International Journal For Technological Research In Engineering
Volume 1, Issue 10, June-2014 *ISSN (Online): 2347 - 4718*

RETRACTION OF CERTIFICATE WITH CLAIMING ABILITY FOR MANETS

Rajesh. K.M[1], Dr. Suresh. M.B[2] [1]M.Tech-Student, dept. of Computer Network Engineering
[2]Professor and Head, dept. of Information Science
East West Institute of Technology, Bangalore, India.

Abstract: Mobile ad hoc networks (MANET) are the instantly created autonomous wireless networks, in which nodes in the network could organize themselves rapidly, in order to communicate with each other. They do not require any fixed infrastructure unlike their conventional counterparts. In the recent past, MANETs has gained much of its attraction due to its unique features such as nomadic nature, dynamicity and also due to its ease in deployment. However, the wireless and dynamic topological natures render them various types of security threats than their wired counterparts. Hence, the major challenge is to guarantee the secure network communication services. In order to depreciate this challenge, certificate retraction is a major component. In this paper, Retraction of Certificate with Claiming Ability for MANETs scheme is proposed in order to evict the interlopers. And to improve the trustworthiness of the scheme, claiming ability is proposed in order to rescue from the deceiving nodes.

Keywords: component; formatting; style; styling; insert (key words)

I. INTRODUCTION

Mobile ad hoc network (MANET) has gained much of its attraction due to its unique features such as mobility, dynamicity and also due to the low cost spent on its network construction. Mobile devices could be laptops, cell phones and any devices which are mobilized. In MANETs the transmission range and battery capability of a device is very limited, hence nodes help each other in order to send and receive the data from source to destination by acting as the cooperative nodes. Thus, due to all these benefits, MANETs are used in various applications. Examples of the MANET's applications are disaster reliefs, military applications and emergency rescue operations. MANET has an open network environment, where any nodes can join and leave the network at anytime. As a consequence of this, security breaches are more. Thus, provisioning security services for such a hostile environment is of prime importance. Since the infrastructure is absent in MANETs, mobile nodes in the networks must implement all aspects of network functionality themselves; they act as both end users and routers, which relay packets for other nodes. Therefore, the dynamic and wireless natures of MANETs expose them more vulnerable to various types of security attacks than their wired counter parts. Crucial among all security issues in a MANET is certificate supervision, which serves as a medium for conveying trust in a public key infrastructure to secure applications and network services. A comprehensive security solution for certificate supervision includes three elements: prevention, detection and retraction. Research efforts are being made on these areas, such as certificate distribution, intrusion detection, and certificate retraction. Certification is a prior thing to secure network communications. It is embodied as a data structure in which the public key is bound to an attribute by the digital signature of the issuer , and can be used to verify that a public key belongs to an individual and to prevent tampering and forging in mobile ad hoc networks. Many research efforts have been dedicated to mitigate malicious attacks on the network. Certificate retraction is an important task of enlisting and removing the certificate and removing the certificates of nodes been detected to launch attacks on the neighborhood. In other words, if a node is misbehaved or compromised, it should be eliminated from the network and cut off from all its activities immediately. This paper mainly focuses on the fundamental security issue of certificate retraction to provide secure communications in MANETs. The remainder of this paper is organized as follows: Section 2, point outs a brief overview of survey works on certificate retraction techniques in MANETs, and analysis of merits and demerits of both election-based and non-election-based schemes. In this section, main focus is on the merits of both election and non-election based scheme in order to improve certificate retraction. Section 3, gives the layout of the proposed certificate retraction scheme. Section 4 describes a new threshold-based mechanism to improve reliability and accuracy of the proposed mechanism. Section 5 describes the implementation and results. Finally, the conclusion.

