Mobile Computing – challenges in Wireless LANs and Mobile Ad hoc Network

Dr. V. Harsha Shastri[1], V.Sreeprada[2], K.Anitha[3]

[1]Faculty, Department of Computer Science, Loyola Academy Degree and P.G College, Secunderabad, TS, India
[2]Faculty, Department of Computer Science, St. Mary's Centenary Degree College, Secunderabad, TS, India
[3]Faculty, Department of Computer Science, Loyola Academy Degree and P.G College, Secunderabad, TS, India

Abstract: *The concept of mobile computing arose due to the decrease in the size of computing machinery together with the increase in their computing power. This resulted in more number of mobile telephones and portable computing units. It paid way for the mobile users to have versatile communication with other people and notification of useful events. In the present mobile communications environment, lot of research is going on to improve the performance in the areas related to issues like handoffs, routing etc. Security is another issue to be considered when a communication channel is set up. An ad hoc network is a collection of nodes equipped with wireless communication forming a temporary network without any need of existing infrastructure. In this paper, we discuss the challenges in ad hoc network.*

Keywords : *Mobile Computing, Ad hoc network, MANET, wireless networks.*

I. Introduction

Mobile Computing is a human-computer interaction by which a computer is expected to be transported during normal usage. It is a technology in the field of computing and information systems where the data is transmitted using a computer without having a fixed physical link.

Mobile computing requires wireless network to support mobility and handoff from one network to another. One of the upcoming technologies is the wireless computing. Previously the computer users used desktop computers to complete their daily tasks. Ubiquitous computing or pervasive computing refers to access of computer network at any location by any person at all the time. With rapid growth in the mobile communication technology, devices like PDAs and laptops are able to communicate with the fixed wired networks. Because of the flexibility and ubiquitous infrastructure, security needs to be provided at every level. Security issues like confidentiality, integrity, authentication, availability, legitimacy and accountability needs to be taken care individually. We need security to protect from all threats like eaves dropping on the communication or intercepting it as wireless communication takes place mainly through radio signals than with wires.

Wireless LANs have gained usefulness and acceptability by providing wider range and increased transfer rates. The most well-known representatives of Wireless LAN are based on the standard IEEE 802.11 [1], HiperLAN and their variants. There are two types of predominant architectures of WLAN by offering two modes of operations- ad-hoc mode and client-server mode. In ad-hoc mode also known as peer-to-peer, connections between two or more devices established instantaneously without the support of central controller. The client- server mode is chosen in architectures where individual network devices connect to the wired network via an access point serving as a bridge between mobile devices and the wired network. Fig 1 illustrates both the architectures as:

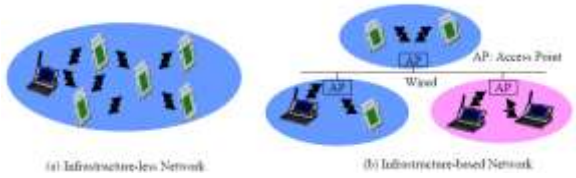

Fig 1: WLAN Architectures

The corresponding two architectures commonly referred to as infrastructure less and infrastructure-based network. Ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any support services regularly available on WAN [2]. Due to self-organizing properties and inherent infrastructure-less, an ad-hoc network provides a method for establishing communications in situations where the constraints are geographically or terrestrial in a distributed network system.
The structure of the paper is as follows: In Section 2, we will discuss various forms of computing. In Section 3, architectures of wireless networks

including the problems and challenges are discussed. In Section 4, the ad hoc networks challenges, and vulnerabilities and advantages are discussed end with conclusion in Section 5.

II. Types of Computing

Researchers refer to computing that uses small portable devices and wireless communication network. There are various forms of computing from mobile computing to ubiquitous computing including the nomadic computing. Figure 2 illustrates the relationship between computing.

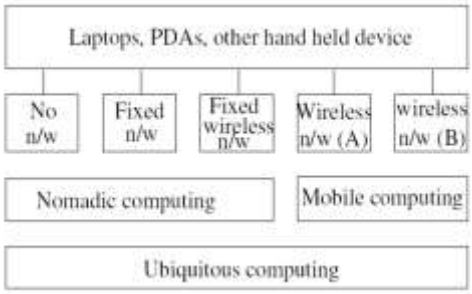

Fig 2: Relationship between Computing

Nomadic computing refers to limited region. Migration is within the building at ordinary speed. Users carrying laptop with dial-up modems are engaged in nomadic computing. Ubiquitous or pervasive computing refers to access to computer network all the time at any location by any person

Wireless LANs operate in one of two modes, ad-hoc or infrastructure. Ad-hoc defines a method of wireless computer peers to exchange data without a predefined network infrastructure. The infrastructure mode of operation is predominantly used for construction of wireless networks and requires two components; wireless access point(s) connected to a traditional wired network and wireless network interface card(s) installed into the computing devices.

