ISSN:0975-9646

Survey on Certificate Revocation Scheme for Mobile Ad Hoc Networks

Ann Grace Attokaren, Mujeebudheen Khan A. I

Department of Information Technology
Rajagiri School of Engineering and Technology,
Rajagiri Valley P O, Cochin, Kerala, India

Abstract – Security is major issues in today's world. Everything in today's world should be done securely. Likewise wireless network are also more vulnerable to various types of security attacks. Mobile Ad hoc Networks (MANETs) is self-configuring wireless networks. MANET is an infrastructure less mobile network formed by a number of self-organized mobile nodes. So in order to guarantee secure network connection we opt for certificate revocation. The main challenge for certificate revocation is to revoke the certificates of malicious nodes promptly and accurately. This survey focuses to isolate attackers by the method of certificate revocation. And here we propose the Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme. Warned nodes need to take part in certificate revocation. So we need to recover them and improve the reliability. And we have threshold mechanism which helps in assessing and clearing the warned nodes whether it is legitimate or not and thus recovering them. This survey paper specifies about certificate revocation method which tells about how to revoke attackers certificate and recover falsely accused certificates.

Keywords – MANET, Certificate Revocation, Clustering, Threshold

I. INTRODUCTION

MANET is a collection of mobile nodes. Here they communicate with each other without wired network. In this we have wireless transmitters and receivers which communicate directly or indirectly via bidirectional wireless links. In MANET communication is not limited within a range, instead it allow communication via intermediate parties. This can be classified by two ways: single hop ,which allow communication within the same range and multi hop, which allow communication between the nodes which do not come under same radio range. MANET can be used in emergency circumstances because of its minimal configuration and quick deployment, like disaster relief, military operation etc. Due to the infrastructure less nature of MANET, MANET should be provided with all network functionalities.

Security is very important prime concern for such networks. Hence various security measures have to be taken. We should identify the attacks and should propose security methods and protect MANET [1]. In MANET we should provide secure communication between the nodes. These nodes can be attacked by malicious attackers and disrupt the security. MANET doesn't have a fixed infrastructure; here all nodes are free to move. Here nodes can join and leave the network freely since it is a open network. Thus MANETs are more exposed to security attacks.

Security in MANETs is combination of process, procedures, and systems that ensure confidentiality, authentication, integrity, availability, and nonrepudation. So it is needed to ensure protection for MANETs, certificate management is opted. This comprises of 3 components: prevention, detection, and revocation. There are various ways by which attacks can be detected. One such way is the routing protocols [2]. And also various certificate revocation [3][4].

Certification plays a vital role in securing network communication. These certificates are issued by certificate authority (CA). Certification is a data structure whose public key is bounded with the attribute but digital signature. This verifies and prevents tampering and forging in MANET. Certification revocation helps in enlisting and removing certificates of those nodes which cause attacks in neighborhood. Thus nodes which cause troubles should be removed or cutoff from all activities immediately.

For a CA it is difficult to revoke certificate from a node because it can also produce false accusation. So we should take this in consideration while making certification revocation mechanisms. In this we bring up with a cluster based mechanism and here the clustering information is never used for routing but it's used for managing certificates in the certification system.

By this method we will be able to detect the malicious nodes easily from each clusters rather than all nodes together. And here the certificates of the malicious nodes are revoked and they are removed from the network, thus stop its access to the network. And thus this method enhances network security.

This survey paper specifies about various certification techniques that exist as well as the cluster based scheme. Section 2 describes about the existing certificate revocation mechanism. Section 3 defines the proposed certificate revocation method. Section 4 includes comparison among the existing protocols.

II. EXISTING MECHANISMS

Intrusion Detection System is a software application that analyzes the network to find whether there are any malicious activities. If any malicious activities are there then it will report to the management station. It provides complete observation regarding the network and securing the network. Determination of intrusion is done through observing various information's.

Intrusion Detection System helps in finding or detecting various attacks in the network. It also gives a better performance and security of analysis.

MANET securities are provided among the different layers. In MANET we can come across various attacks [10],[11],[12] (fig 1) like

i) Internal: Here attacks are directly on the nodes on the network and links that interface them. Here broadcasting of wrong information happens [10].

ii) External: This attack causes network overhead and cause abnormal communication [10].

a) Active: in this the messages are attacked. There are external and internal active attacks. Among this internal attack is more severe. Due to this attack attacker get an unauthorized access to the network [10][12].

b) Passive: In this no alteration of data happens instead it collects data or listens to the traffic of the network. It's difficult to detect cause it doesn't have any impact on the network operations [10][12].

