INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

PRIVACY WITH MOBILE COMPUTING

MISS. SHRADDHA A. MEHARE[1], PROF. A. R. MUNE[2]

1. Student of Master of Engineering in (CSE), IBSS college of Engineering and Technology, Amravati, India.
2. Assistant professor Department of (CSE), IBSS College of Engineering and Technology, Amravati, India.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: As more and more people enjoy the various services brought by mobile computing, it is becoming a global trend in today's world. At the same time, securing mobile computing has been paid increasing attention. In this article security issues in mobile computing environment. We analyze the security risks confronted by mobile computing and present the existing security mechanisms [1]. Storage capacity and communication bandwidth are two factors that significantly impact the design and implementation of mobile system. Furthermore, storage density is increasing at an exponential rate faster than the associated communication bandwidth. High-density storage in very small form factors will enable this new classes of applications that would not be possible in system which rely heavily on communication [2].

Keywords: Mobile Computing, Privacy

Corresponding Author: MS. SHRADDHA A. MEHARE

Access Online On:

www.ijpret.com

How to Cite This Article:

Shraddha A. Mehare, IJPRET, 2015; Volume 3 (9): 1281-1288

PAPER-QR CODE

INTRODUCTION

The last few years have seen a true revolution in the telecommunications world. Besides the three generations of wireless cellular systems, ubiquitous computing has been possible due to the advances in wireless communication technology and availability of many light-weight, compact, portable computing devices, like laptops, PDAs, cellular phones, and electronic organizers. The term of mobile computing is often used to describe this type of technology, combining wireless networking and computing. Various mobile computing paradigms are developed, and some of them are already in daily use for business work as well as for personal applications. Wireless personal area networks (WPANs), covering smaller areas with low power transmission, can be used to exchange information between devices within the reach of a person. A WPAN can be easily formed by replacing cables between computers and their peripherals, helping people do their everyday chores or establish location aware services. One noteworthy technique of WPANs is a Bluetooth based network. However, WPANs are constrained by short communication range and cannot scale very well for a longer distance. Wireless local area networks (WLANs) have gained enhanced usefulness and acceptability by providing a wider coverage range and an increased transfer rates. The most well-known representatives of WLANs are based on the standards IEEE, Hiper LAN and their variants. IEEE has been the predominant standard for WLANs, which support two types of WLAN architectures by offering two modes of operation, ad-hoc mode and client-server mode. In ad-hoc (also known as peer-to-peer) mode connections between two or more devices are established in an instantaneous manner without the support of a central controller. The client-server mode is chosen in architectures where individual network devices connect to the wired network via a dedicated infrastructure (known as access point), which serves as a bridge between the mobile devices and the wired network. This type of connection is comparable to a centralized LAN architecture with servers offering services and clients accessing them. A larger area can be covered by installing several access points, as with cellular structure having overlapped access areas. The corresponding two architectures are 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 centralized administration or standard support services regularly available on the wide area network. Due to its inherent infrastructure-less and self-organizing properties, an ad hoc network provides an extremely flexible method for establishing communications in situations where geographical or terrestrial constraints demand totally distributed network system, such as military tracking, hazardous environment exploration, reconnaissance surveillance and instant conference. While we are enjoying the various services brought by mobile computing, we have to realize that it comes with a price: security vulnerabilities[2].

Security Issue:-

Security is a prerequisite for every network, but mobile computing presents more security issues than traditional networks due to the additional constraints imposed by the characteristics of wireless transmission and the demand for mobility and portability. We address the security problems for both infrastructure-based WLANs and infrastructure-less ad hoc networks.

1. Security Risks of Infrastructure-Based WLANs

Because a wireless LAN signal is not limited to the physical boundary of a building, potential exists for unauthorized access to the network from personnel outside the intended coverage area. Most security concerns arise from this aspect of a WLANs and fall into the following basic categories:

- ***Limited Physical Security*:**

Unlike traditional LANs, which require a wire to connect a user's computer to the network, a WLAN connects computers and other components to the network using an access point (AP) device. As shown in Figure 1 an access point communicates with devices equipped with wireless network adaptors and connects to a fixed network infrastructure. Since there is no physical link between the nodes of the wireless network and the access point, the users transmit information through the "air" and hence anyone within the radio range (approximately 300 feet for 802.11b) can easily intercept or eavesdrop on the communication channels. Further, an attacker can deploy unauthorized devices or create new wireless networks by plugging in unauthorized clients or setting up renegade access points.

