ISSN:0975-9646

Study and Analysis on Certificate Revocation in MANETS

Naresh Kumar G , Mounika T ,Lingam Sunitha ,Venkata Ramana E, Sridevi

Abstract-In Mobile Ad hoc Networks (MANETs), certification systems play an important role to achieve network security. Handling the issue of certificate revocation in wired network is somewhat easy compared to the MANETs. In wired network when the certificate of a malicious node get revoked then the certificate authorities add the information about the revoked node in to certificate revocation lists (CRLs) otherwise broadcast the CRLs to each and every node present in the network or either store them on accessible repositories. Whereas the certificate revocation is a challenging task in MANETs and also this conventional method of certificate revocation is not useful for MANETs due to absence of centralized repositories and trusted authorities. In this paper, we propose a threshold based certificate revocation scheme for MANETs which will revoke the certificate of malicious nodes as soon as it detect the first misbehavior of nodes. The proposed scheme also solves the improper certificate revocation which can occur due to false accusations made by malicious node also the problem of window of opportunity where revoked certificates get assigned as a valid to new nodes.

Keywords: MANETs, Certificate Authority (CA), Certificate Revocation and Digital Certificate (DC).

1. INTRODUCTION

Mobile ad hoc networks (MANETs) are autonomous collection of mobile nodes which communicate over relatively bandwidth constrained wireless links. MANETs differ from conventional wireless networks, such as cellular networks and IEEE 802.11 (infrastructure mode) networks, in that they are self-containing: the network nodes can communicate directly with each other without reliance on centralized infrastructures such as base stations.

Additionally, MANETs are self organizing and adaptive they can therefore form and de-form on-the-fly without the need for any system administration. These unique features make MANETs very attractive for scenarios which will require rapid network deployment, such as search and rescue operations. The decentralized nature of MANETs, particularly the absence of centralized entities, and hence the avoidance of single point of failures, makes these network paradigms also ideal for military and commercial applications that require high degree of robustness. There are however some challenging security issues which need to be addressed before MANETs are ready for widespread commercial or military deployment.

One of the core security issues is trust management. Trust is generally established and managed in wired and other wireless networks via centralized entities, such as CAs or key distribution center (KDC). The absence of centralized entities in MANETs makes trust management security issue challenging task. The unavailability of trusted authorities also creates problem to perform necessary functions such as the revocation of DC. Another interesting MANET security problem is the issue of false accusation in the presence of malicious nodes, which will try to prove the legitimate node as malicious node due to which legitimate node get removed from the network. The malicious nodes can cause various communication problems such as window of opportunity problem.

The principal objective of this paper is to address the above-mentioned MANETs security issues such as implementing better trust management, Revoking certificate of malicious nodes only, solving false accusation and window of opportunity problem .The wireless technology makes MANETs more vulnerable to security attacks and due to this the traditional security methods does not provide a novel solution to MANETs . A new protocol need to be developed to overcome the drawback in the traditional security methods such as DC, Symmetric key cryptography method which will require trusted third party and central repositories to maintain information about node whose certificate is get revoked but these traditional security methods are yet fail in providing the desired security in the case of wireless networks such as MANET's. In other words, the scope of the traditional security methods is only limited to the wired networks and to some extent in the wireless networks because the number of security threats is greater in wireless networks compared to wired networks.An ultimate solution to such scenario is the threshold cryptography. This (k, n) threshold cryptography scheme was introduced by Shamir in. This scheme distributes trust and functionality of CA that provides efficient security measures to the wireless networks by distributing functionality of CA such as certificate validation, certificate revocation, managing certificate except issuing of certificate to all the nodes present in the network compared to the traditional cryptographic measures.

2. CERTIFICATE REVOCATIONS

Any data with a digital signature could be called a certificate. Certificates are tamper evident (modifying the data makes the signature invalid) and unforgivable (only the holder of the secret, signing key can produce the signature). These properties make certificates useful in conducting secure electronic transactions. When a certificate is issued, its validity is limited by an expiration date. However, there are circumstances (such as when a private key is revealed, or when a key holder changes affiliation or position) where a

certificate must be revoked prior to its expiration date Security requirements of wireless ad hoc networks are similar to that of other networks.

The aim of using clusters is to enable CHs to detect false accusations. Requests for 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. In order for clustering-based certificate revocation to work, 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.

