ISSN:0975-9646

Securing MANETs using Cluster-based Certificate Revocation Method: An Overview

Mrs. **Dipti S. Sawant**
Dept. of Computer Engineering,
Sinhgad College of Engineering,
Pune, India. 411 041

Prof. **J. E. Kamalasekaran**
Dept. of Computer Engineering,
Sinhgad College of Engineering,
Pune, India. 411 041

***Abstract*—Security is an important issue in Mobile Ad-hoc NETworks. It is difficult to secure MANET because of its dynamic topology and lack of infrastructure. Certificate Revocation is widely used and reliable method to secure the MANET. Certificate Revocation isolates the attackers from further participating in network activities. False accusation of legitimate node as an attacker node is an issue with certificate revocation system. This paper presents an overview of Cluster-based Certificate Revocation system, which can address the said issue. In this, Cluster Head (CH) plays an important role in detecting the falsely accused nodes within its cluster and revoking their certificates to solve the issue of false accusation. The following four modules of this system are discussed: 1) cluster communication, 2) function performed by Certificate Authority (CA), 3) classification of the nodes and 4) certificate revocation. This method overcomes the limitations of the existing certificate revocation schemes and enhances the network security and performance of MANET.**

***Keywords*— Mobile Ad-hoc Network, Certificate Revocation, Clustering, Certificate Authority (CA).**

I. Introduction

Mobile Ad-hoc NETwork (MANET) is a collection of wireless nodes such as laptops, cell phones, walkie-talkie etc. These nodes can be dynamically set up anywhere and anytime without using any pre-existing infrastructure. Fig. 1 shows structure of MANET. These nodes can communicate with each other via radio waves. In MANET communication is not limited within a range. Communication in MANET is achieved by intermediate nodes i.e. mobile nodes uses multi-hop communication [1]. MANET is an open network environment. In an open network environment, mobile nodes can join and leave the network at any time. That means MANETs are in dynamic nature. This wireless and dynamic nature of MANET makes them more vulnerable to various types of security attacks than wired networks. Any un-trusted node can join the network at any time and this cause the damage to the network by either dropping the packets or provides wrong information to the network i.e. mobile nodes can be attacked by malicious attackers and these attackers can disrupt the security. Protecting the legitimate nodes from the malicious attacks is achieved by using key management scheme.

Key management scheme [8] involves concept of certification. Certificates are signed by Certificate Authority (CA) to ensure that, nodes can communicate with each other in the network. CA acts as a Trusted Third Party (TTP). CA is responsible for distribution and management of the certificates. Management of the certificate includes issuing and revoking of certificates.

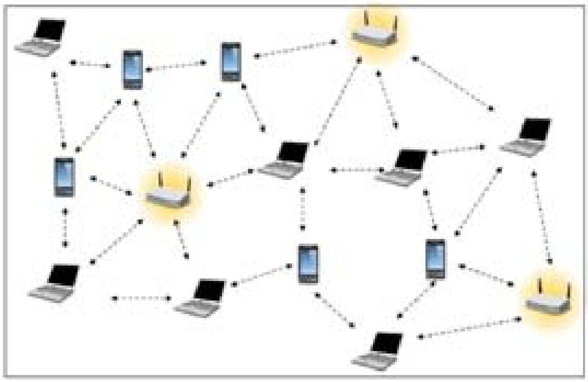

Fig. 1. Mobile Ad-hoc NETwork (MANET) Structure

Before nodes can join the network, they have to acquire a valid certificate from Certificate Authority (CA). Mechanism performed by the CA plays an important role in enhancing a network security. Sometimes, malicious nodes will try to remove the legitimate nodes from the network by falsely accusing them as an attacker. Therefore issue of false accusation must be considered during designing of certificate revocation mechanism. Cluster-based certificate revocation mechanism can be used to address this issue. The reminder of this paper is organized as follows. In Section II, brief overview of the related work on certificate revocation technique in MANET is discussed. Section III describes the structure of the cluster-based certificate revocation scheme and certificate revocation process. The entire concept is summarized in section IV. Finally future scope of work is given in Section V.

