Cluster Based Certificate Revocation in MANETs with Distributed Certification Authority (CA)

Sarika S. Jadhav¹ * and Prof. Vinod S. Wadne²

¹Department of Computer Science, JSPM’s ICOER, Wagholi, Pune, India.
²Department of Computer Science, JSPM’s ICOER, Wagholi, Pune, India

ABSTRACT

Now a Days mobile Ad-hoc networks (MANETs) gaining more popularity because of the mobile in nature and formation of dynamic topology. One of the issue in the mobile Ad hoc network is security. To provide security in mobile Ad hoc network we are providing valid certificate to each node and by using that certificates nodes are securely communicate with each other. All information regarding to maintaining the warned list (WL), black list (BL) providing the valid certificate is done by certification authority (CA) but there is a issue of CA as it works centralized. If in case CA goes down or moves out of the range then it is difficult to handle whole network so our proposed work is to make the CA as a decentralized. When we will make CA as decentralized it is possible to recover the whole information regarding to the downed CA. Also it is possible to provide more accuracy by using dynamic threshold based mechanism for removing the normal node present in the WL and allow that node to take part in revocation process and mark it as normal node.

Keyword: Certification Authority (CA), Dynamic threshold, Mobile Ad-hoc Networks (MANETs), valid certificate, Warned list, Black list, Decentralized.

[1]. INTRODUCTION

In recent years Mobile Ad hoc network gaining more attention due to their mobility in nature and in MANETs topologies are dynamically formed. Due to their mobility in nature it is not possible to providing the physical security. To provide the security in mobile ad hoc network we are using valid certificate for secure communication in the network. Certificate is nothing but it’s a signed message by issuer which containing the identity of holder (node), public key, unique certificate serial no., validity or expiration date of that certificate. The certificates distribution [1], [2] is done by the CA present in network. CA having the authority to providing the valid certificate to newly joining node, maintaining the WL and BL, keeping the identity of each node along with expiration date of that certificate. By using that certificates nodes are able to securely communicate with each other. In network if any node doing some malicious activity then we are revoking the certificate of that node, in other word we are removing that node from all communication links.
When new node want to join the network first it take the valid certificate from the CA, after taking the certificate he join the cluster or become CM or CH of the cluster depends on the present situation in the network. In cluster some nodes are doing malicious activity, so our first step is find the malicious nodes present in the cluster and after that revoking the certificate of the malicious node. In this system there is the possibility of false accusation. False accusation means neighboring node providing the wrong information to the CA and CA revoking the certificate of that node. In false accusation there is possibility of revocation of normal node certificate. So our responsibility is to avoid false accusation. The first step find the falsely accused normal node in black list and removing that node from BL to WL. Second step is removing normal node from WL providing all authorities to that node.

In our proposed scheme we will make the replicas of CA. In any case anyone CA goes down then we will retrieve the information from the other CA. By using this we will provide more reliability in the network.

[2]. STATE OF THE ART

Mobile Ad hoc network gets much attention because in mobile Ad hoc network topologies are dynamically formed, it is infrastructure less and mobile in nature. Because of the mobility in nature it is difficult to provide security in the mobile Ad hoc networks. Provide security in mobile Ad-hoc network we forming the cluster and providing the valid certificate to each node present in that network. By using that certificate nodes are securely communicating with each other. Suppose any node doing some malicious activity then in that case certificate of that node is revoked. For revoking the certificate of misbehaving node there are mainly two techniques

2.1 Voting based Technique
2.2 Non-voting Based Technique

In voting based technique we are considering the votes from all nodes present in the cluster and depends on that votes we are revoking the certificate of that node. In 2004 URSA[3] proposed the voting based system to revoking the certificate of malicious node. In this System this system the concept of CA is not used. In this certificates are provided by the neighboring nodes present in the network. Suppose any node doing the malicious activity in the network then election is taken out. Each node present in the network votes with variable weight for the malicious node. Variable weight is nothing but trustworthiness of that node or past behavior of that node. If the numbers of negative votes are exceed the threshold value then certificate of that node is revoked. But there is no technique for finding out the false accusation and also CA does not exist.

Advantages of voting based System - Accuracy is high because opinion of each node is taken that’s why accuracy is greater.

Disadvantage of Voting based System-It require large time for revoking the certificate of the malicious node because it consider the opinion about the malicious node from each node present in the network.

2.2 Non-voting based technique

Sarika S. Jadhav, and Prof. Vinod S. Wadne
J.clulow and T.moore [4] proposed one system as a “suicide for common good”. In this system consideration of only one node is taken. Suppose one node present in the network found that neighboring node doing some malicious activity, then that node tells to CA this is a malicious node then certificate of that malicious node revoked and CA listed the accuser into the WL and accused node into the BL. So accuser sacrifices itself for removing the malicious node.

Park et al. [5] proposed a cluster based certificate revocation system. In this CA is responsible for managing WL, BL and certificate of each node. In this certificate of malicious node is revoked by only one neighboring node. Considerations of other nodes are not taken.

