias and P. Comesaña, "Fast sequential forensic detection of camera fingerprint," 2016 IEEE International Conference on Image Processing (ICIP), Phoenix, AZ, 2016, pp. 3902-3906.

[6] M. Hildebrandt and J. Dittmann, "StirTraceV3.0 and printed fingerprint detection: Simulation of acquisition condition tilting and its impact to latent fingerprint detection feature spaces for crime scene forgeries," 2016 4th International Conference on Biometrics and Forensics (IWBF), Limassol, 2016, pp. 1-6.

[7] R. Haraksim, A. Anthonioz, C. Champod, M. Olsen, J. Ellingsgaard and B. Christophe, "Altered fingerprint detection – algorithm performance evaluation," 2016 4th International Conference on Biometrics and Forensics (IWBF), Limassol, 2016, pp. 1-6.

[8] X. Yang, J. Feng, J. Zhou and Shutao Xia, "Detection and segmentation of latent fingerprints," 2015 IEEE International Workshop on Information Forensics and Security (WIFS), Rome, 2015, pp. 1-6.

[9] B. Alias, G. Johnson and A. Thomas, "New approach for fingerprint detection based on singular points," Fourth International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom2012), Bangalore, India, 2012, pp. 263-265.

[10] S. Selvarani, S. Jebapriya and R. S. Mary, "Automatic Identification and Detection of Altered Fingerprints," 2014 International Conference on Intelligent Computing Applications, Coimbatore, 2014, pp. 239-243.

[11] A.K. Jain, A. Ross, S. Prabhakar: An Introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1):4-20, 2004.

[12] Y. Adini, Y. Moses, S. Ullman: Face recognition: the problem of compensating for changes in illumination direction. IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(7):721-732, 1997.

[13] A.K. Jain, A. Ross, S. Prabhakar: Biometrics: a tool for information security. IEEE Transactions on Information Forensics and Security, 1(2):125-143, 2006.

[14] J.P. Campbell: Speaker recognition: a tutorial. Proceedings of the IEEE, 85(9):1437-1462, 1997.

[15] J. Ortega-Garcia, J. Bigun, D. Reynolds, J. Gonzalez-Rodriguez: Authentication gets personal with biometrics. IEEE Signal Processing Magazine, 21(2):50-62, 2004.

[16] M. Gifford, N. Edwards: Trial of dynamic signature verification for a real-world identification solution. BT Technology Journal, 23(2):259-266, 2005.

[17] F. Monrose, A.D. Rubin: Keystroke dynamics as a biometric for authentication. Future Generation Computer Systems, 16(4):351-359, 2000.