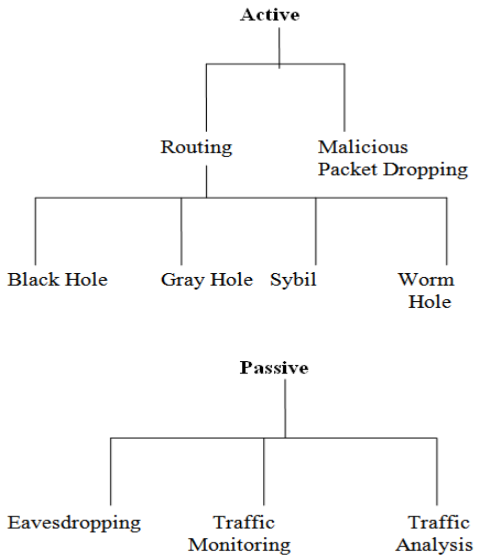

Fig 1: Active and Passive Attacks

Active**:**

(i) Black hole Attack: In this the malicious node claims that it has the shortest path to node whose packet it want attack. On getting a request from the node the malicious node say it has the shortest path nd thus the sender node will send the information to that node and thus malicious node will drop all the information it receives instead of forwarding them to destination to bring the attack.

(ii) Gray hole Attack: In this malicious node will give a fake message saying that it has a route to the destination node. And on receiving the message it will drop that message. This also known as routing misbehavior attack.

(iii) Sybil Attack: In this the fake nodes have several identities instead of single node. These extra identities are known as Sybil nodes. This can be stolen from the legitimate nodes. Due to this instead of seeing in many locations we can see these in several operations and launch attacks in the network.

(iv) Worm hole Attack: In this there exist tunnel between two malicious nodes and this tunnel is known as wormhole. When the information is received at one point it is tunneled to other point in the network. This attack severe threat for routing protocols of MANETs.

Passive:

(i) Eavesdropping: Nodes observe the network for any secret information and latter on this information is used by the attacker nodes.

(ii) Traffic Monitoring: Here identifying nodes which are responsible for launching attacks. Almost all wireless networks suffer from this attack.

(iii) Traffic Analysis: Attackers get an idea of location of nodes, their network topology and roles etc.

The security related to MANETs are difficult due to the vulnerability of wireless links, limited protection of nodes, changing topology which occur dynamically, and lack of infrastructure.

Clustering means grouping the nodes 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 communicate each other. Nodes within this cluster are called as cluster members (CM). Every cluster will have cluster members and a cluster head (CH).CH's are the backbone for communication in the network. These nodes will have certificate before joining the network, which they receive from CA.

CH communicates with other cluster members and vice versa. With this clustering method the nodes in MANET are provided with features like code separation (among clusters), channel access, routing, power control, virtual circuit support and bandwidth allocation. Nodes within the warning list and blacklist cannot become CH.

Proper selection of CH is important. CH communicates with its direct neighbors and they also communicate each other. There are variants in selection of CH[17].

First variant, says that CH is chosen depending on the nodes that are dependent on this CH is at distance of h hops.

Second variant, it depends on the size of the cluster and it should not be larger than τ.

Third variant is combination of first and second. And is known as Distance—and-Size-Constrained CH Selection.

Certain methods for choosing Cluster Head are:

a) Efficient Trust Model [18]: Choose CH's which are trustworthy and stable among the nodes, thus enhancing a secure communication. In this selection is based on TRUST VALUE. If TRUST VALUE is less than one then CH remains the same else we compare the values and determine the CH.

b) Cluster Head Election Mechanism [16]: Here at first CH are self Elected with an assumption there are no affected nodes. If this CH fails then the new CH is selected by all nodes using a secret Ballot. Here an election is done and nodes votes for the CH. The current CH counts the vote and the node elected with second majority is chosen as the Cluster Head. And the elected CH have to face certain challenges put forwarded by the current CH. If it fails then it is listed in blacklist and information is broadcasted and procedure repeated.

There have been many certificate revocation methods related to its security. Those are classified as voting-based and non-voting based mechanisms.

A. Voting-Based Mechanism

It is defined as a method in which malicious attacker's certificate is revoked through the votes from the valid neighboring nodes.

Voting based scheme proposed by Luo et al. is known as URSA [5] .It is to expel nodes of MANET which are malicious. Issuing and revocation of the certificates are done by the neighbors of newly joined nodes. In URSA, each node exchanges monitoring information with its neighbors which is obtained by one-hop monitoring. The certificate will be revoked when the vote exceeds a certain number and thus it is removed from the network and made isolated because it requires certificates to communicate URSA is not able to resolve its issue in addressing false accusations from the attacking nodes.