II. Related Work

Mobile Ad-hoc NETworks (MANETs) are very popular because of its infrastructure less nature. Security is an important issue in Mobile Ad-hoc NETworks. It is difficult to secure MANET because of its dynamic topology and lack of infrastructure. Certificate revocation scheme can be used to address this issue. Certificate revocation helps to quickly revoke attacker’s certificates and recover falsely accused certificates. Certificate revocation isolates the attackers from further participating in network activities.

Any data with a digital signature is known as a certificate [4]. Certification is considered as a primary task to secure network communication. A certificate revocation lists and removes the certificates of the nodes, which are detected to launch attacks on neighborhoods [3]. Thus, nodes which launch the attacks are removed from the network. In this way, certificate revocation provides secure communication in MANET.

A. Existing Method

Existing approaches for Certificate Revocation is classified into two categories as voting-based mechanism and non-voting-based mechanism.

1. Voting-based mechanism

In voting-based mechanism, malicious attacker's certificate is revoked through the votes from the valid neighboring nodes [1]. It is based on URSA (Ubiquitous and Robust Security Architecture) proposed by H. Luo et al. [6] and mechanism used in this is called as a voting-based mechanism. In URSA, two neighboring nodes receive their certificates from each other and also exchange the certificate information about other nodes that they know. Nodes sharing the same certificate information are regarded as belonging to the same network. In these networks, the certificate of a attacker node can be revoked when the number of accusations against the node exceeds a certain threshold. URSA does not use a Third-party component such as Certificate Authorities (CA).

Advantages:

- Voting based scheme having high accuracy to revoke the certificate.

Disadvantages:

- Decision process to satisfy the condition of certificate revocation is slow.
- There is high overhead to exchange the information.
- It takes longer time to judge the malicious node in a network or time increases to revoke the certificate because all the nodes are required to participate in voting.
- Operational cost is high.

2. Non-voting-based mechanism

In non-voting-based mechanism, a node with proper certificate can decide whether a node is malicious attacker or not [1]. It is based on decentralized suicide based approach, proposed by J. Clulow et al. [8]. In this approach, simultaneously certificates of both the accused and accusing node have to be revoked.

Advantages:

- It takes Fast decisions.
- It reduces the communication overhead.
- It takes the less time to judge the suspicious node.

Disadvantages:

- It having low accuracy.
- It having low reliability.

B. Limitations of Existing method

Certificate revocation method does not provide a mechanism to differentiate falsely accused legitimate nodes from properly accused malicious nodes. Because of this the accuracy and effectiveness are degraded.

C. Need of Cluster Based certification Revocation Method

Certificate Revocation with existing approaches has limitation that sometimes malicious nodes will try to remove legitimate nodes from the network by falsely accusing them as attackers. Also existing Voting-based and non-voting-based systems are having certain limitations in terms of cost, speed, accuracy, reliability and communication overhead.

Cluster-based approach can address this issue of false accusation. By the formation of cluster, it is easy to exchange the information between the interacting nodes. Cluster Head (CH) plays an important role in detecting the falsely accused nodes within its cluster and revoking their certificates to solve the issue of false accusation. It can achieve quick revocation and small overhead as compared to voting-based scheme and improves the reliability and accuracy as compared to non-voting-based scheme. Thus, cluster-based certificate revocation has ability to enhance the network security and performance of MANET.

.

III. Cluster Based Certificate Revocation Method

Clustering is the method of grouping the nodes present in the MANET. Due to cluster formation it is easy to exchange information between the interacting nodes. There can be more than one cluster and these clusters are communicate with each other. Nodes within this cluster are called as Cluster Members (CM). Every cluster will have Cluster Members (CMs) and a Cluster Head (CH). Cluster Heads are the backbone for communication in the network. Cluster Head (CH) is also called as a manager of the cluster. Communication between the adjacent clusters is managed by Cluster Gateway (GW). All the nodes will have certificate before joining the network, which they receive from certificate authority (CA) [3]. Fig. 2 shows the cluster members, cluster head and gateway nodes. Where,

CH= Cluster Head,
CM= Cluster Member,
GW= Gateway Node.

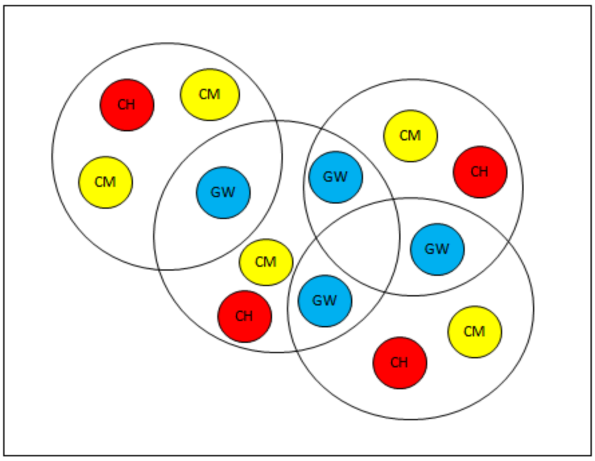

Fig. 2. Cluster Head and gateway nodes

Fig. 2 shows that there is availability of Custer Heads (CHs) in each cluster, which maintains the information of other nodes. Gateway nodes are also present in a clusters. Data is transmitted between two clusters through intermediate nodes i.e. Gateway Nodes (GW) only.

A. *Cluster-based Certificate Revocation Architecture*

Cluster-based Certificate Revocation consists of four modules such as –

1. Cluster Communication.
2. Functions performed by Certificate Authority (CA).
3. Node Classification.
4. Certificate Revocation.

1) *Cluster Communication:*

Each cluster consists of a Cluster Head (CH) with addition of some Cluster Members (CM’s). Both are located within the transmission range of their CH. The CH node sends a CH hello packet (CHP) to all of its neighboring nodes and those nodes are in CHs transmission range will accept the packet and replies with CM hello packet (CMP). After this they will join the cluster. Single CM belongs to two different clusters for providing robustness in a topology. So when it moves out of one range it can search for another CHP and join new cluster [1].

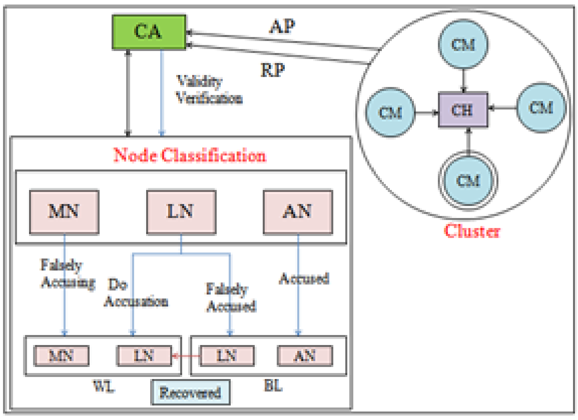

Fig. 3. System Architecture

Fig.3 shows system architecture.
Where,

AN = Attacker Node,
AP = Accusation Packet,
BL = Black List,
CM with double circle = Accused Node,
MN = Malicious Node,
LN = Legitimate Node,
RP = Recovery Packet,
WL = Warning List.

When the neighboring nodes detect the attacks from any one node in a cluster then each of the nodes can sends out an Accusation Packet (AP) to the Certificate Authority (CA) against the attacker node. According to the first received packet, the CA can holds neighboring node and attacker node in the Warning List (WL) and Black List (BL), respectively. After verifying the validity of the neighboring node, CA broadcasts the revocation message to all nodes in the network. After receiving the revocation message nodes update their local WL and BL to revoke the attacker’s certificate. Meanwhile, CH updates their WL and BL and determines that one of the nodes was framed. Then some of the nodes send Recovery Packet (RP) to the CA to get back the falsely accused node. Upon receiving the first Recovery Packet (RP), the CA removes the falsely accused node from the BL and WL can holds both the falsely accused node and normal node. After that, broadcast the information to all the nodes. Finally, the nodes update their WL and BL to recover the falsely accused node [5].