III. Wireless Networks Architectures

The architecture of Wireless LAN is designed to serve small low powered terminals capable of wireless access. It can be further connected to fixed network such as LAN and WAN. It has limited range and is designed to use in local environments. Wireless networks communicate by modulating radio waves or infrared light. Wireless communication is linked to the wired network infrastructure by stationary transceivers. The area covered by an individual transceiver's signal is known as cell. Cell size can vary widely. Fig 3 demonstrates the architecture of Wireless network.

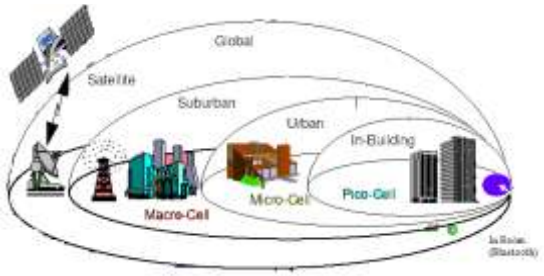

Fig 3: Architecture of Wireless Networks

A. *Problems in Wireless Networks*

- ***Disconnection***- Due to high degree of noise and interference as well as inter-cell handoffs, wireless communications can suffer from many disconnections.
- ***Heterogeneous Network***- To achieve wireless communication, a mobile host must be connected to different and heterogeneous network.
- ***Bandwidth and Interface Variability***- When the user moves from indoor to outdoor, from infrared to radio.
- ***Security Risks***- the security of wireless communication can be compromised easily than wired ones.

B. *Challenges in Wireless Networks*

Since wireless devices need to be small and wireless networks are bandwidth limited, some challenges are data rate enhancements, minimizing cost, low power networking, user security, and Quality of Service.

Signal Fading- signals transmitted over wireless medium can be distorted or faded as they propagate over open and unprotected medium. The same signal can travel different paths due to reflection, diffraction, and scattering many obstacles before they reach the destination. The resulting signal at the receiver cannot be same one as original signal and the transmitted data cannot be received properly. Due to the unreliability of wireless medium, there can be substantial number of loss in packets.

Mobility- all devices in wireless network are free to move. An on-going connection should be kept alive as user roams around. A handoff occurs when the mobile host moves from coverage of the base station to another one. A protocol must be ensured for seamless transmission. We need to decide when the handoff occurs and how the data should be routed

during handoff. A packet loss may occur during handoff.

Power and Energy- a mobile device is generally handy and small size. It performs only some of the dedicated functions. The power source may not be able to deliver much power. When the device moves freely, it would generally be hard to receive a continuous supply of power. It should be able to transmit and receive in an intelligent manner so as to minimize the number of transmissions and receptions for certain communication operations. [7]

Date Rate- The current data rate must be improved significantly to support high-speed applications such as multimedia service. Data rate is a function of various factors such as the data compression algorithm, interference mitigation through error-resilient coding, power control, and the data transfer protocol. Data compression plays a major role when multimedia applications such as video conferencing transmitted by a wireless network. Currently, compression standards such as MPEG-4 produce compression ratios of the order of 75 to 100. The challenge is to improve data compression algorithms to produce high quality audio and video. Highly compressed multimedia data is more sensitive to network errors and interference and we need to use algorithms to protect sensitive data from being corrupted.

Security- As the users move from one location to another, security is of great concern in these networks. Currently, wireless networks employ authentication and data encryption techniques on the air interface to provide security. The IEEE 801.11 standard [3] describes wired equivalent privacy (WEP) that defines a method to authenticate users and encrypt data between PC card and access point.

QoS (Quality of service)- Quality of Service is a measure of network performance that reflects the network's transmission quality and service availability. For each flow of network traffic, QoS can be characterized by four parameters as reliability, delay, jitter, and bandwidth.

IV. Ad hoc Networks

An ad hoc network is a collection of nodes equipped with wireless communication adapters; these nodes dynamically form a temporary network without the need of existing network infrastructure. The devices have limited resources such as CPU, storage, etc. The topology changes frequently due to node's mobility and the unreliability and bandwidth limitation of wireless channels. Fig 4 demonstrates ad hoc network.

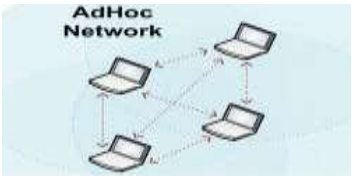

Fig 4: Ad hoc Network

A. *Security requirements of ad hoc networks*

The goal is to protect the information and the resources from attack and misbehaviour. There are many requirements that an effective security must ensure:

- ***Availability***: the desired network services must be available whenever they are expected in spite of attacks.
- ***Authenticity***: communication between the nodes is genuine. A malicious node cannot masquerade as trusted one.
- ***Data Confidentiality***: Only the recipients must understand the message but not by others, that can be achieved by cryptography.
- ***Integrity*** [5] : the message sent from node A to node B was not modified by node C during transmission.
- ***Non-repudiation*****:** ensures that an entity can prove the transmission or reception of information by another entity, i.e., a sender/receiver cannot falsely deny having received or sent certain data. Digital signature is used to ensure nonrepudiation.

B. Applications in Ad hoc Networks

As the number of lightweight devices are increasing and with the evolution of wireless communication, the ad hoc networking technology is gaining effort with increased number of wide spread applications. Ad hoc network can be used in real time business applications, corporate companies to increase product and profit. Ad hoc network can be classified as MANET, which is self-arranging infrastructure less network of mobile devices communicated through wireless link; Vehicular Ad-hoc network also known as VANET uses travelling cars as nodes in a network to create a mobile network. In Ad hoc network, routing is a great challenge. Ad hoc networks occur in many areas such as:

- Emergency disaster management.
- Military operations in remote sites.

- Business meeting venues without infrastructure support.
- Blue tooth
- Personal area network

C. Vulnerabilities in Ad hoc networks

In Ad hoc networks, mobile hosts are not bound to any centralized control like base stations or access points. They are able to move freely with arbitrary speed and direction. The topology can change; information is transferred in multiple hops. Each node can act as host or router forwarding packets for those nodes that are not in direct transmission range with each other. They are prone to more security threats. The weaknesses are as follows:

- ***Lack of infrastructure*** – the network functions by cooperative participation of all nodes in a distributed fashion, but the network can be prone to attack that are designed to break the cooperative algorithm. A malicious user can simply block or modify the traffic traversing it by refusing to cooperate and break the cooperative algorithm. Key management cannot be applied as there are no trusted entities.
- **Dynamically changing topology**- the attacker can update routing information maliciously pretending that the route is a legitimate route. For Ad hoc networks, nodes must exchange information about the route so that the routes can be established between nodes for communication. The intruder may give false routing information.
- ***Energy consumption attack***- nodes are forwarding packets of other nodes. The intruder may overload the network by sending old messages to a node and deplete the node's resources. An attack called rushing attack can be created by sending many routing request packets with high frequency in an attempt to keep other nodes busy with the route discovery process.
- ***Node selfishness***- all the nodes in the ad hoc network carry out routing and network management tasks. But some nodes can become selfish nodes as they want to save their resources such as battery power, memory and CPU.

D. Advantages of Ad hoc network

Ad hoc technology is widely used in portable devices such as laptop, mobile phone to access web services; telephone calls when the user is in travelling. This self-organizing network decreases the communication cost. Ad hoc network is simple to design and install. The following are the advantages:

- Self-configuring nodes are also routers.
- Separation from central network administration.
- Self-healing through continuous re-configuration.
- Scalability incorporates the addition of more nodes.
- The nodes in ad hoc network need not rely on any hardware and software. So, it can be connected and communicated quickly.
- Flexible ad hoc can be temporarily setup at any time in any place.

V. Conclusion

Mobile Computing is an evolving technology. It enables user to communicate and interact with the fixed organizational information system while remaining unconstrained at a physical location. Mobile computing can be implemented in hardware, software, and communication technologies. It provides any time service and anywhere to users by combining wireless networks and mobility. Securing Mobile computing is an on-going research area. In this paper, we have studied various challenges in Wireless networks and in Ad hoc networks with their infrastructures. Security must be a primary consideration, which is proportional to risk.

ACKNOWLEDGMENT

We would like to take this opportunity to express our profound gratitude and deep regard to the Principal Rev Fr. Dr. K.S.Casimir SJ and Rev Fr. D. Sunder Reddy SJ for their constant encouragement and support.

REFERENCES

[1] Chang-Seop Park, " On Certificate-Based Security Protocols for Wireless Mobile Communication Systems."IEEE Network 1997.

[2] R.K.Ghosh ,CSE100, April 2005.

[3] J. Walker, "Overview of IEEE 802.11b Security", http://www.intel.com/technology/itj/q22000/pdf/art_5.pdf.

[4] Abolfazli, Saeid; Sanaei, Zohreh; Ahmed, Ejaz; Gani, Abdullah; Buyya, Rajkumar (1 July 2013). "Cloud-Based Augmentation for Mobile Devices: Motivation, Taxonomies, and Open Challenges".IEEE Communications Surveys & Tutorials 99 (pp):

[5] William Stallings. Cryptography and Network Security principles and practices. Pearson Education Inc, third edition, 2003.

[6] Vipul Gupta and Sumit Gupta "Securing the Wireless Internet" IEEE Communications 2001.

[7] Forman, G.H. and Zahorian, J. (1994) The Challenges of Mobile Computing. IEEE Computer, April 1994, 38- 47.

[8] .Wireless and Mobile Computing, by Fran Turisco and Joanna Case, First Consulting Group Mobile Computing, by Vijay Kumar, University of Missouri-Kansas City Kansas City, MO 64110, USA.