Another scheme was proposed by Arboit et al. [6] allows all nodes in the network to vote together. It differs from URSA in the way nodes vote with variable weights. It's based on weighted accusation. The weight of a node is calculated in terms of the reliability and trustworthiness of the node that is derived from its past behaviors. The weights of the accusations from nodes that are considered to be trustworthy are higher than those from less trustworthy nodes. The stronger its reliability, the greater the weight will be acquired. If the weighted sum of voting cross a predefined value, then the certificate can be revoked. And this help in increasing accuracy of certificate revocation. In this all nodes need to vote, so it leads a high communications overhead caused due to voting information exchange and that also leads to high revocation time.

B. Non-Voting Based Mechanism

In the non-voting-based mechanism, a node with proper certificate can decide whether a node is malicious attacker or not..

The "suicide for the common good " strategy proposed by Clulow et al. [7] is a method by which certificate revocation can be quickly completed by only one accusation. Thus the accusing node is sacrificing itself because its certificate is also revoked. To remove the attacker in order to make the network secure. This mechanism reduces both time required to evict a node and communications over head of the certificate revocation procedure due to its suicidal strategy. This does not take into account of differentiating falsely accused nodes from genuine malicious attackers. As a consequence, the accuracy is degraded.

Park et al. [8] proposed a cluster-based certificate revocation scheme. Nodes are organized as clusters. Here in this method we have a certificate authority to manage control messages, holding the accuser and accused node in the warning list (WL) and blacklist (BL), respectively. By any single neighboring node the the certificate of the malicious attacker node can be revoked. It also deals with the issue of false accusation that enables the falsely accused node to be removed from the blacklist by its cluster head (CH). It takes a short time to complete the process of handling the certificate revocation.

III. Cluster Based Scheme

In this scheme [19] cluster head plays an important role in identifying the falsely accused node and recovering their certificates and thus solving the false accusation issue. Here revoking happens as soon as receiving only one accusation from neighboring node. The scheme maintains two lists: Warning List (WL) and Black List (BL).

Here we assume that all nodes receive their certificates before joining the network. Once malicious attacker is identified then we focus on certificate revocation rather than attack detection.

A.Cluster Communication

The CH node sends a CH hello packet all of its neighboring nodes and those in CH's transmission range will accept it. And replies with CM hello packet. After this they will join the cluster. And we can see single CM belong to two different clusters for providing robustness in topology. So when it moves out of one range it can search for another CHP and join new cluster.

B.Function of Certification Authority

CA is deployed to enable each node to preload the certificate. And also it is in charge of updating WL and BL.

C.Reliability-Based Node Classification

Classified as 3 types:

1. Legitimate node: this is deemed to secure communications with other nodes. It is able to correctly detect attacks from malicious attacker nodes and accuse them positively, and to revoke their certificates in order to guarantee network security.
2. Malicious node: it does not execute protocols to identify misbehavior, vote honestly, and revoke malicious attackers. In particular, it is able to falsely accuse a legitimate node to revoke its certificate successfully.

3. Attacker node: it is defined as a special malicious node which can launch attacks on its neighbors to disrupt secure communications in the network.

Based on Reliability classified as:

1. Normal node: it does not launch attack.
2. Warned node: Nodes listed in the WL.
3. Revoked node: malicious attackers deprived of their certificates and evicted from the network.

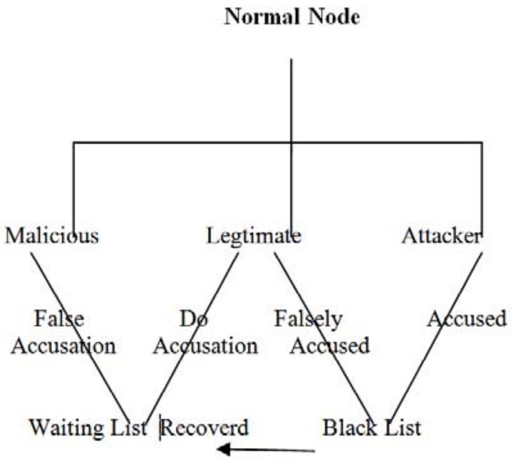

Fig.2. The classification of nodes in our scheme.

D.Certificate Revocation

1. How to Revoke Malicious Certificates

For revoking a malicious attacker's certificate we should take in consideration 3 stages: accusing, verification, and notifying.

Step 1 . Malicious node launches attack on the neighboring nodes. i.e. M attacks B, C,D, and E .

