Art Survey of Secure Mobile Computing

P. Mounika
MTech 2nd Year, Dept. of CSE, CVSR College, Hyderabad, Telangana, India
S. Deepika
Assistant Professor, Dept. of CSE, CVSR College, Hyderabad, Telangana, India
Dr G. Vishnu Murthy
Associate Professor, Dept. of CSE, CVSR College, Hyderabad, Telangana, India

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, we discuss the security issues in mobile computing environment. We analyze the security risks confronted by mobile computing and present the existing security mechanisms.

1. 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 (from a couple of centimeters to few meters) 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 802.11 [1], HiperLAN and their variants. IEEE 802.11 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 (Figure 1(a)), connections between two or more devices are established in an instantaneous manner without the support of a central controller. The client-server mode (Figure 1(b)) 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.

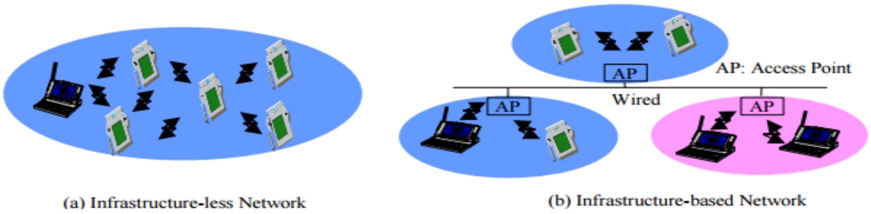

AP: Access Point
AP
Wired
AP
AP
(a) Infrastructure-less Network
(b) Infrastructure-based Network

Fig.1: WLAN Architectures

2. WHY IS SECURITY AN 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.

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 that 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.

SECURITY COUNTERMEASURES

Secure mobile computing is critical in the development of any application of wireless networks.

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.

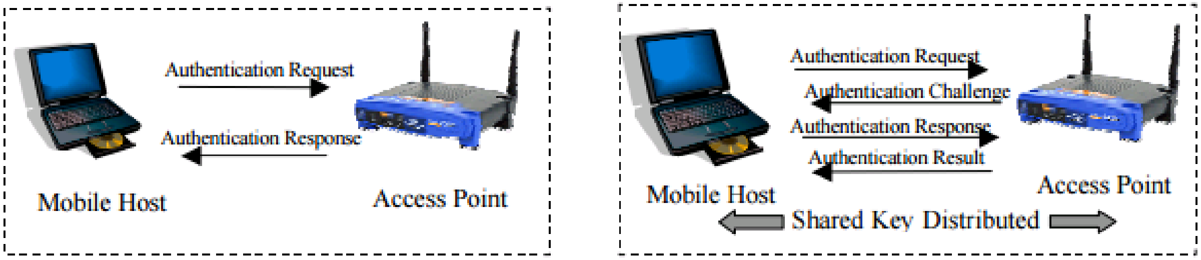
Confidentiality ensures that the transmitted information can only be accessed by the intended receivers and is never disclosed to unauthorized entities.

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.

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.

SECURITY SCHEMES FOR AD HOC NETWORKS



Open System Authentication

Shared Key Authentication

Fig.2: IEEE 802.11 Authentication Modes

The IEEE 802.11b standard identifies several security services such as encryption and authentication to provide a secure operating environment and to make the wireless traffic as secure as wired traffic. In the IEEE 802.11b standard, these services are provided largely by the WEP (Wired Equivalent Privacy) protocol to protect link-level data during wireless transmission between clients and APs. That is, WEP does not provide any end-to-end security but only for the wireless portion of the connection. Apart from WEP, other well-known methods that are built into 802.11b networks are: Service Set Identifier (SSID), Media Access Control (MAC) address filtering, and open system or shared-key authentication. SSID: Network access control can be implemented using an SSID associated with an AP or group of APs. Each AP is programmed with an SSID corresponding to a specific wireless LAN. To access this network, client computers must be configured with the correct SSID. Typically, a client computer can be configured with multiple SSIDs for users who require access to the network from a variety of different locations. Because a client computer must present the correct SSID to access the AP, the SSID acts as a simple password and, thus, provides a measure of security. However, this minimal security is compromised if the AP is configured to "broadcast" its SSID. When this broadcast feature is enabled, any client computer that is not configured with a specific SSID is allowed to receive the SSID and access the AP. MAC Address Filtering: While an AP can be identified by an SSID, a client computer can be identified by a unique MAC address of its 802.11b network card. To increase the security of an 802.11b network, each AP can be programmed with a list of MAC addresses associated with the client computers allowed to access the AP. If a client's MAC address is not included in this list, the client is not allowed to associate with the AP. MAC address filtering (along with SSIDs) provides improved security, but is best suited to small networks where the MAC address list can be efficiently managed. Each AP must be manually programmed with a list of MAC addresses, and the list must be kept up-to-date.

WEP2: As an interim improved solution to the many flaws of WEP, the TGI Working Group of the IEEE proposed WEP2. Unfortunately, similar to major problems with WEP, WEP2 is not an ideal solution. The main improvement of WEP2 is to increase the IV key space to 128 bits, but it fails to prevent IV replay and still permits IV key reuse. The weakness of plaintext exploits and same IV replay are the same with that in WEP. In WEP2, the authentication is still a one-way authentication mode, and the problem of rogue AP is not solved.

