International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

Security Challenges in Mobile Computing – A State of Art Survey

S. Chohitha , Dr Shirina Samreen , Dr G. Vishnu Murthy
[1]MTech 2nd Year, Dept. of CSE, CVSR College, Hyderabad, Telangana, India
[2,3]Associate Professor, Dept. of CSE, CVSR College, Hyderabad, Telangana, India

ABSTRACT

In this paper, we summarized Mobile computing with WirelessLAN and its mobile Ad hoc network and infrastructure. We define the operational model of our mobile computing environment, where we plan to demonstrate our proposed solutions. Mobile cloud computing is the combination of both cloud computing and mobile networks to bring benefits for mobile users, network operators, as well as cloud computing providers. In the present mobile communication environment, lot of research is going on, to improve the performance of issues like handoffs, routing etc. Security is another key issue that needs to be considered, when the setup of communication channel is to be set. Wireless local area network (WLAN) security are inherently weak and do not provide adequate security. Newer, more robust, wireless security technologies are being developed but have not had widespread acceptance within corporate information infrastructures. 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. Earlier studies on ad hoc networks aimed to propose solutions to some fundamental problems, such as routing, coping with the new challenges caused by networks and nodes' features without taking the security issues into account.

Keywords: Mobile computing, mobile computing security, mobile agent's security, mobile ad hoc networks, wireless networks.

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. These well-equipped devices allow the creation of wireless mobile networks, which make the vision of nomadic computing with its ubiquitous access more and more attractive.

VARIOUS FORMS OF COMPUTING

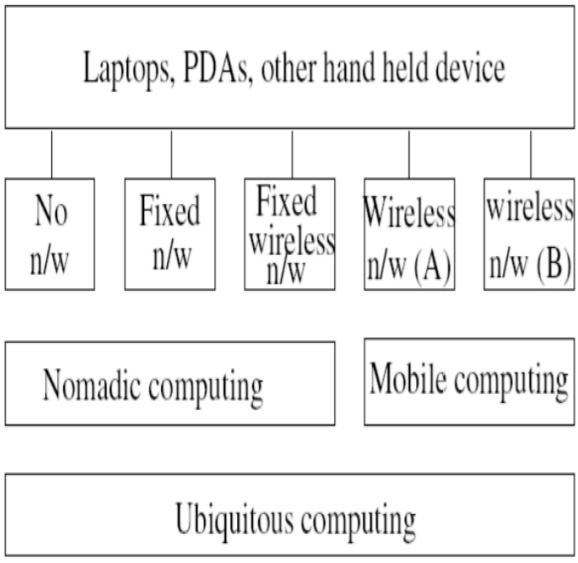


Fig.1: Relationship between computing

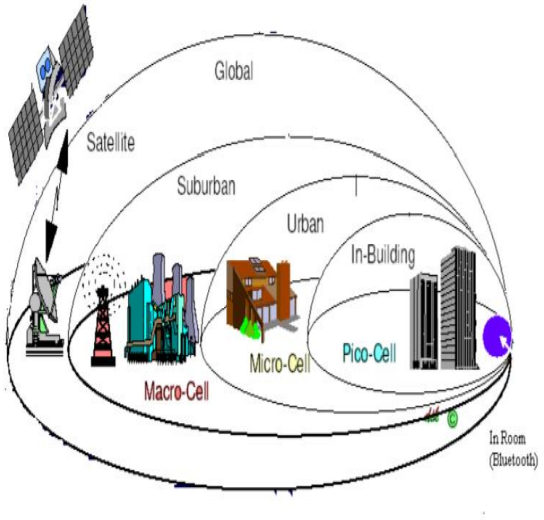
Mobile, ubiquitous, nomadic, untethered, pervasive and anytime, anywhere, any person computing are used by researchers to refer to computing that uses small portable devices and wireless communication network. Nomadic computing refers to limited migration. Migration is within a building at a pedestrian speed. In the same vein, users carrying laptop with DIAL-UP modems are engaged in nomadic computing. Ubiquitous computing or pervasive computing refers to access to computer network all the time at any location by any person. Ubiquitous computing cannot be realized unless mobile computing matures. One of the more exciting information technologies to come about in the last several years was wireless computing. WirelessLANs 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 and has not met with great success. 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.

