Secure Mobile Computing

Dharma P. Agrawal[1], Hongmei Deng[1], Rajani Poosarla[1] and Sugata Sanyal[2]

[1.] Center for Distributed and Mobile Computing
University of Cincinnati, Cincinnati, OH 45221-0030
{dpa, hdeng, poosarrd}@ececs.uc.edu

[2.] School of Technology and Computer Science
Tata Institute of Fundamental Research
Homi Bhabha Road, Mumbai 400005, India
sanyal@tifr.res.in

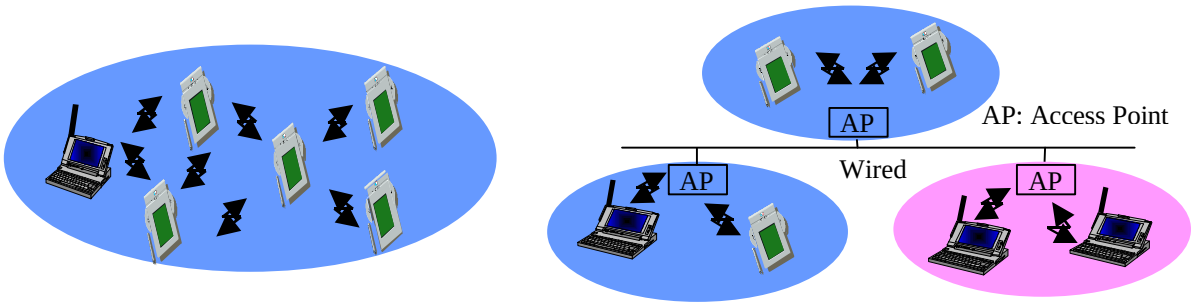
Abstract. As more and more people enjoy the various services brought by mobile computing, it is becoming a global trend in today's world. At the same time, securing mobile computing has been paid increasing attention. In this article, we discuss the security issues in mobile computing environment. We analyze the security risks confronted by mobile computing and present the existing security mechanisms.

1. Mobile Computing At a Glance

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.

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 [2]. 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.



(a) Infrastructure-less Network (b) Infrastructure-based Network

Figure 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.

2.1 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 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.

2.2 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 is prone 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).

3. Security Countermeasures

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

3.1 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.

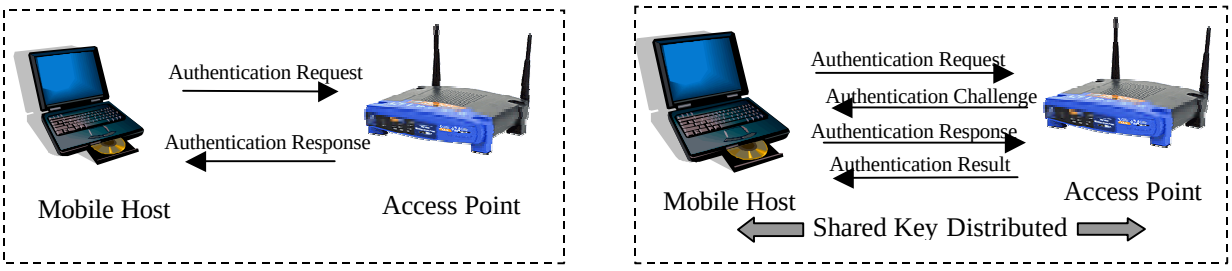
Non-repudiation ensures that an entity can prove the transmission or reception of information by another entity, i.e., a sender/receiver cannot falsely deny having received or sent certain data.

3.2 WLAN Basic Security Mechanisms

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.



Open System Authentication

Shared Key Authentication

Figure 2. IEEE 802.11 Authentication Modes

Authentication: In a WLAN, an AP must authenticate a client before the client can associate with the AP or communicate with the network. The IEEE 802.11b standard has defined two types of authentication methods: open system and shared Key. Open system authentication allows any device to join the network, assuming that the device SSID matches the access point SSID. Alternatively, the device can use the "ANY" SSID option to associate with any available AP within range, regardless of its SSID. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. When wireless devices are configured to operate in this mode, Wired Equivalent Privacy (WEP) data encryption is used and it requires that the station and the AP have the same WEP Key to authenticate, thus preventing the client from sending and receiving data from the AP, unless the client has the correct WEP key. Figure 2 illustrates the two authentication modes. By default, IEEE 802.11b wireless devices operate in an open system authentication mode. Both of these authentication modes are one-way

authentication, i.e., the mobile clients can be authenticated by the APs, but the authenticity of APs is not authenticated. Thereby, a rogue node may masquerade as an AP and establish communication with the mobile nodes.

WEP-Based Security: WEP security protocol encrypts the communication between the client and an AP. It employs the symmetric key encryption algorithm, RC4 Pseudo Random Number Generator. Under WEP, all clients and APs on a wireless network typically use the same key to encrypt and decrypt data. The key resides in the client computer and in each AP on the network. The 802.11b standard does not specify a key-management protocol, so all WEP keys on a network usually must be managed manually and are static for a long period of time. This is a well-known security vulnerability. Support for WEP is standard on most current 802.11 cards and APs. WEP specifies the use of a 40-bit encryption key. The encryption key is concatenated with a 24-bit "initialization vector" (IV), resulting in a 64-bit key. This key is input into a pseudorandom number generator. The resulting sequence is used to encrypt the data to be transmitted. However, WEP encryption has been shown to be vulnerable to several cryptographic attacks that reveal the shared key used to encrypt and authenticate data, such as IV key reuse, keystream reuse, message injection, and so on [3][4]. Because of this, static WEP is only suitable for small, tightly managed networks with low-to-medium security requirements.

It is clear that these traditional WLAN security that relies on SSIDs, open system or shared key authentication, MAC address filtering, and static WEP keys is better than no security at all, but it is insufficient, and a new security solution is needed to secure mobile computing.

3.3 Advanced WLAN Security Mechanisms

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 "auto-re-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.

TKIP primarily addresses the shortcomings of WEP and fixes the well-known problems with WEP, including small initialization vector (IV) and short encryption keys. TKIP uses RC4, the same encryption algorithm as WEP to make it updateable from WEP, but it extends the IV from 24-bit to 48-bit in order to defend against the existing cryptographic attacks against WEP. Moreover, TKIP implements 128-bit encryption key to address the short-key

problem of WEP. TKIP changes the way keys are derived and periodically rotates the broadcast keys to avoid the attack that is based on capturing large amount of data encrypted by the same key. It also adds a message-integrity-check function to prevent packet forgeries. TKIP is part of the existing WPA industry standard.

Counter mode CBC-MAC is designed to provide link layer data confidentiality and integrity. A new strong symmetric encryption standard, advanced encryption standard (AES) is deployed, in which a 128-bit encryption key and 48-bit IV are used. Different from TKIP, counter mode CBC-MAC has little resemblance to WEP, and it is set to be a part of the second generation WPA standard.

IEEE 802.11x is an authentication and key management protocol, which is designed for wired LANs, but has been extended to WLANs. IEEE 802.11x authentication occurs when a client first joins a network. Then authentication periodically recurs to verify the client has not been subverted or spoofed. The centralized, server-based 802.11x authentication process for WLANs is shown is Figure 3. A mobile client sends an authentication request to an associated access point. The access point forwards the authentication information to a back-end authentication server via Remote Authentication Dial-In User Service (RADIUS) for verification. Once the verification process completes, the authentication server sends a response message to the access point that the client has been authenticated and network access should be granted. In 802.11i, the response message should contain the cryptographic keys sent to the client. After that, the access point transfers the mobile client to authenticated state and allows the access of the mobile client.

Figure 3. IEEE 802.11x Authentication

IEEE 802.1X is not a single authentication method; rather it utilizes Extensible Authentication Protocol (EAP) as its authentication framework. This means that 802.1X-enabled switches and access points can support a wide variety of authentication methods, including certificate-based authentication, smartcards, token cards, one-time passwords, etc. However, the 802.1X specification itself does not specify or mandate any authentication methods. Since switches and access points act as a "pass through" for EAP, new authentication methods can be added without the need to upgrade the switch or access point, by adding software on the host and backend authentication server. Several common EAP methods have been defined in various IETF draft or other industry documents, such as EAP-MD5, EAP-TLS, etc. While TKIP and counter mode CBC-MAC are still unimplemented by most vendors, 802.11x support is already integrated into some operating systems.

In summary, TKIP/WPA provides enhanced security for existing infrastructure. Counter mode CBC-MAC protects the data integrity and confidentiality and 802.11x presents a fully extensible authentication mechanism. Combining these techniques, 802.11i RSN is significantly stronger than WEP. However, 802.11i has not yet been standardized. It requires changes to firmware and software drivers and may not be backward-compatible with some legacy devices and operating systems. Hence, not all users will be able to take advantage of it. A phased adoption process for this standard is anticipated because of the large amount of installed 802.11 devices.

3.4 Additional Security Requirements of Ad Hoc Networks

As ad hoc networking is somewhat different from the traditional approaches, designing an efficient security scheme to protect ad hoc networks is confronted with several new requirements.

First, the key management mechanism should be implemented in a distributed fashion1. Ad hoc network is a distributed network, in which network connectivity and network services, for example, routing, are maintained by the nodes themselves within the network. Each node has an equal functionality. There are no dedicated service nodes, which can work as a trusted authority to generate and distribute the network keys or provide certificates to the nodes, as the certificate authority (CA) does in the traditional public key infrastructure (PKI) supported approaches. Even if the service node can be defined, keeping the availability of the service node to all the nodes in such a dynamic network is not an easy task. Moreover, with limited physical protection, the service node is prone to

[1] Here, we consider the ad hoc network working in a truly ad hoc mode. Depending on the network origin, an ad hoc network can be a planned network, in which some initial data structure such as pre-distributed public keys and shared keys can be assumed.

a single point of failure, i.e., by only damaging the service node, the whole network would be paralyzed. Thus, distributed key generation and management approach is needed to secure ad hoc networks.

Secondly, light-weight authentication and encryption scheme with resource awareness are required. The low resource availability necessitates their efficient utilization and prevents the use of complex authentication and encryption algorithms. Public-key cryptography based authentication and encryption mechanisms are fully developed in securing traditional networks. Unfortunately, generation and verification of digital signatures are relatively expensive, which limits its acceptance to ad hoc networks. Symmetric cryptography is more efficient than public-key based asymmetric primitives due to its moderate resource consumption, but it requires both the sender and receiver to share a secret. In ad hoc networks, the problem is how to distribute the shared keys safely so that only the two parties (correct sender and receiver) would get it and not anyone else. It is thus challenging to define some new efficient cryptography algorithms for designing a light-weight authentication and encryption scheme.

Thirdly, combination of intrusion prevention and intrusion detection mechanisms is necessary. The work on securing wireless ad hoc networks can be classified into two types, intrusion prevention and intrusion detection [12] [13]. Intrusion prevention implies developing secured protocols or modifying the logic of existing protocols to make them secure. Most of the key based security protocols belong to this type. The idea of intrusion detection is to characterize the user normal behavior within the network in terms of a set of relevant system features. Once the set of system features is selected, the classification model is built to detect the anomalies from its normal behavior. Currently, the research on intrusion prevention and intrusion detection is done separately, and intrusion prevention has been paid more attention. But actually, they are not independent of each other, and should work together to provide security services. For example, intrusion prevention approaches can efficiently deal with the attacks coming from the outsiders by constraining the network access control, but it has no way to handle the denial of service attacks performed by the compromised nodes who have all the keys to access the network. Indeed, some active attacks can be efficiently detected because of a large deviation of attackers' behavior from the normal user behavior. Therefore, a security scheme combining these two mechanisms is suitable to better secure ad hoc networks.

3.5 Security Schemes for Ad Hoc Networks

In the recent research of security in wireless ad hoc networks, several good security approaches have been proposed, and they generally fall into three categories, secure routing, trust and key management, and service availability protection.

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.

Using public-key cryptography imposes a high processing overhead. Some researchers have proposed the use of *symmetric* key cryptography for authenticating ad hoc routing protocols, based on the assumption that a security association (a shared key K_{SD}) between the source node S and the destination node D exists. In [7], a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol, called SEAD, has been proposed. In this approach, one-way hash function is employed to authenticate routing updates sent by a distance-vector protocol. Another approach, Ariadne [8], proposed by the same authors, uses one broadcast authentication scheme TESLA [9] for securing DSR routing protocol. Venkatraman and Agrawal [10] have proposed a scheme that prevents replay attack by authenticating route reply messages. The scheme implements *Message authentication code* (MAC) to ensure integrity of route request packets. Papadimitratos and Hass [11] also proposed a symmetric key based Securing Routing Protocol (SRP), which can be applied to several existing routing

protocols. Symmetric encryption is more suitable for ad hoc networks due to its lower resource consumption. The problem is how to distribute the key in the first place.

Some efforts are also being made to use intrusion detection mechanism in protecting ad hoc networks. Zhang and Lee [12] present a distributed intrusion detection and response architecture, which provides an excellent guide on designing intrusion detection system in wireless ad hoc networks. Sergio Marti et al. [13] introduced Watchdog and Pathrater techniques that improve throughput in an ad hoc network by identifying misbehaving nodes that agree to forward the packets but never do so. The Watchdog can be considered as a simple version of intrusion detection agent to identify misbehaving nodes, and the Pathrater works as the response agent to help routing protocols avoid these nodes. However, the Watchdog can only detect the nodes who do not forward the packets, and the method only works on the source routing protocol since two-hop routing information is needed. In [14], two different detection models, distributed hierarchical model and completely distributed model, are proposed and the intrusion detection can be performed in a supervised or unsupervised way depending on the availability of attack data. The main problems of intrusion detection approach rely on two aspects: first, not all malicious behaviors are detectable, in particular, the dynamically changing topology in ad hoc networks makes detection more difficult; second, even if some attacks can be detected, a false alarm rate is still expected to be present. Therefore, intrusion detection usually works as a complementary approach to provide a second line of defense to the network.

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.

4. 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.

In this article, we discussed the security issues faced by mobile computing technology. We analyzed the various security threats and describe the existing current countermeasures. We have seen that many security solutions have been proposed to securing WLANs, but no one is able to claim that it solves all the security problems, or even most of them. In essence, secure mobile computing would be a long-term ongoing research topic.

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.

[9] A. Perrig, R. Canetti, B. Whillock, "TESLA: Multicast Source Authentication Transform Specification", *http://www.ietf.org/internet-drafts/draft-ietf-msec-tesla-spec-00.txt*, October 2002.

[10] 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*, Vol. 63, No. 2, Feb. 2003, pp. 214-227.

[11] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad Hoc Networks," *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, January 2002.

[12] 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.

[13] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *Proceedings of the 6th International Conference on Mobile Computing and Networking (MOBICOM'00)*, pp.255-265, August 2000.

[14] H. Deng, Q-A. Zeng, and D. P. Agrawal, "SVM-based Intrusion Detection System for Wireless Ad Hoc Networks," *IEEE Vehicular Technology Conference*, Orlando, October 6-9, Fall, 2003.

[15] L. Zhou and Z. J. Hass,"Securing Ad Hoc Networks," *IEEE Networks Special Issue on Network Security*, November/December, 1999.

[16] 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 (ICNP'01)*, 2001.

[17] Levente Buttyan and Jean-Pierre Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc WANs," *Proceedings of the IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Boston, MA, USA, August 2000.

[18] Pietro Michiardi, Refik Molva, "Core: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks," Proceedings of the Conference on Communication and Multimedia Security, 2002.

Acknowledgment

This work has been supported by the Ohio Board of Regents, Doctoral Enhancement Funds and the National Science Foundation under Grant No. CCR-0113361.