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; it consists of the following info: Number of accusations against node i(Ai): The total number of accusations—limited to one per node—made against node i..Number of additional accusations made by node i(Alpha i): The total number of accusations—limited to one per node—made by node I minus one.

$$\beta_i = 1 - \lambda A_i \qquad (1)$$

$\lambda = \frac{1}{2N-3}$, where N is the node count.

Behavior index of node i: The behavior index of a node I (Beta i) is a number such that.0<Bi<=1. It is a measure of the status of a node amongst its peers. The greater the value of Bi, the higher the status of the given node i,Bi is computed as follows: Weight of node i accusation (wi): The weight of a node accusation or potential accusation (if the node has not made any accusation to-date), depends on the node's behavior index and the number of accusations it made. wi is a number. such that 0<=wi<=1. It can be calculated as follows.

$$\omega_i = \beta_i - \lambda\alpha_i \qquad (2)$$

Similarly, $\lambda = \frac{1}{2N-3}$, where N is the node count.

Revocation quotient (Rj) This number determines whether or not the certificate for node should be revoked. It is computed as follows:

$$R_j = \sum_{i=1}^{N} \sigma_{ij}\omega_i \qquad (3)$$

If an accusation graph is constructed using the data in the profile table, such that the nodes of the graph represent the network nodes, and the edges represent accusations;

Certificate status (C i): Indicates whether or not the certificate of node i is revoked.

Underlined principle of scheme

The principal aim of the scheme we presented is to prevent malicious accusations from succeeding in causing the revocation of certificates of well-behaving, trustworthy 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.

3. SYSTEM ARCHITECTURE

The total system architecture is given in the following Figure.

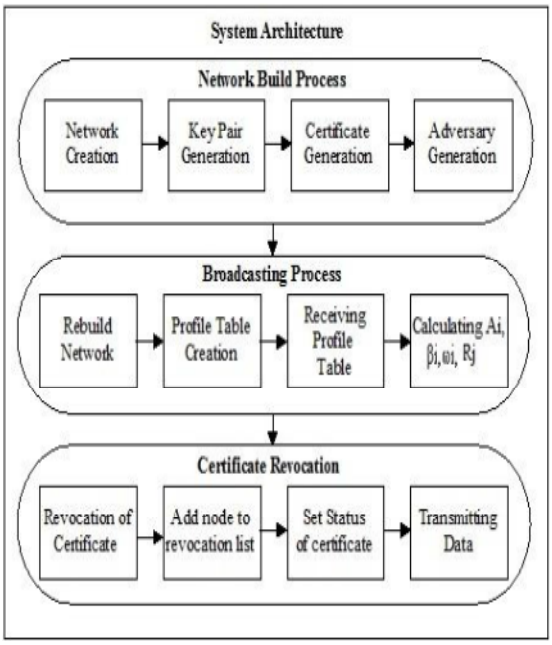

Figure 1: System Architecture

4. MODULES

4.1 Module 1- Network Creation

Network creation is the first module of the proposed scheme. The name itself will indicate that, it is used to create the network topology according to user requirement. To build the network, user needs to specify how many number of nodes 'N' needs to be present in the network so the network get created as per the user requirements. If user specifies N=5 then this module creates the network with 5 nodes. Following are some situations in which this module is not able to create network:

- If user has not provided the value of number of nodes N.
- If user has specified the negative value for the N.
- If user has given the floating value for the N.

In these 3 situations this module is not able to create the network.

4.2 Module 2- Certificate Acquisition and Certificate Storing

In the proposed scheme, the individual nodes within a network are responsible for all key management tasks such as certificate storing, assigning key pair to nodes, revoking certificate, except issuing of certificate due to the absence of central repositories and infrastructure support. The nodes in the MANETs need to be equipped with all aspect of network functionalities, such as routing, relaying packets etc thus the individual nodes in network is responsible for all key management task.

The certificate gets issued by a CA trusted by other network peers. A node is required to have a valid certificate issued by a CA before entering into a network. All the nodes present in network have valid certificate initially because after some period of time if it get detected as an adversary node then certificate of that node get revoked to protect the network. This module is used to issue the certificate to the nodes and store the certificate of all the nodes.

4.3 Module 3- Requests for PT

When any new node gets entered into the network then that node required to perform 2 things that are first job which the newly entered node is required to perform is:

Broadcast its certificate to all the nodes which are present in the network: The newly entered node is required to broadcast its certificate to all other nodes which are already present in the network so that the nodes already present in network obtain the information about it.

Send Request to all the nodes present in the network to send their PT: The newly entered node also required to simultaneously send request to all the nodes in the network to send their PT to obtain information about the nodes that has been detected as adversary before this new node has entered into the network. Using this information the newly entered node is able to send and receive data only form non-adversary node thus the network gets protected from adversary node.

4.4 Module 4-Certificate Revocation:

This module is used to revoke the certificate of the node that has been detected as an adversary. It makes use of the information present in the PT and constructs ST from it. The ST holds values of different parameters which will help to revoke the certificate of adversary node that are , , The value of , , parameters are get calculated from equation(1), equation(2) and equation(3). Users need to specify value of and if value of a node j exceeds then this module revokes the certificate of the node j otherwise not. The status of the node j whose certificate gets revoked is set true.

5. CASE STUDY

Suppose there is one network consisting 3 nodes as shown below Figure 2. It is not necessary that the every time when user creates network with N nodes at that time the position of N nodes will be the same as shown in below Figure 2 because in MANETs the position of the nodes does not fixed. In Figure2 nodes are represented by a mobile image and the number below the node indicate mobile node number.

Different tables are used to maintain information about the mobile nodes that are PT, ST, Certificate Repository table, Certificate Information table. The fields of these tables and their description are given below:

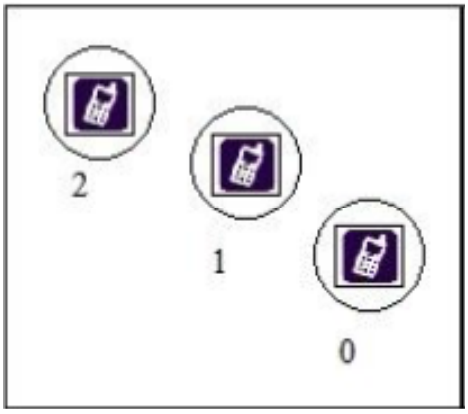

Figure 2: MANETs with 3 Nodes

5.1 Certificate Information Table:

Table 2: Certificate Information Table

Certificate Information Table At Node 1	
Fields	Value
Serial Number	1351511028573
Issuer DN	CN=Node No:1
Not Before	DD/MM/YY
Not After	DD/MM/YY
Version	1

Certificate information table get maintained by each and every node present in the network. The fields of certificate information table are shown in above Table2. It gives various information about certificate which is assigned to the node-1. It shows that, the certificate serial number of node-1 is 1351511028573 and other things.

The MANETs shown in Figure2 consisting of 3 nodes so the proposed scheme will maintain Table2 for node-0, node-1 and node-2 having information of node-0, node-1 and node-2 respectively.

Suppose user has selected node-1 as an adversary node as shown in below Figure 3.

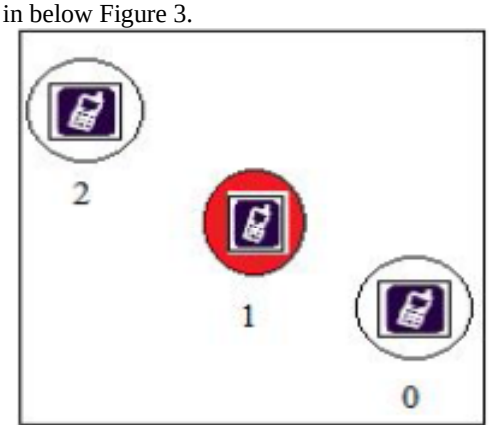

Figure 3: The adversary node indicated in red color.

5.2 Certificate Repository Table

Each and every node in the network maintains this table. It gives information about legitimate nodes. Table3 shows the fields of certificate repository table. After doing comparison of the fields present in Table2 and Table3 user will found that both tables are having same fields but they represent different information.

After making node-1 as an adversary node as shown in Figure3, the certificate repository table at node-1 gives the information as shown in Table3. Table3 gives information about node-0 and node-2 because these are legitimate nodes whereas node-1 is adversary node so it will not gives any information about node-1.

Table 3: Certificate Repository Table

Certificate Repository At Node: 1				
Serial Number	Issuer DN Not	Not Before	Not After	Version
1351511028420	CN=Node No:0	Mon Oct 29	Mon Oct 29	1
1351511028720	CN=Node No:2	Mon Oct 29	Mon Oct 29	1

5.3 Profile Table (PT):

It is also maintained by each and every node in the network. It gives information about adversary node whereas the PT at adversary node does not contain any information. Fields of the PT are shown in below Table 4.

Table 4: Profile Table

Profile Table of Node: 2			
Peer Id	Cert Signature	Cert Status	Accusation Date
1	1351511028573	TRUE	Mon Oct 29

Table4 gives information about node-1 only because user has made only node-1 as an adversary node as shown in above Figure 3.

6. CONCLUSION

In this paper we have seen that Ad hoc network security schemes utilizing threshold cryptography, potentially provide greater flexibility and security. However, the computational cost, particularly for low-powered wireless nodes, might be too prohibitive. In addition, these schemes require unselfish cooperation of the communicating peers, which cannot be guaranteed in certain networks environments. This paper proposed certificate revocation scheme for ad hoc networks, which provided some measures of protection against malicious accusation succeeding in causing the revocation of certificates of well-behaving nodes.

REFERENCES

1. Wei Liu, Hiroki Nishiyama, N. Ansari, N.Kato, "A study on Certificate Revocation in Mobile Ad Hoc Networks", IEEE 2011.
2. Claude Crêpeau and Carlton R. Davis," A Certificate Revocation Scheme for Wireless Ad Hoc Networks "School of Computer Science, McGill University, Montreal, QC, Canada H3A 2A7.
3. Arthur Conklin.W.M, Gregory B.Whit, Chuck Cothren, Dwayne Williams, Roger L .Davis, "Principles ofcomputer security", 2004.
4. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, November 1979.
5 L. Zhou and Z.J. Haas, "Securing ad hoc networks," IEEE Network Magazine, 13 (6), pp. 24-30, 1999.
6. K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate revocation to cope with false accusations in mobile ad hoc networks," Proc. 2010 IEEE 71st Vehicular Technology Conference: VTC2010-Spring, Taipei,Taiwan, May 16-19, 2010.
7. J. Clulow and T. Moore, "Suicide for the Common Good: A NewStrategy for Credential Revocation in Selforganizing Systems," ACMSIGOPS Operating Systems Reviews, vol. 40, no. 3, pp.18-21, Jul.2006.
8. H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: ubiquitous and robust access control for mobile adhoc networks," IEEE/ACM Trans. Networking, vol. 12, no. 6, pp.1049-1063, Oct. 2004.
9. G. Arboit, C. Crepeau, C. R. Davis, and Maheswaran, "A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks," Ad Ho Network, vol. 6, no. 1, pp. 17-31, Jan. 2008.
10. P. Sakarindr and N. Ansari, "Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless sensor networks," IEEE Wireless Communications, 14(5), pp. 8-20, 2007.
11. R. Housley, W. Polk, W. Ford, D. Solo, Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile, Internet Request for Comments (RFC 3280), April 2002.
12. M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, X.509 internet public key infrastructure online certificate status protocol – OCSP, Internet Request for Comments (RFC 2560), June 1999.

AUTHORS

Naresh kumar G pursuing M-Tech in Vidya Vikas Institute Of Technology,Chevella. His areas of intreast are computer networks and adhoc networks.

Mounika T pursuing M-Tech in "Vivekananda institute of science and information technology" chattanpally, shadnagar, mahabubnaga .Her areas of interested are adhoc networks and software engineering.

Lingam sunitha received her MCA from Kakatiya University in 1999, and M.Tech (CSE) from JNTU, Hyderabad in 2009. She is now working as Associate Professor and also pursuing Ph.D in Computer Science and Engineering from JNTU Hyderabad, India. Her area of specialization is Data Mining.

Venkata Ramana E,Hod Cse,Vidya Vikas Institute Of Technology,Chevella, and presently working as associate proessor and head of the department in vidya vikas institute of technology. Research intrestes includes computer networks and security.

Sridevi, working as Assistant professor in "Vivekananda institute of science and information and technology" at ShadNagar, Andrapradesh,India Her areas of intreast are computer networks and adhoc networks.