Step 2.On detecting the attacks each of them sends out an accusation packet to the CA against Malicious node say M.

Step 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 and M in the WL and BL.

Step 4. Broadcast the revocation message to all nodes in the network.

Step 5. Thus nodes update their local WL and BL to revoke M's certificate.

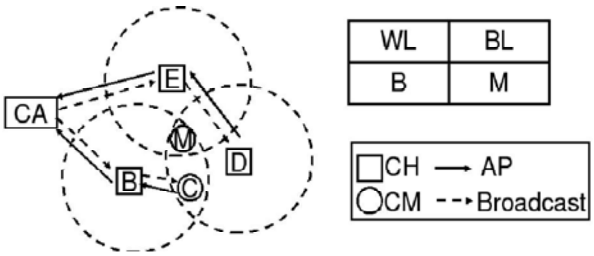

Fig. 3. Revoking a node's certificate.

2.Coping with False Accusation

CH is enabled to detect the false accusation and restore the node.

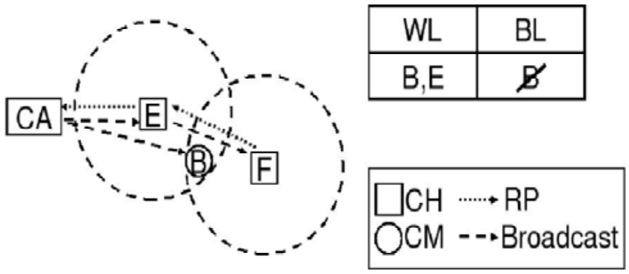

Fig. 4. Dealing with false accusation.

Step 1. The CA broadcast the information of the WL and BL to all nodes in the network.

Step 2. CH E and F update their WL and BL, and determine that node B was framed.

Step 3. E and F send a recovery packet to the CA to revive the falsely accused node B.

Step 4**.** Upon receiving the first recovery packet (e.g., from E), the CA removes B from the BL and holds B and E in the WL, and will inform all other nodes.

Step 5. The nodes update their WL and BL to recover node B.

IV.WL MANAGEMENT

A.Normal Nodes Depreciation

In order to prevent further damage, accusation packets from the nodes in WL is not accepted by CA. thus if malicious nodes increase then nodes in waiting list (WL) also increases which turn will make difficult to accuse the attacker nodes which affect the reliability.

If there is a normal node around attacker it will be easy to detect and revoke the attacker. Therefore, the probability that there are exactly k normal nodes (k being a non-negative integer, k = 0, 1, 2 ...) in a specific area in MANETs is equal to

$$Pr\ (m) = \frac{\lambda^{m}\ e^{-\lambda}}{m!}$$

where ρ is the node density per unit area, which is dependent on the location in space; θ is the proportion of normal nodes in the network; S represents the transmission area of a malicious node.

When m = 0, i.e., no normal nodes within an attacker's transmission range, the probability is

$$Pr\ (m=0) = e^{-\theta\rho S}$$

This probability should be reduced to guarantee a certain number of normal nodes in the network to revoke the malicious nodes. The good nodes should be removed from the WL to increase the normal nodes to enhance robustness and reliability against the decreasing normal nodes.

B.Node Releasing

In order to release nodes from WL we opt for a threshold mechanism which increase the number of normal nodes in the network. Before releasing we should be able to distinguish between legitimate and misbehaving nodes. This is done because legitimate nodes correctly accuses the attacker node and malicious node should be enlisted in the WL to avoid false accusations.

For that we have a node releasing mechanism :

i. Counter for CA to record accusation against each accused nodes
ii. CA continues to receive accusations against the accused node following a voting period of time, Tv.
iii. Compare with a threshold, K
iv. If no. of accusations=K, a real attack occurs
v. Otherwise, detained in the WL

For this the threshold we propose should be less than the misbehaving nodes in the network. To determine the number of nodes N, we have

$$N = (\pi r^2 + 2rvT_v)\rho,$$

where r denotes the transmission range of nodes, v is the velocity, and ρ is the density of nodes in the network. Based on the obtained number of neighboring nodes N, we can confirm the value of threshold K.

V.COMPARISON BETWEEN CERTIFICATE REVOCATION MECHANISMS

Voting-Based is the high accuracy in confirming the given accused node as a real malicious attacker or not, whereas non-voting based can revoke a suspicious misbehaved node by only one accusation from any single node with valid certification in the network. The accuracy of determining an accused node as a malicious attacker and the reliability of certificate revocation will be degraded as compared with the voting-based method.

