International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 4, April-2014, pp: (386-388), Impact Factor: 1.252, Available online at: www.erpublications.com

Improved Distributed Certificate Authority revocation in secure cluster-based Mobile ad hoc network

C. Padma Priya[1], Mr. T. Ganesan[2]
[1]Department of CSE, E.G.S. Pillai Engineering College, Tamilnadu, India
[2]Associate Professor, E.G.S. Pillai Engineering College, Tamilnadu, India

Abstract: The Mobile Ad Hoc Networks (MANETs) having wireless and dynamic nature. MANETs are more susceptible to security attacks rather than wired networks. So they are vulnerable to security attacks from malicious node due to which it is important to detect malicious nodes to avoid attacks. In this paper certificate Authority Revocation (CAR) provides its secret key to all nodes (normal). To secure communication in mobile ad hoc network is extremely challenging because of the dynamic nature of the network and the lack of centralized management. This makes public key cryptographic services particularly difficult to support. We propose a distributed certificate authority revocation intended for deployment in dynamic cluster-based architecture. We also outline procedures for maintaining this distributed certificate authority amongst a highly dynamic membership of shareholding nodes.

Keywords: CA, CAR, DCAR, MANET.

1. INTRODUCTION

Mobile ad hoc networks or MANETs are vulnerable to various passive and active security attacks that are launched by internal and external attackers. But because of special characteristics of MANETs, such as lack of any fixed infrastructure, mobility of nodes and limited bandwidth of wireless communication, establishing security in MANETs is a challenging issue. Numerous solutions have been designed and presented in the literature to increase the security level of these networks. Certificate authorities are trusted third parties that are used for issuing, revoking and managing of user certificates. The mobile ad hoc networks have made their security a real concern. As a result, mobile ad hoc network security has been subject to extensive recent study. While much attention has been spent looking at security of routing protocols in ad hoc networks, for example [1] it is equally important to secure communications in ad hoc networks. In order to employ security mechanisms that are based on public key technology, it is necessary to establish the supporting key management infrastructure, which is normally based around the concept of a certificate authority (CA). The security implemented in mobile ad hoc networks is particularly challenging in network.

The use of key management in which public key, secrete key is shared between the Certificate Authority (CA) and other nodes. CA signs certificates of nodes presents in the network. CA [5] plays an important role in enhancing the network security. It digitally signs a valid certificate for each node to ensure that nodes can communicate with each other in the network. In such type of network CA invalids the attacker certificate for keeping network secured. If there are much of accusers showing that it is an attacker, then attacker's certificate can be revoked. But, it is not possible to determine, is it accusations are false or true. So, there is needed to take it into account the issue of false accusations.

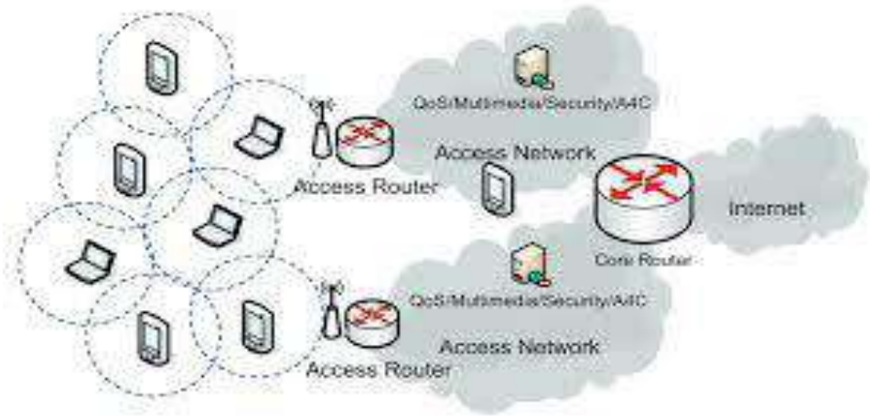

Figure 1: Mobile ad hoc network

1.1 Internal Attacks

In MANET, several different types of attacks that cause threat, due to their dynamic nature, each type of attack is different from another. Among them some are active and others are passive. Active attacks may be internal or external. The internal type of attacks launches attack inside of MANET, so it is dangerous when the node is considered as a trusted node at beginning .They directly leads to the attacks on nodes present in the network. It may broadcast wrong type of routing information to other nodes.

1.2 External Attacks

External attacks try to cause congestion in the network, Denial of Services (DoS) [4].Some external attacks are modification attacks, dropping attacks, fabrication attacks and timing attacks.