II. RELATED WORKS AND MOTIVATION

In the recent past, a comprehensive research work has been carried out by the researchers on the MANET's security issues. Due to its wireless nature, limited physical protection of the nodes, dynamic topology and the lack of infrastructure MANETs are vulnerable to various kinds of security threats. Different kinds of certificate retraction techniques have been proposed to enhance network security in the literature. This section briefly gives an overview on the existing approaches for retraction, namely, election-based mechanism and non-election-based mechanism

A. Electing Mechanism

In the election-based mechanism, interloper's certificate is retracted on the basis of votes from trusted neighboring nodes. Ubiquitous and Robust Access Control Solution (URSA) uses

an election based mechanism to evict nodes. This mechanism makes use of the ticket-based approach. Certified ticket for the newly joining nodes is issued by their neighboring nodes. The operation of URSA access control emphasizes multiple node consensus and fully localized instantiation. Since individual nodes are subject to misbehaviors, this scheme does not rely on any single node. Instead, this scheme leverages the nature of cooperative computing in an ad hoc network and depends on the collective behavior of multiple local nodes. Depending on the behavior of a node, these collaborative nodes will decide whether or not to renew the expiring certified-ticket or not. If a node is legitimate then its ticket is renewed, otherwise if it is found malicious its certified ticket will be retracted and cut off from all its network activities. This scheme faces the problem of setting the threshold value. Another critical issue is that this scheme does not address false complaints from malicious nodes. The scheme proposed by Arboit et al. allows all nodes in the network to vote collaboratively. As with URSA, no Issuing Authority (IA) is present in the network. Hence each node monitors the behavior of its neighbors. The primary difference from URSA is that nodes vote with variable weights. The weight of a node is calculated in terms of the reliability and trustworthiness of the node that is derived from its past behaviors, like the number of complaints against other nodes and that against itself from others. The stronger its reliability, the greater the weight will be acquired. The certificate of an accused node is retracted when the weighted sum from voters against the node exceeds a predefined threshold. By doing so, the accuracy of certificate retraction can be improved. However, since all nodes are required to participate in each election, the communications overhead used to exchange election information is quite high, and it increases the retraction time as well.

B. Discarding mechanism

In the non-election-based mechanism, a given node can be regarded as a malicious attacker will be decided by any node with a valid certificate. The mechanism "suicide for the common good" which is a credential retraction strategy, where the certificate retraction can be done quickly by only one complaint. However, certificates of both accuser and accused nodes must be retracted together. In other words, accuser has to sacrifice itself to remove an attacker from the network. This mechanism drastically reduces the retraction time and communication overhead in the network but due to its suicidal approach, its application is limited. This scheme does not address the issue of false complaints from genuine attackers; as a result accuracy is degraded. "Certificate retraction scheme" uses a centralized certificate issuing authority to monitor the control messages. In this scheme, nodes are collocated themselves to form clusters. Trusted Certificate Issuing Authority (CIA) is responsible for holding accuser node and accused node in the warning list (WL) and black list (BL), respectively. The certificate of the spiteful attacker node can be retracted by any single neighboring node. In addition, it can also handle the issue of deceitful complaint that enables the bogusly complained nodes to be removed from the blacklist by its cluster head (CH). It takes short time to complete the process of certificate retraction.

C. Motivation

Comparisons of both election-based and non-election-based mechanisms discussed above gives us the idea about their merits and demerits. The election-based mechanism has high accuracy in determining whether the accused node is malicious or not. However, retraction process is slow and also, it incurs heavy communication overhead, since all nodes in the network must share complaint details with each other. In contrast, non-election-based method can retract a mischievous node by a single complaint from a legitimate node with valid certificate in the network. This scheme dramatically reduces the retraction time and improves the performance. However, accuracy and reliability will be degraded, in deeming a node whether it is malicious or not. Finally, accentuating the significant difference between election and non-election based methods, former achieves higher accuracy in detecting malicious node, but consumes more time; latter can expedite the retraction process. In this paper, Retraction of Certificate with Claiming Ability for MANET scheme is proposed. As in existing schemes, cluster is subsumed in this scheme, where cluster head is engaged in determining falsely accused nodes within its cluster and regaining their certificates to solve the dispute of false complaint. On the other hand, proposed scheme consolidates the merits of both election-based and non-election based schemes, in accomplishing sincere retraction and depreciating overhead as compared to the election-based scheme, improving the reliability and accuracy as compared to the non-election based scheme. Proposed scheme can swiftly retract the spiteful device's certificate, cease the node's access to the network, and elevate network security

III. PROPOSED METHOD

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. This section gives the introduction of proposed cluster-based model which achieves quick retraction upon receiving only single complaint from its neighboring node. The proposed scheme maintains two different lists, one is warning list and other is blacklist, in order to guard against spiteful nodes from further framing other legitimate nodes. By incorporating the clustering architecture, the cluster head can resolve bogus complaint to relook the bogusly retracted nodes. Since the proposed scheme deals only with issue of certificate retraction, the scheme assumes all nodes have already possessed certificates before entering into the network. In contrary, the scheme focuses mainly on the procedure of certificate retraction once a malicious attacker has been identified, rather than the attack detection mechanism itself. Every single node in the network is able to determine its neighboring attacker nodes which are in the range of one hop away.