Virtual Private Networking (VPN): To further address the concerns with WEP security, many organizations adopt the virtual private network (VPN) technology. The VPN approach has a number of advantages. Firstly, it is scalable to a large number of 802.11 clients and has low administration requirements for the IEEE 802.11 APs and clients. Secondly, the VPN servers can be centrally administered and the traffic to the internal network is isolated until VPN authentication is performed. Thirdly, if this approach is deployed then a WEP key and MAC address list management is not needed because of security measures created by the VPN channel itself. This is a good solution for networks, particularly with existing VPN infrastructure for remote access. However, though the VPN approach enhances the air-interface security significantly, this approach does not completely address security on the enterprise network. For example, authentication and authorization to enterprise applications are not always addressed with this security solution. Some VPN devices can use user-specific policies to require authentication before accessing enterprise applications. Another drawback in the VPN solution is the lack of support for multicasting, which is a technique used to deliver data efficiently in real time from one source to many users over a network. Multicasting is useful for streaming audio and video applications such as press conferences and training classes. Also, a minor issue of VPNs is that roaming between wireless networks is not completely transparent. Users receive a logon dialog when roaming between VPN servers on a network or when the client system resumes from standby mode. Some VPN solutions address this issue by providing the ability to "autore-connect" to the VPN.

IEEE 802.11i Robust Security Network (RSN) standard: To help overcome this security gap in wireless networks, the IEEE 802.11 working group instituted Task Group i (802.11i) has proposed significant modifications to the existing IEEE 802.11 standard as a long-term solution for security, called Robust Security Network (RSN). An interim draft of IEEE 802.11i is now available, known as Wi-Fi Protected Access (WPA). The draft of IEEE 802.11i standard consists of three major parts: Temporal Key Integrity Protocol (TKIP), counter mode cipher block chaining with message authentication codes (counter mode CBC-MAC) and IEEE 802.11x access control.

Secure Routing Establishing correct route between communicating nodes in ad hoc network is a pre-requisite for guaranteeing the messages to be delivered in a timely manner. If routing is misdirected, the entire network can be paralyzed. The function of route discovery is performed by routing protocols, and hence securing routing protocols has been paid more attention. The routing protocols designed for ad hoc networks assume that all the nodes within the network behave properly according to the routing protocols and no malicious nodes exist in the network. Obviously this assumption is too strong to be practical. The use of asymmetric key cryptography have been proposed [5][6] to secure ad hoc network routing protocols. Dahill et al. [5] propose ARAN, in which every node forwarding a route request and route reply message must sign it. Although their approach could provide strong security, performing a digital signature on every routing packet could lead to performance bottleneck on both bandwidth and computation. In [6], Zapata proposed a secure extension of the Ad Hoc On-demand Distance Vector routing protocol, named SAODV. The basic idea of SAODV is to use RSA signature and one-way hash chain (i.e., the result of n consecutive hash calculations on a random number) to secure the AODV routing messages. The effectiveness of this approach is sensitive to the tunneling attacks. IP spoofing is still possible in SAODV routing protocol.

Trust and Key Management Most of the protocols discussed above make an assumption that efficient key distribution and management has been implemented by some kind of key distribution center, or by a certificate authority, which has super power to keep connecting to the network and can not be compromised, but how to maintain the server safely and keep it available when needed presents another major issue and can not be easily solved. To mitigate this problem, the concept of threshold secret sharing is introduced and there are two proposed approaches. Zhou and Hass [15] use a partially distributed certificate authority scheme, in which a group of special nodes is capable of generating partial certificates using their shares of the certificate signing key. This work is the first to introduce the threshold scheme into security protocols in ad hoc networks and provides an excellent guide to the following work. The problem of this solution is that it still requires an administrative infrastructure available to distribute the shares to the special nodes and issue the public/private key pairs to all the nodes. How to keep the n special nodes available when needed and how the normal nodes know how to locate the server nodes make the system maintenance difficult. In [16], Kong et al. proposed another threshold cryptography scheme by distributing the RSA certificate signing key to all the nodes in the network. This scheme can be considered as having a fully distributed certificate authority, in which the capabilities of certificate authority are distributed to all nodes and any operations requiring the certificate authority's private key can only be performed by a coalition of k or more nodes. This solution is better in the sense that it is easier for a node to locate k neighbor nodes and request the certificate authority service since all nodes are part of the certificate authority service, but it requires a set of complex maintenance protocols.

Service Availability Protection To protect the network from the problem of service unavailability due to the existence of selfish nodes, Buttyan and Hubaux proposed so-called Nuglets [17] that serve as a per-hop payment in every packet or counters to encourage forwarding. Both nuglets and counters reside in a secure module in each node, are incremented when nodes forward for others and decremented when they send packets as an originator. Another approach, the Collaborative Reputation Mechanism (CORE) [18] is proposed, in which node cooperation is stimulated by a collaborative monitoring and a reputation mechanism. Each network entity keeps track of other entities' collaboration using a technique called reputation. The reputation is calculated based on various types of information. Since there is no incentive for a node to maliciously spread negative information about other nodes, simple denial of service attacks using collaborative technique itself are prevented.

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.

REFERENCE:

[1] "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.

[2] D. P. Agrawal and Q-A. Zeng, Introduction to Wireless and Mobile Systems, Brooks/Cole publisher, 2002.

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

[4] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: the Insecurity of 802.11", http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf.

[5] B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A Secure Routing Protocol for Ad Hoc Networks," Technical Report UM-CS-2001-037, Electrical Engineering and Computer Science, University of Michigan, August 2001.

[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,” Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02), pp. 3-13, 2002.

[8] Y. C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,” Proceedings of the 8th ACM International Conference on Mobile Computing and Networking, September, 2002.