Securing Node Communication in MANET using Certificate Revocation

D. Vikram Raj Reddy[1], M. Gangappa[2]

[1]*M.Tech Student (SE), VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India*

[2]*Associate Professor (CSE), VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India*

Abstract— **Mobile Ad hoc Network is a type of network which frequently changes locations and configures itself in movement. MANETS are mobile in nature and use wireless communication, so the main disadvantage for MANETS is providing Security to the nodes. In order to secure the communication between nodes we use one important action called Certificate Revocation. The previous work is done using voting and Non-voting based communication. The proposed system uses Cluster based certificate revocation where it classifies the topology into clusters and finds the malicious nodes. It finds the false accused nodes with the help of Cluster Head (CH). The system also maintains two important lists 1) Warning List 2) Black Lists. This method overcomes the existing system by enhancing the security and increasing the performance of detecting the malicious nodes.**

Keywords— **Mobile Ad-hoc Network, Certificate Revocation, Cluster Head (CH)**

I. Introduction

MANETs is a collection of wireless mobile nodes such as cell phones, Laptops, PDAs, etc,. These nodes can be dynamically set up anywhere without using any pre-existing infrastructure. The nodes in MANETs communicate through same Radio range and use relay nodes to communicate with nodes of other range. There is no fixed infrastructure and nodes are fully distributed thought the network. Fig.1 shows a MANET with five nodes.

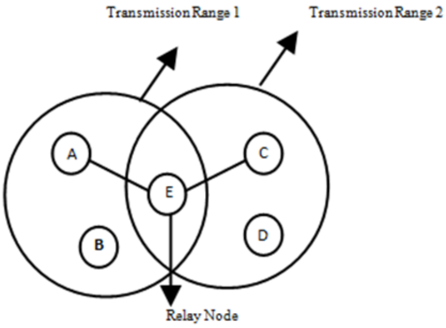


Fig.1. Example of MANET

Characteristics of MANETs

a) Nodes are Mobile All nodes within a MANET are free to move inside a reachable bandwidth and they are having routing capability to deliver packets to other nodes.

b) Rapidly Changing Network Topology Network topology is highly dependent on the relative locations and connections between nodes in the network. Thus the resulting topology will be dynamic in nature.

c) Easily Deployable The network deployment is very easy as the network topology is rapidly changing.

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.

To guarantee secure network services is a major challenge associated with any MANET [7]. 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).

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.

Certificate Revocation is a phase associated with Certificate Management which is a widely accepted method to provide trustworthy public key infrastructure [9] for both application security and network service security. In the process of certificate management the three phases needed are: prevent, detect and revocate. Therefore issue of false accusation must be considered during designing of certificate revocation mechanism.

The reminder of this paper is organized as follows. In Section II, brief overview on voting and Non-voting based techniques is discussed. Section III, describes the structure of the node clustering. The entire concept is summarized in section IV. We give the implementation results and discussions in Section V. Finally, we conclude this paper.

II. Related Work

In this section, we first introduce voting and non-voting based techniques. Then the problems in these techniques are discussed.

A. Voting Based technique

In voting-based mechanism, malicious attacker’s certificate is revoked through the votes from the valid neighbouring nodes [5]. 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 neighbouring 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. Amplify-and-Forward
- Decode-and-Forward.

B. *Non-voting-based Technique*

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. [10]. 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.

In these techniques 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.

Also existing techniques 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. NODE CLUSTERING

In this section we describe the process of node clustering. 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 communicated 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.