A. Cluster Formation

Proposed scheme uses cluster-based architecture to form the topology. Nodes in the network work together to form clusters, which consists of a Cluster-Head (CH) and Cluster Members (CMs) which are within the transmission range of their CH. Certification Authority (CA) is responsible for the allocation and management of certificates of all nodes. Before a node enters into the network it must possess valid certificate from the CA in order to communicate unrestrictedly in a mobile ad hoc network. A node in a network is allowed to declare itself as a CH with a probability P. Routing discovery protocols, such as periodical broadcast of the hello packets, are effective approaches to check the availability of the links. If a node receives new hello packet, then a new link is found. Meanwhile, if node receives none of the hello packets within the given interval, then the link is considered as disconnected. In the Cluster-based model, if a node declares itself as a CH, it disseminates the Cluster-Head Hello Packet (CHHP) to report neighboring nodes in a timely manner. The nodes which are within the transmission range of the CH can accept the hello packet to confirm their participation in the cluster as cluster members. Upon receiving the CHHP, the CMs reply with a CM Hello Packet (CMHP) to set up connection with the CH. Thereafter, the CM will join this cluster; at the same time, CH and CM keep in touch with each other by exchanging CCHP and CHMP in the time interval Ti. In order to provide stability against the topological changes, it is assumed that, CM belongs to two different clusters. If a CM moves out of the transmission range of the CH, it has to search for other CHHP to join a new cluster. Meanwhile, if a node does not receive any CHHP for the interval 2Ti, then there is no CH within its one-hop range. Hence, the node declares itself as the CH and disseminates CHHP to form a new cluster. On the other hand, if there is no CM nodes within one hop range of the CH, but if there are other CHs in its neighborhood, this node assigns itself as a CM to communicate with two of the CHs and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

B. Function of Issuing Authority (CA)

Certification Authority (CA) is a trusted third party, which is responsible for providing the valid certificates to all nodes in the cluster. It is also responsible for tracking Warning Lists (WL) and Black Lists (BL) to hold accusing and accused nodes, respectively. The CA does this on the basis of received control messages. Each neighboring node has permission to accuse other nodes only once. Furthermore, CA is responsible for disseminating the information of WL and BL to the entire network in order to retract attacker's certificates listed in BL and remove them from further participating in the network activities. Classification of nodes in the scheme based on their behaviours and reliability According to node's behavior in the network, classification can be done in three ways: legitimate node, malicious node and attacker node. A legitimate node is one which is loyal to all other nodes in the network and ensures secure communication with them. It further, detects the attacks from the malicious attacker nodes and helps CA to retract their certificates and ensuring security within the network. A malicious node is one which accuses falsely against legitimate nodes to retract their certificates. Furthermore, it does not votes honestly and detect attacker nodes which are misbehaving. The attacker node is type of malicious node, which launches attacks on its neighboring nodes to disrupt secure communication. In the proposed scheme nodes are further classified into three types based on their reliability: normal node, warned node and retracted node. When a node enters into the network, it is regarded as the legitimate node if it does not set attacks against the other nodes in the network. This kind of a node can be considered as highly reliable node and can accuse misbehaving nodes and it could become CH or CM. Furthermore, normal nodes may consist of both malicious as well as legitimate nodes. The nodes which are enlisted in the warning list are considered as accused nodes with less reliability. Since, normal nodes consists the combination of both legitimate and malicious nodes, warned nodes are considered as distrust nodes. Warned nodes are permitted to communicate with their neighbors with some restrictions, e.g., they cannot accuse other nodes in the network to avoid false complaint by these malicious nodes. The nodes which are enlisted in the blacklist are considered as retracted nodes with low reliability. Certificates of these nodes are retracted and hence, they are evicted from the network activities.