GENERAL ARCHITECTURE OF WIRELESS NETWORKS

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. Wireless networks communicate by modulating radio waves or pulsing 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 a cell. Cell sizes vary widely:

Fig.2: Architecture of wireless networks



A. Operational problems associated with wireless network

1. Disconnection:-Wireless communications suffer from frequent disconnections due to a higher degree of noise and interference as well as the process of inter-cell hand-offs. Disconnections can be hidden by asynchronous operation.
2. Heterogeneous network:-To achieve wireless communication a mobile host must get connected to different and heterogeneous networks. The general problem of heterogeneity can be addressed by exploiting emerging distributed systems. Bandwidth and Interface
3. Variability:-Bandwidth can shift one to four orders of magnitude, depending on whether the system is plugged in or using wireless access

or switching interfaces, e.g. from infrared to radio when the user moves from indoors to outdoors. Mobile applications have to adapt their behavior properly.

4. Security Risks:- Precisely because connection to a wireless link is so easy, the security of wireless communication can be compromised much more easily than that of wired communication.

B. Challenges regarding wireless network Main cause of loss of packets in wired network is congestion because error rates are very low. In wireless network, congestion still remains a problem, but this situation is somewhat reversed. Wired and wireless network require different techniques to achieve reliability and flow control. TCP works is unsuitable for wireless network as it interprets errors as packet loss. ITCP (split/indirect TCP) splits TCP into two parts, one between sender and local MSS of the recipient. The other between local MSS and recipient. If MH switches cell during life time of a ITCP Connection center point of connection moves to new MSS sender remains completely unaware about it.

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.

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, in spite 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). Data confidentiality is typically enabled by applying cryptography

Integrity: denotes the authenticity of data sent from one node to another. That is, it ensures that a message sent from node A to node B was not modified by a malicious node, C, during transmission.

Non-repudiation ensures that the origin of the message is legitimate. i.e. when one node receives a false message from another, non repudiation allows the former to accuse the later of sending the false message and enables all other nodes to know about it. Digital signature may be used to ensure non repudiation.

B. Challenges regarding Ad hoc network

Ad hoc network routing is the ultimate challenge. Ad hoc networks arise in rapid deployment scenarios:

1. Emergency disaster management.
2. Military operation in remote sites.
3. Business meeting venues without infrastructure support. Many routing algorithms are designed: AODV, DSR, DSDV, TORA, FSR, LAR, ABR, etc. There are interesting applications of conventional graph theoretic problems in ad hoc network routing.

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. Extreme situations can be

1. Mobile unit never informs works for units receiving few messages and for units which don't move during receiving.
2. Always informs works well for units receiving messages frequently.

COMPARISION

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

SI.NO	Protocol	Highlighting Features	Requirements	Weaknesses/Overheads
1	T. Ghosh et al. [12]	isolates malicious nodes acting independently or in collusion	requires the existence of a Public Key Infrastructure	increases delay in Route Discovery
2	T. Ghosh et al. [13]	model also works for colluding malicious nodes	all the nodes have identical radio range, requires Public Key Infrastructure	malicious node sends false accusation message, increases delay in Route Discovery
3	Pirzada et al. [16]	The trust model makes use of trust agents that reside and run on each node	nodes do not collude, uses promiscuous mode for trust assignment	increases the delay in route discovery as well as the resulting returned route may be long
4	Pirzada et al. [17]	divided into three components: Trust agent, Reputation agent and the Combiner	Assumes that nodes do not have varying transmission power	uses promiscuous mode for trust assignment, trust is based solely on the forwarding behavior
5	TAODV [20]	trust is represented by opinion as used in subjective logic	requires the nodes to authenticate each other by verifying the certificate	unable to detect in case a malicious node authenticates itself but later on acts as a blackhole
6	DMTR [21]	contains three components: the Requestor, the Decision Maker and the Executant	Uses Trust Network Connect (TNC) and barrel theory	Exchange of trust table between nodes requires lots of bandwidth

CONCLUSION

In this paper we have studied the different challenges regarding WirelessLAN, 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 http://www.cs.umd.edu/%7Ewaa/wireless.pdf

[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] SumiHelal,Ph.D Associate professor, computer & information science & Engineering Department , University of Florida, Gainesville.FL32611,helal@cise.ufl.edu.

[8] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," Future generation computer systems, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[9] V. Turner, J. F. Gantz, D. Reinsel, and S. Minton, "The digital universe of opportunities: Rich data and the increasing value of the internet of things," IDC, White paper, Apr. 2014.

[10] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," IEEE Communications Surveys & Tutorials, vol. pp, Aug. 2017.

[11] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, Jun. 2016.

[12] W. Shi and S. Dustdar, "The promise of edge computing," Computer, vol. 49, no. 5, pp. 78–81, May. 2016.

[13] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," Future generation computer systems, vol. 29, no. 1, pp. 84–106, Jan. 2013.