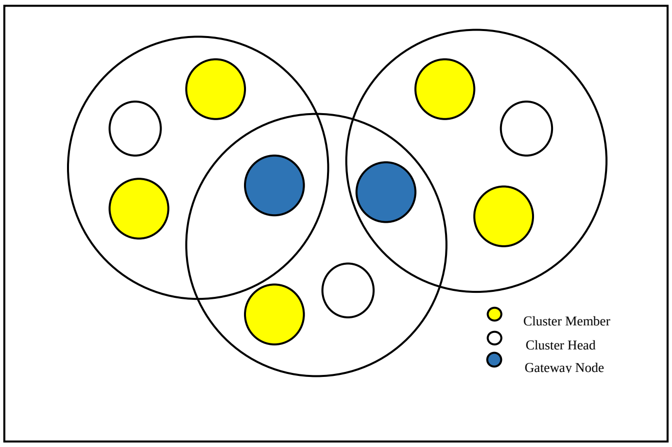
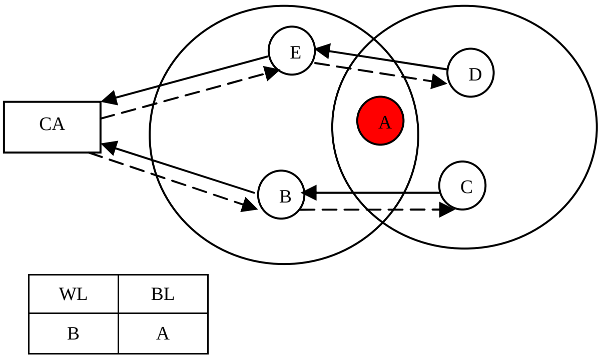


Fig.2. Cluster Construction

IV. CLUSTER BASED CERTIFICATE REVOCATION

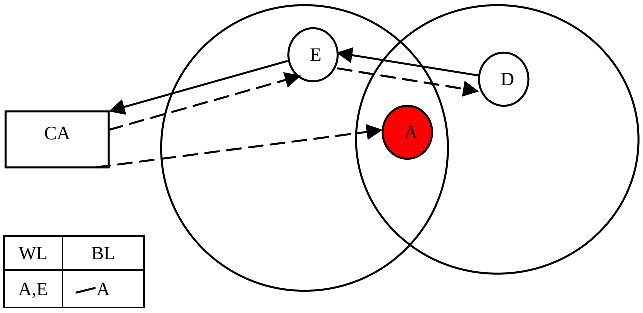
In this section we give the complete process of cluster-based certificate revocation scheme, which was originally proposed in [4]. Although a centralized CA manages certificates for all the nodes in the network, cluster construction is decentralized and performed autonomously. Nodes cooperate to form 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. Each CM belongs to two different clusters in order to provide robustness against changes in topology due to mobility. It should be noted that because the clusters overlap, a node within the communication range of a CH is not necessary part of its cluster. 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. 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.

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. 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. The reliability of each node is determined by the CA as follows. The CA maintains both a Black List (BL) and a Warning List. When the CA receives an ADP from an accuser, the accused node is regarded as an attacker and is immediately registered in the BL. The BL includes nodes which are classified as attackers and have had their certificates revoked. The accuser of the attacker is then listed in the WL because the accuser might actually be making a false accusation. However, falsely accused nodes will be restored quickly by their CHs. We consider false accusation and false recovery as an act of misbehaviour, and define nodes that do such act as misbehaving nodes.



WL	BL
B	A

Fig.3. Process of False accusation



WL	BL
A,E	—A

Fig.4. Process of certificate revocation

Fig.3 and Fig.4 shows examples of certificate revocation and recovery procedures. As shown in Fig.3, node A is a malicious node and launches attacks on its neighbours, i.e. nodes B, C, D and E. Its neighbours detect the attacks and send ADPs to the CA to accuse node A. Upon receiving the first ADP from node B, the CA puts it into the WL as an accuser and node A into the BL as an attacker. It then broadcasts the information contained in the WL and BL to the entire network. Fig.2 shows the procedure of certificate recovery. When node E and D, which are the CHs of node A, are informed that node A is listed in the BL, if they have never detected any attacks coming from A, the accusation as a false one. They will then send a CRP to the CA to recover node A's certificate. Upon receiving the first arrival CRP from node E, the CA removes the falsely accused node A from the BL, and enlists it into the WL along with node E. After the broadcast of the updated WL and BL, the certificate of node A will be recovered successful.

V. IMPLEMENTATION OF CLUSTER BASED CERTIFICATION REVOCATION

In this section we give the implementation of the system. For developing we have used Java programming language to implement the proposed scheme. In the remainder of this section, we give the implementation of the certificate revocation scheme.

We have developed a graph which has several nodes connected. This graph is developed based on DSDV technique. The number of nodes for the network can be given by the user. The figure shows the nodes in the network.

