Volume: 03, Issue: 01 Pages:1012-1016 (2011)

Disseminated Public-Key Management and Certificate Generation Scheme for MANET

Sanjay Kumar Chowlam
Department of Master of Computer Applications, Sri Krishna Devaraya University, Anantapur
Email: sanju_c2000@yahoo.com
Dr. N. Geethanjali
Department of Master of Computer Applications, Sri Krishna Devaraya University, Anantapur
Email: geethanjali.sku@gmail.com

----------**ABSTRACT**----------

In this paper, we first discuss the predominant assail abilities in the mobile ad hoc networks, which have made it much easier to prone to attacks than the traditional wired network. Then we discuss the basic operations of our public-key management scheme: creation of public (and private) keys, issuing public-key certificates, storage of certificates, and key authentication by the nodes themselves without the control of any principal authority. More over the public key management scheme serves as an underlying mechanism for both key distribution and establishing security relationships between nodes.

Keywords – **Mobile Adhoc Network, Ubiquitous, Public key, Assail ability, Misbehaving Users.**

Date of Submission: February 18, 2011 Revised: April 24, 2011 Date of Acceptance: April 28, 2011

I. INTRODUCTION

In recent years, the explosive growth of mobile computing devices, which mainly include laptops, personal digital assistants (PDA s) and handheld digital devices, has impelled a revolutionary change in the computing world: computing will not merely rely on the capability provided by the personal computers, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer science society [1]. In the ubiquitous computing environment, individual users utilize, at the same time, several electronic platforms through which they can access all the required information whenever and wherever they may be [2]. The nature of the ubiquitous computing has made it necessary to adopt wireless network as the interconnection method: it is not possible for the ubiquitous devices to get wired network link whenever and wherever they need to connect with other ubiquitous devices. The Mobile Ad Hoc Network is one of the wireless networks that have attracted most concentrations from many researchers.

A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension [3]. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication 2 automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. The mobile ad hoc network has the following typical features [4]:

Unreliability of wireless links between nodes: Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.

Constantly changing topology: Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.

Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of assail abilities in the statically configured routing protocol. Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the awful behaviors than the traditional wired networks.

Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks.

The rest of the paper is organized as follows: In Section 2, we discuss the predominant assail abilities that make the mobile ad hoc networks not secure. In Section 3, we survey the current security solutions for the mobile ad hoc networks and analyze the feasibility of them. In Section 4, we draw the conclusion for the paper and point out some potential works in the future.

Volume: 03, Issue: 01 Pages:1012-1016 (2011)

II. ASSAIL ABILITIES OF THE MOBILE AD HOC NETWORKS

Because mobile ad hoc networks have far more assail abilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network. In this section, we discuss the various assail abilities that exist in the mobile ad hoc networks.

2.1. Lack of Secure Boundaries

The meanings of this assail ability is self-evident: there is not such a clear secure *boundary* in the mobile ad hoc network, which can be compared with the clear line of defense in the traditional wired network. This assails ability originates from the nature of the mobile ad hoc network: freedom to join, leave and move inside the network.

In the wired network, adversaries must get physical access to the network medium, or even pass through several lines of defense such as firewall and gateway before they can perform awful behavior to the targets [6]. However, in the mobile ad hoc network, there is no need for an adversary to gain the physical access to visit the network: once the adversary is in the radio range of any other nodes in the mobile ad hoc network, it can communicate with those nodes in its radio range and thus join the network automatically. As a result, the mobile ad hoc network does not provide the so-called secure boundary to protect the network from some potentially dangerous network accesses.

Lack of secure boundaries makes the mobile ad hoc network susceptible to the attacks. The mobile ad hoc network suffers from all-weather attacks, which can come from any node that is in the radio range of any node in the network, at any time, and target to any other node(s) in the network. To make matters worse, there are various link attacks that can jeopardize the mobile ad hoc network, which make it even harder for the nodes in the network to resist the attacks. The attacks predominantly include passive eavesdropping, active interfering, and leakage of secret information, data tampering, message replay, message contamination, and denial of service [4].

2.2. Threats from Compromised nodes inside the Network

In the previous subsection, we mainly discuss the assail ability that there is no clear secure boundaries in the mobile ad hoc network, which may cause the occurrences of various link attacks. These link attacks place their emphasis on the links between the nodes, and try to perform some awful behaviors to make destruction to the links. However, there are some other attacks that aim to gain the control over the nodes themselves by some unrighteous means and then use the compromised nodes to execute further actions. This assail ability can be viewed as the threats that come from the compromised nodes inside the network.