Advantage-Less Time is required for revoking the certificate of the malicious node.
Disadvantage-Accuracy is less as compare to the voting based mechanism because consideration of only one neighboring node is taken.

[3]. IMPLEMENTATION DETAILS

In this part we will see how the clusters are form, certificate revocation [4], [5], [7], [8] process, process of removing the normal node from BL to WL and realizing the normal node from WL by using the dynamic threshold based value.

3.1 Certification Authority

It is a trusted third party having authority of providing valid certificate to node present in the cluster as well as newly joining node. It is also having the responsibility of maintaining the updated warned list and black list. Warned list

Containing the accuser node and black list containing the accused node present in the network. Another responsibility of CA is to broadcast updated warned list and black list to node present in the entire network.

3.2 Classification of node

In our scheme we are classifying the node into three types

1. Normal node-Those nodes that are secure and communicate with other node securely. It also having the authority to revoking the certificate of accused node

2. Malicious node- Those nodes that are insecure for communication. They are performing the malicious activity in the network and does not having any authority to revoking the certificate of node present in the network.

3. Warned node-warned node means those nodes that accusing the other nodes are consider as warned node. Also it does not having any authority to revoking the certificate of other malicious nodes. Only it is having the permission to communicate with other nodes along with some restriction.

3.3 Cluster formation
We are using cluster based [5] mechanism for formation of cluster in the mobile Ad hoc network. Each cluster having the cluster head (CH), cluster members and the group of cluster having one CA. If any node come in the particular range then firstly it take valid certificate from the CA. CA having the responsibility of providing the valid certificate to newly joining node in the cluster, managing the warned list, black list, certificate details of each node present in the cluster. After taking the certificate from CA it consider itself as a cluster head and send the cluster head hello packet (CHP) to tell its neighboring nodes as he is the new cluster head. If that newly joining node getting the reply from other node then he is become the CH with probability R. Otherwise he will become the CM. Those node that are present in particular transmission range they are waiting for CHP packet from the CH. After getting the CHP packet from CH they send cluster member hello packet (CMP) to the CH and the connection is established between CH and CM. CH and CA keep in touch with each other by sending the CHP and CMP packet to each other in time period T. If any CM moves from out of the transmission range then CM is waiting for another CHP. When CM getting the another CHP then again CM send CMH to that CH and connection is established between CH and CM.

Steps for implementing the cluster

Step 1- If new node then first take valid certificate from CA.
Step 2- New node sends the CHP packet to the neighboring nodes
Step 3-a) If that node doesn’t getting any reply within time period T then it becomes CH.
b) If any node sending the CMP packet to new node then new node become the CH otherwise he become the cluster member.
Step 4- If CM moves from out of the range then he wait for CHP. In time period T If he getting the CHP then he is the cluster member otherwise he declare itself as a cluster head.

3.4 Certificate Revocation

In the cluster if any node wants to communicate with other node then by using the valid certificate they securely communicate with each other. Suppose in the network some nodes are doing the malicious activity and it is found by the neighboring node then neighboring node first check the local black list. If that node present in that black list then the certificate of the malicious node is directly revoked by that neighboring node by using non-voting based Scheme [4] otherwise it send the accusation packet (AP) to the CA. Accusation packet containing all the information of accuser, accused node and destination. After sending the information CA check the certificate of accuser. If it is valid then it put accuser into WL and accused node in BL and the list is updated. Finally updated information is send to the all nodes that are present in the network.

Example- How the nodes are listed in black list and warned list. In below Fig. 3.1.one cluster is there along with one CA and four cluster heads are A, B, C and D. These are the steps for revoking the certificate of the malicious node-
Step 1- Neighboring nodes C, D, R and B detect attack from node S.
Step 2- Each of them sends the accusation packet against S.
Step 3- According to first received packet form the node the CA holds Accuser (i.e. C) in WL and accused node (i.e. S) in the WL.

Sarika S. Jadhav, and Prof. Vinod S. Wadne
Step 4 - CA sends the revocation message to all nodes present in the network.
Step 5 - CA updates the WL and BL and sends them in the network.

In this way, we are revoking the certificate of a malicious node present in the network. However, one of the drawbacks in the above scheme is that if the accuser itself is a malicious node, there is a possibility of false accusation. Means, if the accuser itself is a malicious node, and the certificate of a normal node present in the cluster is revoked, then the normal node is listed in WL and the malicious node is listed in BL. This false accusation decreases the accuracy of certificate revocation. Therefore, there is a need to cope with false accusations.

3.5 Coping with False Accusation

In this scheme, we enable CH to detect false accusation present in the cluster. For finding the falsely accused node present in the cluster, first, CH monitors all attacks done by the CMs. After monitoring, CH sends a recovery packet to CA to recover the certificate of the falsely accused node. CA verifies the recovery packet received from CH and removes the falsely accused node from BL to WL. However, here is another problem: the number of nodes in WL increases, and the accuracy of revoking the certificate of a malicious node in the network decreases because no normal nodes are present.

Normal nodes in the network are less. So to overcome the above problem, we propose a dynamic threshold-based method. Fig. 3.2 is an example for managing false accusation present in the cluster.
These are the steps for managing the false accusation:

Step 1 - CA sends the updated copies of BL and WL to nodes present in the network.

Step 2 - Cluster head B and C update the BL and WL. He found the S is not malicious node then he sends the accusation packet to the CA, for recovering the node in BL.

Step 3 - After receiving the accusation packet it remove the node from BL to WL.

Step 5 - CA update the BL and WL send it to each node present in the Network.

3.6 Dynamic threshold based mechanism for realizing normal node in WL

To overcome the above problem we will take the majority based voting in normal nodes present in the cluster for a time period T. In this scheme we design one counter to keeping the track of no of accusations against the accused node present in the BL. If no of accusation is exceed the threshold value then we conclude that this is accused node and keep that node in black list and removing the accusing node from the WL and mark the status of that node as a normal node. Above procedure is taken when no of nodes present in the WL are greater than the Normal node present in the network for time period of T.

In previous static threshold value [6] is used, because of the static threshold value accuracy of realizing normal node from WL is less. That’s why we are proposing the concept of Dynamic threshold value. First we see how to calculate the no node present in the cluster.

No. of node present in the transmission range = n [6]

\[ n = (\pi r^2 + 2rvT) p \]  \hspace{1cm} (1)

Where,

T= Time period
r=Transmission range
v=Velocity of the node
p=Density Of the node

Then find the no of normal node (N) present in the cluster for that

\[ N = n - (\text{No. Of nodes in WL} + \text{No. nodes in BL}) \] \hspace{1cm} (2)

Sarika S. Jadhav, and Prof. Vinod S. Wadne
Dynamic threshold value \( (K) \) is calculated by using the following formulas given below

\[
K = M \times \frac{N}{10}
\]  

(3)

Where, 
- \( M \) - Mean of number of normal nodes present in the cluster
- \( N \) - Number of normal node present in the network

Value of \( M \) is calculated by, \( M = \frac{N}{2} \).

This dynamic threshold value is calculated when the number of nodes are present in the WL are greater than the number of normal node in the network then in that case we will take the decision for removing the node from WL to normal node. By this mechanism it is possible to remove the normal node from WL and allow that normal node to take a part in revocation process.

3.7 Distributed CA based Approach

In present system there is the possibility of CA goes down or change its position and join to the other cluster then in that case there is need to efficiently managing the WL, BL and certificate of the node. For this purpose we proposed the distributed type of CA. In this we will maintain the multiple replicas of CA and also managing the neighboring CA identity and location of CA. When any CA goes down or changing its position then in that case CH and CM having the list of neighboring CA, by using this list CH and CM retrieve the information from the neighboring CA.

Fig 3.3 distributed CA based approach

[5]. CONCLUSION
In this we are also taking the advantages of non-voting based and voting based technique for revoking the certificate of malicious node. Also we are dealing with false accusation means we recover the node which falsely accused by the neighboring node.

In this paper we are providing a secure communication in the network by using the certificate. If any nodes doing some malicious activity then in that case we are using the cluster based certificate revocation technique for the secure communication.

We are proposing one dynamic threshold based method. In this method we are calculating the Dynamic threshold value to recover the normal node present in WL and increases the availability of normal node in the cluster, by using this method accuracy is increases. Also we are using the distributed CA based approach for maintaining the data on CA. Because in any case CA goes down then it is difficult to handle the network. To avoid this problem we will use the distributed CA based approach for maintaining the data in CA.

REFERENCES


Author[s] brief Introduction

Sarika S. Jadhav, and Prof. Vinod S. Wadne
Sarika S. Jadhav: Pune, 26/09/1990. She has received the graduation degree in Computer Science and Engineering from Orchid College of Engineering and Technology, Solapur, Maharashtra, India (Solapur University) in 2012. She is pursuing post-graduation degree in Computer Engineering at JSPM’s Imperial College of Engineering & Research, Wagholi, Pune (Pune University.)

Prof Vinod S. Wadne: Pune, 22/05/1981. He has received the post-graduation degree in Computer Science & Engineering from KBN College of Engineering, Gulbarga, Karnataka, India (Visveswarya Technological University, Belgaum) in 2011 & Graduation degree in Computer Science & Engineering from TPCT’s College of Engineering Osmanabad, Maharashtra, India(Dr. BAM University, Aurangabad) in 2003. He has 10 years of experience in teaching field, presently working as Assistant Professor and Head of Computer Engineering Department at JSPM’s Imperial College of Engineering & Research, Wagholi, Pune. He has published 4 papers in national & international journals. Prof. Vinod S. Wadne is having a Life membership of ISTE.