- ***Constrained Network Bandwidth:-***

The use of wireless communication typically implies a lower bandwidth than tha of traditional wired networks. This may limit the number and size of the message transmitted during protocol execution. An attacker with the proper equipment and tools can easily flood the 2.4 GHz frequency, corrupting the signal until the network ceases to function. Since the aim of this type of attack is to disable accessing network service from the legitimate network users, they are often named denial of service (DoS) attack. Denial of service can originate from outside the work area serviced by the access point, or can inadvertently arrive from other 802.11b devices installed in other work areas that degrade the overall signal.

Energy Constrained Mobile Hosts:-

To support mobility and portability, mobile devices generally obtain their energy through batteries or other exhaustive means, hence they are considered as energy constrained mobile hosts. Moreover, they are also resource-constraint relative to static elements in terms of storage memory, computational capability, weight and size. In WLANs, two wireless clients can talk directly to each other, bypassing the access point. A wireless device can create a new type of denial of service attack by flooding other wireless clients with bogus packets to consume its limited energy and resources.

2. More Vulnerabilities of Infrastructure-less Ad Hoc Networks

In ad hoc networks, mobile hosts are not bound to any centralized control like base stations or access points. They are roaming independently and are able to move freely with an arbitrary speed and direction. Thus, the topology of the network may change randomly and frequently. In such a network, the information transfer is implemented in a multi-hop fashion, i.e., each node acts not only as a host, but also as a router, forwarding packets for those nodes that are not in direct transmission range with each other. By nature, an ad hoc network is a highly dynamic self-organizing network with scarce channels. Besides these security risks, ad hoc networks are prone to more security threats due to their difference from conventional infrastructure-based wireless networks. ***The Lack of Pre-fixed Infrastructure*** means there is no centralized control for the network services. The network functions by cooperative participation of all nodes in a distributed fashion. The decentralized decision making isprone to the attacks that are designed to break the cooperative algorithms. A malicious user could simply block or modify the traffic traversing it by refusing to cooperate and break the cooperative algorithms. Moreover, since there are no trusted entities that can calculate and distribute the secure keys, the traditional key management scheme cannot be applied directly.

Dynamically Changing Topology aids the attackers to update routing information maliciously by pretending this to be legitimate topological change. In most routing protocols for ad hoc networks, nodes exchange information about the topology of the network so that the routes could be established between communicating nodes. Any intruder can maliciously give incorrect updating information. For instance, DoS attack can be easily launched if a malicious node floods the network with spurious routing messages. The other nodes may unknowingly propagate the messages.

Energy Consumption Attack is more serious as each mobile node also forwards packets for other nodes. An attacker can easily send some old messages to a node, aiming to overload the network and deplete the node's resources. More seriously, an attack can create a *rushing attack* by sending many routing request packets with high frequency, in an attempt to keep other nodes busy with the route discovery process, so the network service cannot be achieved by other legitimate nodes.

Node Selfishness is a specific security issue to ad hoc network. Since routing and network management are carried by all available nodes in ad hoc networks, some nodes may selfishly deny the routing request from other nodes to save their own resources (e.g., battery power, memory, CPU)[2]

3. Predictions for future mobile design:-

There are eventually going to be physical limits for the storage density achieved by rotating magnetic disk technology; however, storage is on a fast research track and it appears there are more physical options that can be applied to improving storage density than exist for improving communication bandwidth or processing capability. These include 3D stacking of memory elements, polymer memories, and MEMS based nano memories. Given the trends we have described in Section 1, and the huge potential of the examples we have provided, it is clear that massive portable storage capabilities will play a significant role in the design of mobile systems in the future. We can expect that PDAs and cell phones will take advantage of the new storage capacity as it comes available. 1GB compact flash cards are already available, and the disk drive on the laptop used to prepare this text has a capacity of 60GB. There is little doubt in our minds that for another decade the storage trends will continue to roll out as predicted. The last example in Section 3 introduces the notion of Proactive Computing [10], which can be an effective tool for mitigating some of the difficulties of mobile computing. Autonomous agents will be the key to moving beyond current models of pervasive computing, particularly as the number of available devices expands beyond what is reasonable for us to manage. Massive file systems enable the proactive *statistical* preparation of data: storing information in case it might be needed – mitigating a computer's inability to make accurate predictions with high-density storage [1].

4. Security Requirements:-

Similar to traditional networks, the goals of securing mobile computing can be defined by the following attributes: availability, confidentiality, integrity, authenticity and non-repudiation.

Availability ensures that the intended network services are available to the intended parties when needed.

Confidentiality ensures that the transmitted information can only be accessed by the intended receivers and is never disclosed to unauthorized entities.

Authenticity allows a user to ensure the identity of the entity it is communicating with. Without authentication, an adversary can masquerade a legitimate user, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of users.