An attractive idea is thus to distribute a CA's functionality amongst ad hoc network nodes. A Distributed Certificate Authority Revocation (DCAR) is realized through the distribution of the CA's private key to a number of special shareholding DCAR nodes [4]. When CAR-related operations are required, such as issuing or signing a certificate, checking public keys, or revoking certificates, a threshold of available shareholding DCAR nodes should participate in the operation. In our proposed method of the security is used for detecting security considerations in real time network process. The process was developed into real time accuracy for providing security aspects presented in the transferring of data from one node to another node present in the real time network processing data. The certificate revocation protocol for ad hoc networks provides a measure protection against false accusation attacks. It rectifies the issue of certificate revocation without taking any input from external entities. Information that are used to decide whether the certificate of node should be revoked or not, that information is shared by all the nodes. The responsibility is given to individual node for certificate revocation and for maintaining information about the status of the certificates of the peers with which they are communicating.

2. RELATED WORK

They have several different types of certificate revocation techniques have been developed for mobile ad hoc networks. The most popular method is a simple certificate control approach by using a Certificate Revocation List (CRL) [7] which is managed by a single CA or shared among multiple CAs. A digital certificate which is valid for a certain time period is assigned to each node by the CA. The CA revokes the certificates of suspicious nodes and adds them to the CRL. Nodes can be accused by any node with a valid certificate and the updated CRL is broadcasted throughout the entire network. The Secure clustering-based certificate revocation scheme that was centralized CA manages certificates for all the nodes in the network. Secure cluster construction is decentralized and performed autonomously [5]. The nodes cooperate to form clusters and each cluster consists of a Cluster Head (CH) along with several Cluster Members (CMs) that are located within the communication range of their CH. The aim of using clusters is to enable CHs to detect false accusations. A CH will send a Certificate Recovery Packet (CRP) to the CA to recover an accused node, particularly in the case where it is a CM in its cluster. Finally we will develop Threshold based mechanism for developing insurance like peak value representation of transferring data from one node consumption to another node present in real network.

The CA to recover the certificates of falsely accused nodes can only be made from CHs. A CH will send a Certificate Recovery Packet (CRP) to the CA to recover an accused node, only in the case where it is a CM in its cluster [3]. This is based on the fact that most types of attacks, such as flooding attack, black hole attack, wormhole attack and Sybil attack, can be detected by any node within the communication range of the attacker. In other words, a CH will be able to detect any attack executed by one of its CMs, implying that a CH can identify whether a CM is malicious or not [4]. Since the CA regularly broadcasts certificate information on nodes which have been accused as malicious nodes, CHs will be able to detect false accusations against their CMs by comparing this information with their own local observations.

3. PROPOSED APPROACH

The secure cluster heads are linked together to form the network backbone. Secure clusters are formed of mobile nodes within one communication hop from the cluster head. Inter-cluster communication is restricted to cluster heads only. Inside a cluster, nodes can communicate directly if they are within one hop of one other, otherwise all communications must pass through the cluster head. A Cluster head thus functions as a gateway and the cluster heads collectively share responsibility for maintaining the routing backbone. This requires cluster heads to constantly monitor and distribute amongst themselves information about changes that occur on the backbone. To get the better and fast revocation we propose a scheme based upon a clustering-based certificate revocation scheme, which outperforms other techniques in terms of being able to quickly revoke attackers' certificates and recover falsely accused certificates. To perform the clustering we use the cluster the nodes. It refers to clusters in the Manets. The scope of this scheme is to make the use of threshold cryptography and create a decentralized CA. Using threshold cryptography the duty of certificate authority is get distributed among several nodes present in the network thus the challenge with management service in MANETs can get resolved.

3.1 Distributed Certificate Authority Revocation (DCAR)

Architecture of a DCAR system specifies its consisting components that are needed for proper operation of a DCAR system. It also determines the functions and tasks of MANET nodes in a distributed certificate authority. Different schemes use different kinds of nodes for providing services, but generally we may have the following nodes in DCAR schemes:

- DCA share holders
- Repositories
- User nodes

There are schemes that use ordinary nodes for performing this task. DCAR schemes that support low number of user nodes do not use special nodes for repository and DCAR share holder or user nodes store their certificates themselves. Finally, although using multiple repositories increases the availability and fault tolerance system, it makes the repositories more vulnerable to security attacks. Thus their security should be established by monitoring and detecting compromised repository nodes. The next tier consists of one or more certificate repositories in each cluster. The top tier consists of DCAR servers. Within each cluster, a fixed number t of nodes are designated as repositories that store the certificates of the nodes within the cluster, the certificates of all servers, the counter-certificates of the network nodes, and the most recent version of the CRL. The repositories might also become compromised and thus become unavailable. However, up to r repositories may be compromised within a cluster before a new node within a cluster is elected to serve as a repository.