WL	RL
N7	N6

C. Certificate Retraction

C.1 Steps to evict malicious attacker nodes

In order to evict malicious attacker node's certificate we must take into account of three stages: complaint, verification and notification. When a node detects the attacks from the neighboring node, it checks it's black list (BL), if the attacker is not detected then, the neighboring node sends the Complaint Information Packet (AIP), to the CA. In this process, all trustful neighboring nodes must participate in the retraction process, in order to forward their opinion against the detected node. After receiving the first received AIP, the CA validates accusing nodes certificate by taking its location ID, if validation is successful then CA retracts attacker nodes certificate and it will be added to the RL. Alongside, CA adds accusing node to the WL. Furthermore, CA disseminates retraction information to all the nodes in the network along with RL and WL. The nodes which are in the RL are retracted nodes.

Algorithm for retraction of a malicious node is given below:

Step 1: Neighboring nodes N7, N8, N4 detects the launched attack of N6.

Step 2: Each of them sends an complaint information packet to the CA against N6.

Step 3: CA checks the validity of first received complaint information packet (e.g. from node N8), the CA holds N8 in WL and N6 in RL.

Step 4: The CA broadcasts the retraction information to all the

nodes in the network.
Step 5: All nodes in the network update their WL and RL to retract N6's certificate.

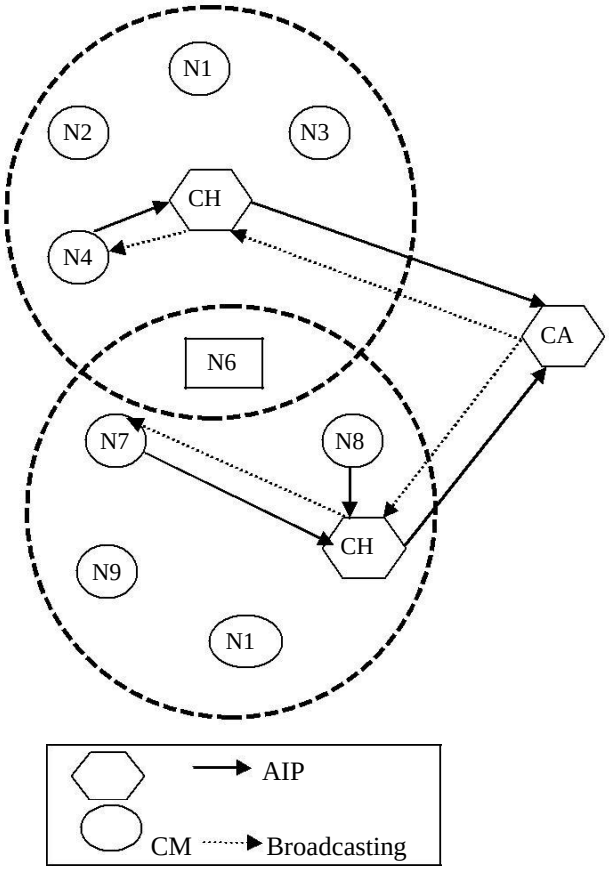

Fig 3 retracting a node's certificate

C.2 Dealing with Fake Complaint from a malicious attacker

In order to increase the accuracy and reliability of the proposed scheme, CH is enabled to detect fake complaint from a malicious attacker and recovering the certificate of falsely accused node within its cluster. Since CH's can intercept the attacks from its CM's, whenever each of these CH's detects the fake complaint from a malicious attacker, it sends recovery information packets (RIPs) to the CA to restore the certificate of a framed node. After receiving the recovery information packet from the CH, CA removes the falsely accused node from RL to restore its certificate. The procedure for handling the fake complaint is described below. The CA broadcasts the information of WL and RL to all the nodes in the network, even if there is a fake complaint. All the nodes in the network update their WL and RL. After updating the WL and RL, CH does not detect any attacks from a specific accused member held in RL from the CA, and CH determines that accused node is framed. Hence, CH sends recovery information packet to CA in order to justify and review this member from the network. Upon receiving the recovery information packet, the CA checks the sender's certificate validity, and further it releases the falsely accused node from the RL and holds in the WL. Further, CA disseminates the RL and WL to all the nodes in the network.

Fig 4 illustrates the procedure to overcome fake complaint.

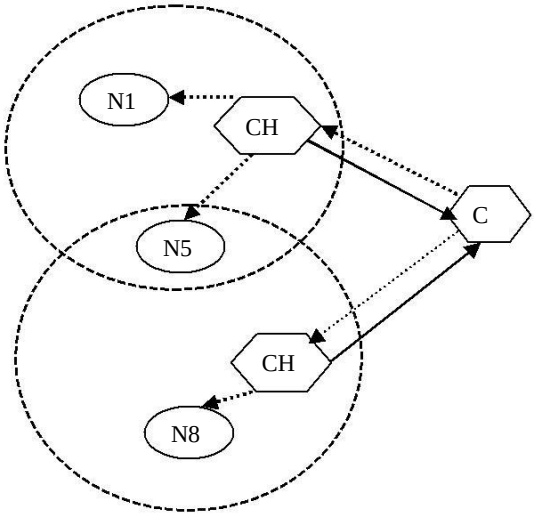

Fig 4. Coping with fake complaint.

Algorithm to overcome false complaint

Step 1: The CA broadcasts the WL and RL to all the nodes in the network.

Step 2: All nodes in the network update their WL and RL, and find that node N5 is framed.

Step 3: Cluster heads CH1 and CH2 send recovery information packet to the CA, in order to recover falsely accused node N5.

Step 4: On receiving the first recovery information packet (e.g. from CH1), CA removes N5 from the RL and holds N5 in the WL, further it broadcasts updated information to all the nodes in the network.

Step 5: All nodes in the network update their WL and RL to restore N5.

IV. NUMERICAL RESULTS

Numerical methods to determine Optimum limit to retract a node's certificate.

Method 1: Reducing the probability of erroneous release.
Probability of erroneous release of spiteful nodes by complaining against genuine node to retract its credentials is given by

$$P_e(M) = \sum_{k=0}^{N}$$

Here, M is the maximum value out of N neighbors falsely complains against genuine node. P denotes the probability of a node which takes part in fake complaining. For example, Fig 5a shows that (1) is decreasing constantly where N is set to 1. Greater the optimal value, lesser the spiteful node released, thus the higher accuracy is. Hence, the value of Pe must be less to reduce the probability of falsely releasing spiteful nodes from CL.

Method 2: Increasing the probability of true release
In this method, the value of O is determined on the basis of probability Pt that at least O out of N nodes must correctly

complain against the spiteful node, in order to release genuine node from the CL.

$$Pt(M) - \sum_{O} \quad (2)$$

Here (1-p) means the probability of a node which takes part in true complaining. The value Pt should be large to successfully release genuine node from the complaining list. As shown in Fig. 5b, Pt drops as optimal value reaches O

WL	RL
CH1,N5	~~N5~~

Method 3: Increasing Accuracy

We know that there is tradeoff between erroneous release probability Pe and true release probability Pt .In order to achieve high accuracy the optimum value F (O) must be the difference between Pe and Pt. Taking N=15, in our example, Fig. 5c shows that the curve of is the maximum when O is equal to N/2, which is the desired optimal value.

$$F(O) = Pe - Pt \quad (3)$$

V. PERFORMANCE EVALUATION.

Simulation has been conducted in NS2 (network simulator) in order to evaluate the performance. Same will be presented in this section. To evaluate performance, simulation runs has been made for retracting certificate, efficiency in releasing genuine nodes and comparing the obtained results with the theoretical results.

A. Deriving optimal value O

In this simulation run, comparisons have been made with obtained results and theoretical results. Simulation is set up for 24 nodes in the network which consists of two hackers and four spiteful nodes. Optimum value O is set to 15 and is varied between 1 and 15, to determine the type of node. As shown in the Fig.6 obtained Pe and Pt are close to the numerical results. Accuracy can be determined by the plot against the Optimum value O and F as shown in the Fig. 6b, which shows O= N/2 is a consistent value. In conclusion, simulation results are close to numerical results.6.2

Retraction time is an important parameter for the performance evaluation. The difference between, attack launching time and the credential retraction time will give retraction time. The Fig 6c shows that the proposed scheme is efficient than existing schemes.

VI. CONCLUSION

In this paper, major security issue of certificate retraction is addressed to enhance network security. This scheme inherits the mechanisms of both election-based and non-election based scheme. In contrast to existing scheme, proposed scheme have ability to sustain fake complaints. Further, analysis of simulation results with theoretical results and comparison of obtained simulation results with previously proposed scheme demonstrates that proposed method is more reliable and accurate in certification retraction of an attacker. Proposed method also reduces the retraction time. Hence, the proposed method is efficient for certificate retraction.