Since mobile nodes are autonomous units that can join or leave the network with freedom, it is hard for the nodes themselves to work out some effective policies to prevent the possible awful behaviors from all the nodes it communicate with because of the behavioral diversity of different nodes. Furthermore, because of the mobility of the ad hoc network, a compromised node can frequently change its attack target and perform awful behavior to different node in the network, thus it is very difficult to track the awful behavior performed by a compromised node especially in a large scale ad hoc network. Therefore, threats from compromised nodes inside the network are far more dangerous than the attacks from outside the network, and these attacks are much harder to detect because they come from the compromised nodes, which behave well before they are compromised.

From above we find that the threats from compromised nodes inside the ad hoc network should be paid more attention, and mobile nodes and infrastructure should not easily trust any node in the network even if it behaves well before because it might have been compromised.

2.3. Lack of Principal Management Facility

Ad hoc networks do not have a principal piece of management machinery such as a name server, which lead to some assailable problems. Now let us discuss this problem in a more detailed manner.

First of all, the absence of principal management machinery makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic in a highly dynamic and large scale ad hoc network [7]. It is rather common in the ad hoc network that benign failures, such as path breakages, transmission impairments and packet dropping, happen frequently.

Therefore, awful failures will be more difficult to detect, especially when adversaries change their attack pattern and their attack target in different periods of time. For each of the victims, because it can only observe the failure that occurs in itself, this short-time observation cannot produce a convincing conclusion that the failure is caused by an adversary.

However, we can easily find from a system point of view that the adversary has performed such a large amount of misbehaviors that we can safely conclude that all of the failures caused by this adversary should be awful failure instead of benign failure, though these failures occur in different nodes at different time. From this example we find that lack of principal management machinery will cause severe problems when we try to detect the attacks in the ad hoc network.

Second, lack of principal management machinery will impede the trust management for the nodes in the ad hoc network [4]. In mobile ad hoc network, all the nodes are required to cooperate in the network operation, while no security association (SA2) can be assumed for all the network nodes. Thus, it is not practical to perform an *a priori* classification, and as a result, the usual practice of establishing a line of defense, which distinguishes nodes as

trusted and non trusted, cannot be achieved here in the mobile ad hoc network.

Third, some algorithms in the mobile ad hoc network rely on the cooperative participation of all nodes and the infrastructure. Because there is no principal authority, and decision making in mobile ad hoc network is sometimes decentralized, the adversary can make use of this assail ability and perform some attacks that can break the cooperative algorithm [6].

In one word, the absence of centralized management machinery will cause assail ability that can influence several aspects of operations in the mobile ad hoc network. Thus we should work out some solutions to deal with this problem, which might be discussed in the later section.

2.4. Scalability

Finally, we need to address the scalability problem when we discuss the assailability in the mobile ad hoc network [4]. Unlike the traditional wired network in that its scale is generally predefined when it is designed and will not change much during the use, the scale of the ad hoc network keeps changing all the time: because of the mobility of the nodes in the mobile ad hoc network, you can hardly predict how many nodes there will be in the network in the future. As a result, the protocols and services that are applied to the ad hoc network such as routing protocol and key management service should be compatible to the continuously changing scale of the ad hoc network, which may range from decades of nodes to hundreds of nodes, or even thousands of nodes. In other words, these protocols and services need to scale up and down efficiently.

2.5. Assail ability of the Mobile Ad Hoc Networks: Summary

From the discussion in this section, we can safely conclude that the mobile ad hoc network is insecure by its nature: there is no such a clear line of defense because of the freedom for the nodes to join, leave and move inside the network; some of the nodes may be compromised by the adversary and thus perform some awful behaviors that are hard to detect; lack of principal machinery may cause some problems when there is a need to have such a principal coordinator; and continuously changing scale of the network has set higher requirement to the scalability of the protocols and services in the mobile ad hoc network. As a result, compared with the wired network, the mobile ad hoc network will need more robust security scheme to ensure the security of it. In the next section, we will discuss several security concerns that can provide some help to improve the security environment in the ad hoc network.

III. BASIC OPERATIONS OF PUBLIC-KEY MANAGEMENT SCHEME

In this section, we discuss basic operations of our public-key management scheme: creation of public (and private) keys, issuing public-key certificates, storage of certificates, and key authentication by the nodes themselves without the control of any principal authority.

3.1. Creation of public keys

The public key and the corresponding private key of each user are created locally by the user herself.