3.2 Certificate Revocation:

In addition to a certificate repository, each node is required to compile and maintain a status table. Initially, it is compiled from the data in the profile table, and updated simultaneously along with the latter when a new, pertinent accusation is

received. The status table is used to ascertain the status of a certificate. The principal aim of the scheme we presented is to prevent malicious accusations from succeeding in causing the revocation of certificates of well-behaving, trust worthy nodes. Secondly, to eliminate or considerably reduce the window of opportunity whereby revoked certificates can be accepted as valid. Our scheme is based on the premise that all accusations should not be treated equally. The Cluster Head CHs must be legitimate. Nodes can be classified into three different categories, normal nodes which are highly trusted, warned nodes with questionable trust, and attacker nodes which cannot be trusted. Only normal nodes are allowed to become CHs and accuse attackers by sending Attack Detection Packets (ADPs) to the CA. Nodes in the Warning List (WL) cannot become CHs or accuse attackers, but they can still join the network as CMs and communicate without any restrictions. Nodes classified as attackers are considered malicious and completely cut off from the network.

4. RESULTS AND DISCUSSIONS

We simulate a mobile ad hoc network with 50 normal nodes and a number of malicious nodes ranging from 10 to 60, which are distributed randomly terrains. The node's transmission range is set to be 250m. We use AODV as an IP routing protocol. Nodes follow the Random-Waypoint mobility model, in which each node moves to a randomly selected location at a constant speed and then chooses another random position after 5 seconds of pause time. The specific parameters are shown in Table 1. In the simulations, we assume that the proportion of misbehavior nodes is actually quite small in the network. A malicious node periodically launches attacks every 5 seconds that can be detected by other nodes within its one hop range. Each simulation was carried out 20 times.

4.1 The detection performance

The curves of the detections time described in the trend in contrast to the previous method on network. The detection time represents the amount of time needed to detect all malicious nodes in the network. By using the previous method, as expected in our analysis, when the number of malicious nodes is less than a specified value (40 in this simulation), the scheme works well and the detection time maintains only a slight escalation with the number of increasing malicious nodes. However, the curve suddenly increases drastically, implying a significant increase in the detection time required to detect the rest of malicious nodes.

4.2 Delay on network

The Delay calculated from packet delay on their network. if the data transmit from node to node intermediately have any traffic or jamming on their network to take some time of the data transmission, that is called as a End-to-End Delay on Network.

$$D = (Tr - Ts)$$

where, Tr is receive Time and Ts is sent Time.

CONCLUSION

A Secure cluster based Distributed Certificate Authority Revocation (DCAR) schema was used to perform quickly revoke attacker's certificate and recover their falsely accused certificates. But it has a limitation in capable of accusing malicious nodes with decreased overtime. So to identify this features we propose to develop a new method i.e. Threshold based approach to enhance secure cluster based distributed certificate authority revocation schema. It provides quick revocation, and it immediately revokes the certificates of attackers and small overhead for control traffic. The effectiveness of the certificate schema in mobile ad hoc networks has been demonstrated through exclusive simulation results. We present our approach of securing a MANET using threshold based intrusion detection system and a secure routing protocol was introduced. While the intrusion and detection system helps to detect attacks on data intrusion and detection processes with incorporate security features of non reputation and authentication without any availability certificate Authority mechanisms.

REFERENCE

[1]. L .Zhou, F.B. Schneider, R. V. Renesse, "Coca:a secure distributed online certification authority", Journal ACM Transactions on Computer Systems (TOCS), Volume 20 Issue 4, November 2002, PP.329-368.
[2]. Y. Dong, A.F.Sui, S.M. Yiu, V.O .K.Li, L.C.K. Hui, "Providing distributed certificate authority service in cluster-based mobile ad hoc networks", Computer Communications, 2007, pp. 2442–2452.
[3]. D. Dhillon, T.S.Randhawa, M.Wang, L.Lamont, "Implementing a fully distributed certificate authority in an OLSR MANET ", IEEE Wireless Communications and Networking Conference, 2004, pp. 682-688.
[4]. G.Chaddoud, K.Martin, "Distributed certificate authority in cluster-based ad hoc networks", 2006, Wireless Communications and Networking Conference, Vol.2, pp. 682-688.
[5]. W.Rao, S.H.Xie, "Merging clustering scheme in distributed certificate authority for ad hoc network", IET International Conference on Wireless, Mobile and Multimedia Networks, 2006, pp.1-4.
[6]. M.E.Elhdhili, L.B.Azzouz, F.Kamoun, "A totally distributed cluster based key management model for ad hoc networks".
[7]. D.Y.Lee, H. C.Jeong, "An efficient certificate management for mobile ad-hoc network", Lecture Notes in Computer Science, 2006, Volume 4104, 355-364.
[8]. C.Zouridaki, B.L.Mark, K.Gaj, R.K.Thomas, "Distributed ca-based PKI for mobile ad hoc networks using elliptic curve cryptography", First European PKI Workshop: Research and Applications, PP.232-245.
[9]. P.Xia, M.Wu, K.Wang,X.Chen, "Identity-based Fully Distributed Certificate Authority in an OLSR MANET", 2008, 4th International Conference on Wireless Communications, Networking and Mobile Computing, PP.1-4.
[10]. S.Yi, R.Kravets, "MOCA:Mobile Certificate Authority for Wireless Ad Hoc Networks", 2nd Annual PKI Research Workshop Program, 2004.