2) *Function performed by Certification Authority (CA):*

Cluster-based certificate revocation scheme includes two lists such as Warning List (WL) and Black List (BL). CA updates these two lists and then they are used to hold accusing and accused nodes information, respectively. BL is responsible for holding attacker node and WL is used to hold the corresponding accusing node. CA updates each list according to the received control packets. After that, the CA broadcasts the information of the WL and BL to the entire network in order to revoke the certificates of nodes which are present in the BL and isolate those nodes from the network [7].

3) *Node Classification:*

Nodes are classified on two bases:

a) Behavior based Node Classification: Nodes are classified according to their behavior as [9]-

- Legitimate node,
- Malicious node,
- Attacker node.

b) Reliability-based Node classification: Nodes are classified according to their reliability as [5]-

- Normal node,
- Warned node,
- Revoked node.

4) *Certificate Revocation:*

Certificate Revocation is an important task of removing the certificates of the attacker nodes from the network. If any node is misbehaved, it should be removed from the network by revoking the certificate.

Cluster-based certificate revocation [9] involves two basic tasks such as:

1. Procedure of Revoking Malicious Certificates
2. Certificate Recovery (False Accusation)

a) Procedure of Revoking Malicious Certificates:

The revocation procedure starts at detecting the presence of attacks from the attacker node. Then, the neighboring node checks the local list of BL to match whether this attacker node has been found or not. If attacker node is not found, the neighboring node broadcasts the Accusation Packet (AP) to the CA. After that, once receiving the first arrived accusation packet, the CA verifies the certificate validation of the accusing node. If certificate is valid, the accused node is considered as a malicious attacker and it is put into the BL. At the same time, the accusing node is present in the WL. Finally, CA broadcasts the information of BL and WL to all the nodes present in the network. Nodes that are present in the BL are successfully revoked from the network [9].

For example, a malicious attacker suppose node M launches attacks within it's one-hop transmission range, as shown in Fig. 4.

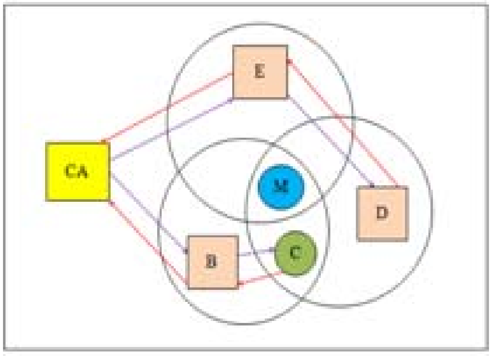

Fig. 4. Revoking a nodes certificate

Where,
Circle= Represents cluster,
M=Malicious Node,
C= Cluster Member,
B, D, and E= Cluster Heads,
CA= Certificate Authority.
Red Line= Indicates Accusation Packet,
Purple line= Indicates Broadcast Revocation Message.

Procedure of Revoking Malicious Certificates:

1) Malicious node such as node M launches attack on the neighboring nodes B, C, D, and E.
2) On detecting the attacks, each of them sends out an Accusation Packet (AP) to the CA against Malicious node M.
3) Upon receiving the first accusation packet (e.g., from node B), the CA will check for B's validation and then it will hold B in WL and M in the BL.
4) CA broadcast the revocation message to all nodes in the network.
5) Thus nodes update their local WL and BL to revoke node M's Certificate.

Results of Revoking malicious certificate:

1. Node B is in Warning List (WL).
2. Node M is in Black List (BL).

b) Certificate Recovery:

The CA broadcasts the information of the WL and BL to all the nodes present in the network. If there is a false accusation, then the nodes update their BL and WL from the CA. Since the CH does not detect any attacks from a particular attacker node present in the BL from the CA, the CH becomes aware of the occurrence of false accusation against its CM. Then, the CH sends a Recovery Packet (RP) to the CA in order to get back this member or node from the network. When the CA accepts the Recovery Packet and verifies the validity of the sender, the falsely accused node will be released from the BL and put them in the WL. Furthermore, the CA propagates this information to all the nodes present in the network [9]. The diagrammatic representation of certificate recovery is described in the following Fig. 5.