3.1.1. Issuing public key certificates

We assume that if a user u believes that a given public key Kv belongs to a given user v, then u can issue a public-key certificate in which Kv is bound to v by the signature of u. There may be many reasons for u to believe that Kv belongs to v. For instance, u may receive Kv on a secure channel that is associated with v, or someone trusted by u claims that Kv belongs to v, etc.

This step can be represented graphically as shown in figure 2.8.

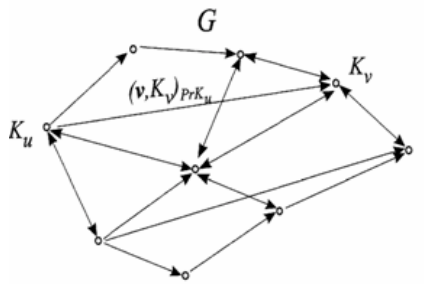

Fig 2.8: Issuing of public key certificates.

3.1.2. Storage of certificates

Certificates issued in the system are stored by the users in a fully decentralized way. Each user maintains a local certificate repository that has two parts: First, each user stores the certificates that she issued. This is necessary in order to store all the certificates of the system at least once. Second, each user stores a set of additional certificates (issued by other users) selected according to an appropriate algorithm. This additional set of certificates is obtained from other users by communicating with their nodes in the network. Here, we assume that some underlying routing mechanisms do exist.

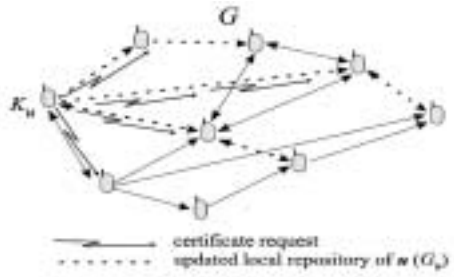

Fig 2.9: Node u constructs its updated repository by communicating with other nodes.

3.1.3. Key Authentication

When a user u wants to obtain the authentic public key Kv of another user v, she asks other users (possibly v herself) for Kv. In order to verify the authenticity of the received

key, v or the user who supplied the key to u also provides u with (a subset of) her local certificate repository. Then, u merges the received repository with her own repository and tries to find an appropriate certificate chain from Ku to Kv in the merged repository. If this fails, u may ask other users for further certificates. For simplicity, we assume that u receives Kv and the certificates that she merges to her local certificate repository from v herself.

3.1.4. Dealing with Misbehaving Users

So far, we assumed that users are honest and do not issue false certificates. However, a dishonest user may try to trick other users into believing in a false key-user binding by issuing false certificates. A dishonest user d may issue several types of false certificates. First, she may issue a certificate that binds a key Kv to a user f instead of user v. In this way, user d may trick other users to believe that Kv is the public key of user f, when it is really the public key of user v. Second, she may issue a certificate that binds user v to a false key K'v, which may then cause other users to believe that K'v is really the key of user v. Third; a malicious user can invent a number of user names and public keys and bind them by appropriate certificates. The malicious user can then use these public keys to issue false certificates and try to convince a given user that the certificates are correct, as they were signed by many other users. As we will see, in our project these attacks are prevented by allowing nodes to detect inconsistent certificates and to determine which user-key bindings are correct.

The certificate exchange mechanism allows nodes to gather all certificates from neighbor nodes. This enables nodes to cross-check user-key bindings in certificates that they hold and to detect any inconsistencies (i.e., conflicting certificates). Two certificates are considered to be conflicting if they contain inconsistent user-key bindings (i.e., if both certificates contain the same username but different public keys, or if they contain the same public-key, but are bound to different usernames).

If a certificate received by a node u contains a user-key binding (v,K_v) not contained in any certificate in the certificate repository of u, then (v,K_v) and the certificates that certify it are labeled by u as unspecified. A certificate labeled unspecified means that the node does not have enough information to assess whether the user-key binding in the certificate is correct. From the moment that (v, K_v) is received, u waits for a predefined period T_P. If within this period u does not receive any conflicting certificates regarding (v,K_v), the status of this binding and of the certificate that certifies it changes to non conflicting. Here, we note that T_P needs to be longer than the expected certificate exchange convergence time T_{CE}. If indeed $T_P > T_{CE}$, nodes will detect inconsistent certificates for all users that exist in the network. For this, each node initially issues a self-signed certificate and exchanges it with other nodes by the certificate exchange mechanism. Thus, the waiting period T_P is actually the expected time for any self-signed certificate to reach all the nodes in the network. However, this mechanism does not prevent users from creating virtual identities or from stealing the identity of people that do not participate in the network.