Integrity guarantees that information is never corrupted during transmission. Only the authorized parties are able to modify It [1].

5. Mobility for Mobile Communication:-

Mobility affects mobile communications on all the components, including devices, networks, and services. To a mobile device, besides the physical requirements like weight, size, power, display, and shape, there still exist other functional requirements e.g. different user interfaces suitable to mobility scenario and the computing and communication capabilities distribution. To a service for mobile case, the most important effect is the requirement on adaptation in which a mobile service should be adaptive to different transmission links, different user mobile devices, and different using contexts. In particular here, we focus on the impacts of mobility on both the architectures and the protocols of networks.

- **Mobility effects to network architectures**

For network architectures different mobility modes can be distinguished resulting in different types of network architectures and communication usages. The mobility modes can be divided into classes according to the different spatial-temporal relations.

- **Mobility effects to protocol stack**

The feature of mobility also affects the whole protocol stack, from the physical, data link, and network layers up to the transport and application layers.

1) At the physical layer, mobility influences are remarkable since most mobile communications are based on wireless media like radio. A wireless channel varies with most mobility factors e.g. velocity, direction, place (outdoor or indoor), etc. Resource reuse and avoiding interference are two important problems at the physical layer.

2) At the data link layer, mobility based on wireless networks brings problems of bandwidth, reliability, and security, for which compression, encryption, and error correction techniques are needed. Other problems include fixed or dynamic channel allocation algorithms, collision detection and avoidance measures, QoS resource management, etc.

3) At the network layer, mobility of mobile nodes means that new routing algorithms are needed in order to change the routing of packets destined for a moving node to its new point of attachment in networks.

4) At the transport layer, a end-to-end connection may mix wired and wireless links. This makes congestion control a complex task due to the different characteristics of wired and wireless networks, since packet loss is caused mainly by high error rates and handoff in wireless networks instead of because of congestion—the situation on wired links. Retransmission mechanism based on increasing interval may lead to an unnecessary drop in the date rate. Function distribution between the transport and the data link layer is a new problem caused by mobility.

5) At the middleware and application layer, mobility brings new requirements on middleware supports. Examples include service discovery schemes, QoS management, and environment auto configuration. Device-aware applications are important to adapt to different types of user devices, while connection-aware applications are needed to adapt to the changing conditions of network connectivity.

- **Mobility management for mobile communications**

Mobility management is the essential technology that supports roaming users with mobile terminals to enjoy their services through wireless networks when they are moving into a new service area. From the viewpoint of functionality, mobility management enables communication networks to track and locate roaming terminals in order to deliver data packets to the new destination and maintain connections with terminals moving into new areas. According to the concept above, mobility management mainly contains two distinct but related components: location management and handoff management[3].

CONCLUSION:-

Mobile computing technology provides anytime and anywhere service to mobile users by combining wireless networking and mobility, which would engender various new applications and services. However, the inherent characteristics of wireless communication and the demand for mobility and portability make mobile computing more vulnerable to various threats than traditional networks. Securing mobile computing is critical to develop viable applications.

REFERENCES:-

1. D. P. Agrawal and Q-A. Zeng, Introduction to Wireless and Mobile Systems, Brooks

2. J. Walker, “Overview of IEEE 802.11b Security”, http://www.intel.com/technology

3. L. Venkatraman and D. P. Agrawal, "Startegies for Enhancing Routing Security in Protocols for Mobile Ad hoc Networks," JPDC Special Issue on Mobile Ad Hoc Networking and Computing

4. LAN Standards of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer (PHY) specification. IEEE Standard 802.11, 1999 Edition,” 1999.

5. N. Borisov, I. Goldberg, and D. Wagner, “Intercepting Mobile Communications: The Insecurityof802.11”,http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf.

6. M. G. Zapata, “Secure Ad hoc On-Demand Distance Vector Routing,” ACM SIGMOBILE Mobile Computing and Communications Review, Vol. 6 , No. 3, pp. 106-107, 2002.

7. Y. C. Hu and D. B. Johnson and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad-Hoc Networks

8. Y. Zhang and W. Lee, “Intrusion Detection in Wireless Ad-Hoc Networks,” Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom'2000), Aug 2000.

9. Kong, P. Zerfos, H. Luo, S. Lu and L. Zhang, “Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks,” Proceedings of the IEEE 9th International Conference on Network Protocols

10. Truman, T.; Pering, T.; Doering, R.; Brodersen, R.,“InfoPad Multimedia Terminal: A Portable Device for Wireless Information Access”, IEEE Transactions on Computers, October 1998,