Voting-based achieves higher accuracy in judging a suspicious node, but takes a longer time, whereas the non-voting based can significantly expedite the revocation process. And our proposed method a Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme inherits the advantages of both voting-based and non-voting based, scheme can revoke an accused node based on a single node's accusation, and reduce the revocation time as compared to the voting-based mechanism, thus lowering overhead.. In addition, we have adopted the cluster-based model to restore falsely accused nodes by the CH, thus improving the accuracy as compared to the non-voting based mechanism and improving the reliability Our scheme can quickly revoke the malicious device's certificate, stop the device access to the network, and enhance network security.

VI.CONCLUSION

MANETs doesn't have a fixed infrastructure and hence they are vulnerable to attacks by intruders**.** Various mechanisms are there to ensure security in the networks. Security attacks that MANET are facing today are also mentioned in this survey. It gives an idea of all those security attack and also the intrusion detection system. Along with this various voting and non-voting based schems. Along with this we propose a certificate revocation method for secure communications in MANETs.

The cluster-based certificate revocation with vindication capability scheme is combined with the merits of both voting-based and non-voting-based mechanisms. With this scheme we were able to revoke the certificates of malicious node and isolating them from the network. And also it deals with problem of false accusation in the network and retrieving the normal nodes and increasing the accuracy of the network . we this we can reduce the revocation time as well. For improving the normal nodes availability and thus improving the efficiency of the network. We have certain methods to restore the legitimate nodes. CCRVC scheme is more effective and efficient in revoking certificates of malicious attacker nodes, reducing revocation time, and improving the accuracy and reliability of certificate revocation.

REFERENCES

[1] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Comm., vol. 11, no. 1, pp. 38-47, Feb. 2004.

[2] B. Kannhavong, H. Nakayama, A. Jamalipour, Y. Nemoto, and N. Kato, "A Survey of Routing Attacks in MANET," IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 85-91, Oct. 2007.

[3] G. Arboit, C. Crepeau, C.R. Davis, and M. Maheswaran, "A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks," Ad Hoc Network, vol. 6, no. 1, pp. 17-31, Jan. 2008.

[4] K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks," Proc. IEEE 71st Vehicular Technology Conf. (VTC '10), May 16-19, 2010.

[5] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks," IEEE/ACM Trans. Networking, vol. 12, no. 6, pp. 1049-1063, Oct. 2004.

[6] G. Arboit, C. Crepeau, C.R. Davis, and M. Maheswaran, "A Localized Certificate evocation Scheme for Mobile Ad Hoc Networks," Ad Hoc Network, vol. 6, no. 1, pp. 17-31, Jan. 2008.

[7] J. Clulow and T. Moore, "Suicide for the Common Good: A New Strategy for Credential Revocation in Self-organizing Systems," ACMSIGOPS Operating Systems Rev., vol. 40, no. 3, pp. 18-21, July 2006.

[8] K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks," Proc. IEEE 71st Vehicular Technology Conf. (VTC '10), May 16-19, 2010.

[9] W. Liu, H. Nishiyama, N. Ansari, and N. Kato, "A Study on Certificate Revocation in Mobile Ad Hoc Network," Proc. IEEE Int'l Conf. Comm. (ICC), June 2011.

[10] Gagandeep, Aashima, Pawan Kumar " Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review".

[11] Priyanka Goyal, Vinti Parmar, Rahul Rishi3 " MANET: Vulnerabilities, Challenges, Attacks, Application".

[12] Adnan Nadeem, Member, IEEE, and Michael P. Howarth "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks"

[13] Priyanka Goyal, Sahil Batra, Ajit Singh, " A Literature Review of Security Attack in Mobile Ad-hoc Networks".

[14] Amara korba, Abdelaziz, Mehdi Nafaa, Ghanemi Salim: "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks".

[15] Kiran Dhangar, Prof. Deepak Kulhare, Arif Khan: Intrusion Detection System (A Layered Based Approach for Finding Attacks)

[16] Garth V. Crosby, Niki Pissinou, James Gadze **"**A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks".

[17] Dang Nguyen, Pascale Minet, Thomas Kunz and Louise Lamont: "On the Selection of Cluster Heads in MANETs".

[18]]Raihana Ferdous, Vallipuram Muthukkumarasamy, Elankayer Sithirasenan: "Trust-based Cluster head Selection Algorithm for Mobile Ad hoc Networks".

[19] Wei Liu, Student Member, IEEE, Hiroki Nishiyama, Member, IEEE, Nirwan Ansari, Fellow, IEEE, Jie Yang, and Nei Kato, Senior Member, IEEE "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks".