

Mobile Computing with Ad hoc Network & Wireless LAN with Challenges

Pankaj Gothwal¹ Divya Sharma²

^{1,2}Assistant Professor

^{1,2}Department of Computer Science & Engineering

^{1,2}SIET, Sikar, India

Abstract— In this paper, we summarized Mobile Computing with Ad hoc Network & Wireless LAN network and infrastructure. We define the operational model of our mobile computing environment, where we plan to demonstrate our proposed solutions. This review paper focus on Wireless Ad Hoc networks where I took review of its types, applications and security goals. The concept of dynamic mobility is also introduced in Ad Hoc network because nodes are moving from one place to another place, within this network any node can join the network and can leave the network at any time. A wireless ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. The decentralized nature of wireless ad-hoc networks makes them suitable for a variety of applications where central nodes can't be relied on and may improve the scalability of networks compared to wireless managed networks. Wireless Ad hoc networks are networks in which communication links are based on wireless technologies and the network structure or topology is not pre-defined rather build through dynamic network connectivity.

Key words: Mobile Computing, Mobile Computing Security, Mobile Agent's Security, Mobile Ad Hoc Networks, Wireless Networks

I. INTRODUCTION

Mobile computing requires wireless network to support outdoor mobility and handoff from one network to the next at a pedestrian or vehicular speed. Traveler in car using laptop connected with a GSM phone engaged in mobile computing. One of the more exciting information technologies to come about in the last several years was wireless computing. Computer users have to be tied to massive desktop computers to accomplish their daily tasks. Ubiquitous computing or pervasive computing refers to access to computer network at any location by any person all the time. With the rapid growth in the wireless mobile communication technology, small devices like PDAs, laptops are able to communicate with the fixed wired network. Because of its flexibility and provision of providing ubiquitous infrastructure, there is need to provide security at any level. As wireless communication takes place mainly through the radio signals rather than wires, it is easier to intercept or eavesdrop on the communication channels. Therefore, it is important to provide security from all these threats. There are different kinds of issues within security like confidentiality, integrity, availability, legitimacy, and accountability that needs to be individually taken care off. Mobile Cloud Computing at its simplest refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage

away from mobile phones and into the cloud, bringing applications and mobile computing to not just Smartphone users but a much broader range of mobile subscribers. Nowadays, microprocessors and wireless adapters are embedded in many devices, as cell-phones, PDAs, Laptops, digital sensors, and GPS receivers.

II. VARIOUS FORMS OF COMPUTING

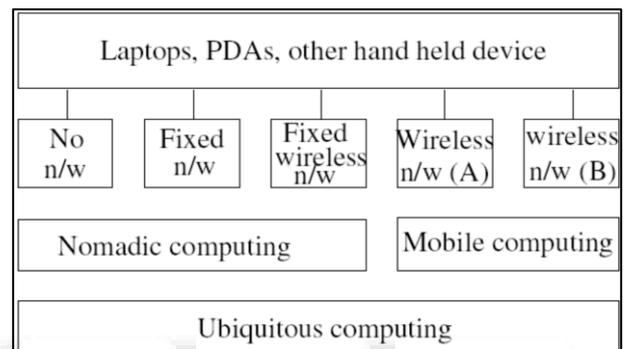


Fig. 1: Various Forms of Computing

III. GENERAL ARCHITECTURE OF WIRELESS NETWORK

Wireless LAN is a traditional LAN architecture extended with a wireless interface to service small low-powered portable terminals capable of wireless access. The wireless LAN is further connected to a more extensive fixed network such as LAN or WAN. Wireless LANs have limited range and are designed to be used only in local environments. There are two types of wireless LAN architectures: ad-hoc networks and infrastructure networks. The Wide-Area Wireless Networks are special mobile radio networks that provide wide coverage for low bandwidth data services. In paging networks the service is usually receive-only and has very low bandwidth. The initial applications for satellite systems are voice and paging. Additional services planned include messaging and fax transmission

IV. AD HOC NETWORK

An ad hoc network is a collection of mobile nodes equipped with wireless communication adapters, these nodes dynamically form a temporary network without the need of any existing network infrastructure. A mobile ad hoc network, or MANET, is a temporary infrastructure less network, formed by a set of mobile hosts that dynamically establish their own network, without relying on any central administration. Mobile hosts used in MANET have to ensure the roles that were ensured by the powerful fixed infrastructure in traditional networks. This is a challenging task, since these devices have limited resources such as CPU, storage, energy, etc. Moreover, the network's environment has some features that add extra complications, such as the

frequent topology changes caused by nodes' mobility, and the unreliability and the bandwidth limitation of wireless channels. A. Security requirements of ad hoc network The security services of ad hoc networks are not different than those of other types of network communication. The goal is to protect the information and the resources from attacks and misbehavior. In working with network security, there are many requirements that an effective security must ensure: □ Availability: ensures that the desired network services are available whenever they are expected, inspite of attacks. Systems that ensure availability seek to combat denial of service and energy starvation attacks that we will present later. Authenticity: ensures communication from one node to another is genuine. It ensures that a malicious node cannot masquerade as a trusted network node. Data confidentiality: is a core security primitive for ad hoc networks, It ensures that a given message cannot be understood by anyone else than its (their) desired recipient(s)

V. CHALLENGES REGARDING MOBILE COMPUTING

Mobile computing affects entire spectrum of issues in computing. First of all it is distributed and mobile computing. Distributed computing as we know works on static wired network. Node may initiate computation somewhere and migrate to another place. So two major problem that arise due to mobility are Searching for current location of a mobile node and to impose a communication structure among nodes. Physical location of mobile is not the network address, so how do we route the message to a mobile host. This question is being addressed by two different communities: Internet community and cellular community. Work of Internet community involves Mobile IP which work as assumes connection-less, packet switching scenario. Cellular community's effort based on location management of cellular phone users. It deals with connection oriented communication, since it is motivated by issues in call-setup in telephony. Main problem in mobility management is to find an appropriate trade-off between searching and informing. Searching is performed when address of the message recipient is not known or at least not known precisely. Informing is a responsibility of the mobile unit when it migrates.

VI. CONCLUSION

In this paper we have studied the different challenges regarding Wireless LAN, its modes Ad hoc network and infrastructure as well as requirement regarding security. As with every Information technology project, security must be a primary consideration. For security to effective, it must be deployed proportional to risk. WLANs present a security risk to organizations but providing security for WLANs is not an insurmountable challenge. There are security solutions available for WLANs to mitigate those most conceivable risks we think securing ad hoc networks is a great challenge that includes many opened problems of research, and receives more and more attention among ad hoc networks community.

REFERENCES

- [1] 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):
- [2] R.K.Ghosh, CSE100, April 2005.
- [3] Arbaugh, W. A., Shankar, N., & Wan, J. Y. (2001). Your 802.11 Wireless Network has No Clothes. Unpublished manuscript, University of Maryland at College Park. Retrieved October 21, 2004, from
- [4] William Stallings. *Cryptography and Network Security principles and practices*. Pearson Education Inc, third edition edition, 2003.
- [5] Frank Stajano and Ross Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In 7th International Security Protocols Workshop, Cambridge, UK, April 1999.
- [6] Duchamp, D. (1992) Issues in Wireless Mobile Computing. *Proceedings Third Workshop on Workstation Operating Systems*, April 1992, 2-10.
- [7] Sumi Helal, Ph.D Associate professor, computer & information science & Engineering Department , University of Florida, Gainesville.FL32611, helal@cise.ufl.edu.
- [8] Berghel, H. (2004). Wireless Infidelity I: War Driving. *Communications of the ACM*, 47(9), 21-28.