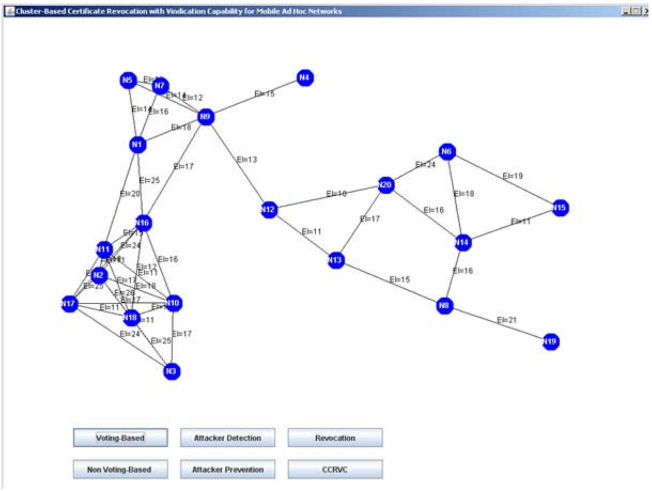


Fig.5. Nodes in the network.

Every node will have the details of the neighbouring nodes, the negative voting for the node and the certificate issued by the certificate authority. Here in the implementation the certificate is generated by using X509certificate which can be imported in java.

The malicious node detection will be done based on the negative voting for the nodes. Here in this system we have given maximum malicious nodes as three nodes. The threshold value will be calculated based on the number of nodes participating in the network to the maximum negative voting number for the nodes.

After detecting malicious node detection form is generated this gives the malicious nodes and the accused nodes in the network. The figure shows the detection form.

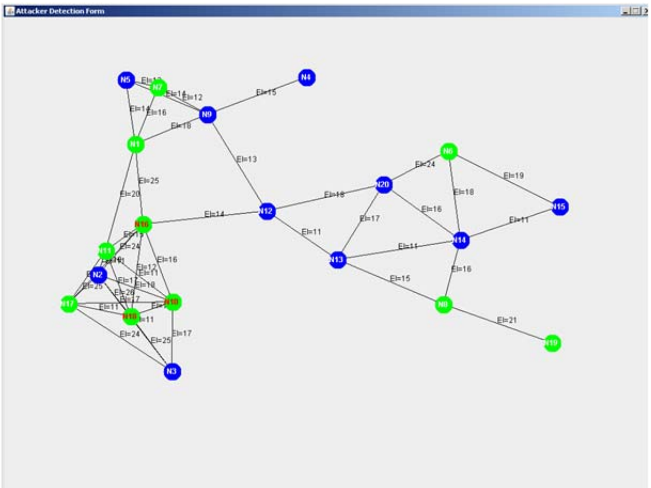


Fig.6. Malicious node detection form

The certificate authority will revoke the malicious nodes certificates and terminate the nodes from the network. If there is false accusation the cluster head of the accused node will inform the Certificate Authority and it revokes removes the accused node from the black list and puts it in the warning list. This is done before generating the detection form. Finally the Certificate authority will remove the nodes from the network and generates a new graph without the malicious nodes.

The performance of the proposed scheme increases based on the previous nodes by increasing the malicious nodes and decreasing the accusing nodes.

VI. CONCLUSION

In this paper, we have introduced voting and non-voting techniques and the security issues in those techniques and proposed a cluster based certificate revocation where it detects the malicious nodes. To improve the security of the MANETs we have implemented false accusing nodes. This technique also increases the performance of the network compared with voting and non-voting rechniques.

REFERENCES

[1] Nausham Shasi, "Efficient Certificate Revocation with Vindication Capability for MANETS" , IJCSIT Vol 5(3) ,2014.

[2] Wei Liu, Student Member , IEEE "Cluster based Certificate Revocation with Vindication Capability for MANETS", IEEE Transactions on Parellel and Distributed System.

[3] Vol 24 No. 2 February 2013

[4] 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

[5] H. Chan, V. Gligor, A. Perrig, and G. Muralidharan, "On the Distribution and Revocation of Cryptographic Keys in Sensor Networks," IEEE Trans. Dependable and Secure Computing, vol. 2, no. 3, pp. 233-247, July 2005.

[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 22503153

[7] 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.

[8] A.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006

[10] A.M. Hegland, E. Winjum, C. Rong, and P. Spilling, "A Survey of Key Management in Ad Hoc Networks," IEEE Comm. Surveys and Tutorials, vol. 8, no. 3, pp. 48-66, Third Quarter 2006

[11] 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