If a certificate received by a node u contains a user-key binding (v,K_v) that conflicts with a user-key binding (v,K'_v) contained in another certificate held by u, both bindings (v,K_v) and (v,K'_v) and the certificates that certified them are labeled conflicting. To resolve the conflict, u tries to find chains of no conflicting and valid certificates to public-keys K_v and K'_v.

3.1.5. Basic operations of public-key management scheme: Summary

In this part, we predominantly discussed the basic operations of our public-key management scheme: creation of public (and private) keys, issuing public-key certificates, storage of certificates, and key authentication by the nodes themselves without the control of any principal authority

IV. CONCLUSION

In this paper, we try to examine the predominant assail abilities in the mobile ad hoc networks, which have made it much easier to prone to attacks than the traditional wired network. Then we discuss the basic operations of our public-key management scheme: creation of public (and private) keys, issuing public-key certificates, storage of certificates, and key authentication by the nodes themselves without the control of any principal authority

First we briefly introduce the basic characteristics of the mobile ad hoc network.

We then discuss some typical and dangerous assail abilities in the mobile ad hoc networks, most of which are caused by the characteristics of the mobile ad hoc networks such as mobility, constantly changing topology, open media. The existence of these assail abilities has made it necessary to find some effective security solutions and protect the mobile ad hoc network from all kinds of security risks.

Finally we discussed the basic operations of our public-key management scheme: creation of public (and private) keys, issuing public-key certificates, storage of certificates, and key authentication by the nodes themselves without the control of any principal authority

REFERENCES

[1] Marco Conti, Body, *Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks* (Chapter 1), CRC Press LLC, 2003.

[2] M. Weiser, The Computer for the Twenty-First Century, *Scientific American*, September 1991.

[3] M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet based Mobile Ad Hoc Networking, *IEEE Internet Computing*, pages 63–70, July-August 1999.

[4] Amitabh Mishra and Ketan M. Nadkarni, *Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad*

Hoc Wireless Networks (Chapter 30) (CRC Press LLC, 2003).

[5] Lidong Zhou and Zygmunt J. Hass, *Securing Ad Hoc Networks*, IEEE Networks Special Issue on Network Security, November/December 1999.

[6] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book *Ad Hoc Networks Technologies and Protocols (Chapter 9) (*Springer, 2005).

[7] Panagiotis Papadimitraos and Zygmunt J. Hass, Securing Mobile Ad Hoc Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 31)* (CRC Press LLC, 2003).

[8] P. Papadimitratos and Z. J. Hass, "Secure routing for mobile ad hoc networks", in Proceedings of *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS),* San Antonio, TX, January 2002.

[9] Y. Hu, A. Perrig and D. Johnson, Ariadne: "A secure on-demand routing protocol for ad hoc networks", *in Proceedings of ACM MOBICOM'02,* 2002

[10] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer," A secure routing protocol for ad hoc networks", in *Proceedings of ICNP'02,* 2002.

[11] Y. Hu, D. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", *Ad Hoc Networks, 1 (1): 175–192*, July 2003.

[12] Jim Parker, Anand Patwardhan, and Anupam Joshi," Detecting wireless misbehavior through cross-layer analysis", in Proceedings of *the IEEE Consumer Communications and Networking Conference Special Sessions (CCNC'2006*), Las Vegas, Nevada, 2006.

[13] P. Krishna, N. H. Vaidya, M. Chatterjee and D. K. Pradhan, "A cluster-based approach for routing in dynamic networks", *ACM SIGCOMM Computer Communication Review, 27(2):49–64,* 1997.

[14] Sergio Marti, T. J. Giuli, Kevin Lai and Mary Baker, "Mitigating routing misbehavior in mobile ad hoc networks", in Proceedings of *the 6th annual international conference on Mobile computing and networking (MobiCom'00), pages 255–265,* Boston, MA, 2000.

Authors Biography

Sanjay Kumar Chowlam has obtained Master of Computer Applications degree from Sri Krishnadevaraya University, Anantapur. He is working as an Assistant Professor in the Department of MCA. He also held the additional responsibility of Assistant Training and Placement officer for 2 years. He has a total of 4.7 years of teaching experience. His areas of interests are Cryptography, Network Security and Software Engineering.

Dr. N. Geethanjali has obtained Master of Science Degree from Sri Krishnadevaraya University, Anantapur. She has obtained PhD in 2004 from Sri Krishnadevaraya University. She is working as Associate Professor in Department of Computer Science & Applications. She has more than 18 years of teaching experience for both UG and PG Courses. Her areas of interests are Data mining, Data Communications, Artificial Intelligence, Cryptography, Network Security, and Programming Languages.