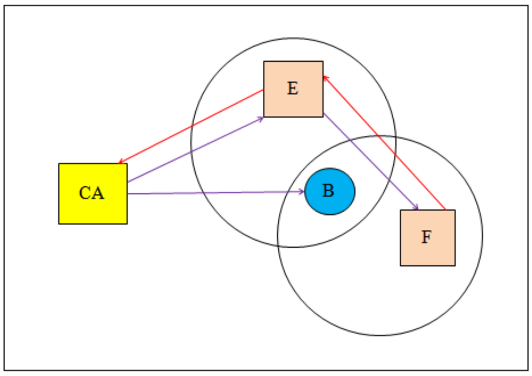

Fig. 5. Procedure of certificate recovery

Where,
Circle= Represents cluster,
B= Cluster Member,
E and F= Cluster Heads,
CA= Certificate Authority,
Red Line= Indicates Recovery Packet,
Purple Line= Indicates Broadcast Revocation Message.

Procedure for Certificate Recovery:

1) The CA broadcast the information of WL and BL to all the nodes in the network.
2) CH such as nodes E and F update their WL and BL, and determine that node B was framed.
3) E and F send a Recovery Packet (RP) to the CA to get the falsely accused node B.
4) Upon receiving the first recovery packet (e.g., from E), the CA removes node B from the BL and put nodes B and E in the WL, and then CA will inform to all other nodes in a network.
5) The nodes update their WL and BL to recover node B.

Results of certificate recovery:

1. Node B which is present in Black List (BL) will get removed from BL and is entered into a WL.
2. Nodes B and E are in Warning List (WL).

B. Advantages of Cluster-based Certificate Revocation mechanism:

1. Certificate revocation is very fast.
2. It solves the problem of false accusation.
3. It enhance the network security.

IV. SUMMARY

This paper provides an overview of a securing communication in network by using cluster-based certificate revocation method. Cluster-based certificate revocation has merits of both voting based and non-voting based mechanisms which revokes malicious certificate quickly. Problem of false accusation is also taken care by using Cluster-based certificate revocation mechanism.

V. FUTRE SCOPE OF WORK

The accuracy and efficiency of the said cluster-based certificate revocation method can be improved by recovering the normal node present in Warning List (WL) using Threshold-based mechanism and so, increase the availability of normal node in the cluster.

REFERENCES

[1] Ann Grace Attokaren, Mujeebudheen Khan A. I, “Survey on Certificate Revocation Scheme for Mobile Ad Hoc Networks”, International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014, 3410-3415.

[2] Dr.Shaveta Rani, Dr.Paramjeet Singh, Raman Preet, “Reviewing MANETs and Configurations of Certification Authority (CA) for node Authentication”, International Journal of Computer Science and Information Technologies, Vol.4 (6), 2013, 974-978.

[3] E.K. Neena, C. Balakrishnan, “Cluster Based Certificate Revocation of Attackers Nodes in MANET”, International Journal of Computer Science and Engineering, Volume 2, Jan.2014.

[4] Naresh Kumar G , Mounika T ,Lingam Sunitha ,Venkata Ramana E, Sridevi, “Study and Analysis on Certificate Revocation in MANETS”, International Journal of Computer Science and Information Technologies, Vol. 4 (4), 2013, 651654.

[5] S.Herman Jeeva, D. Saravanan, RM. Chandrasekaran,“ Enhancing Security in MANET Using CCRVC Scheme” International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 1, March 2014.

[6] T. R. Panke, “Clustering Based Certificate Revocation Scheme for Malicious Nodes in MANET”, International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013 1 ISSN 2250-3153.

[7] V. Kalaivani, M.Ashwin, “Efficient Certificate Revocation of Attacker nodes using CCRVC in Mobile Ad Hoc Networks”, International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 1, January 2014.

[8] Wei Liu, Hiroki Nishiyama, Nirwan Ansari, Nei Kato, “A Study on Certificate Revocation in Mobile Ad Hoc Networks”, IEEE ICC 2011.

[9] Wei Liu, Hiroki Nishiyama, Nirwan Ansari, Nei Kato, “Cluster-Based Certificate Revocation with vindication Capability for Mobile Ad-Hoc Networks”, IEEE transactions on parallel and distributed systems, vol.24, Feb., 2013.