ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

IJIRSET

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, January 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th Feburary Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering,Rasipuram,Tamilnadu, India

Efficient Certificate Revocation of Attacker nodes using CCRVC in Mobile Ad Hoc Networks

V. Kalaivani [1], M. Ashwin [2]

[1, 2] Department of Computer Science and Engineering, Adhiyamaan college of Engineering, Hosur, India

***Abstract* - Mobile Ad Hoc Networks (MANETs) is a self-configuring, infrastructure less network of mobile devices connected by wireless. The wireless and dynamic nature of MANET leads to various types of security attacks. The primary task is to provide the secure communication. To come across this challenge, we propose Cluster based Certificate Revocation with Vindication Capability scheme for certificate revocation from the attacker node and isolate the attackers from further communication in the network. In addition, we have adopted the one-hop neighbor selection method for none of the intermediate node is an attacker node from source to destination. This provides an effective and efficient secure communication in MANET.**

***Index Terms:*Mobile Ad Hoc Networks, Certificate Revocation, Security, One-hop neighbor selection method**

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a collection of mobile devices that can communicate with each other without any centralized administration; A MANET can be constructed quickly at low cost and flexible in nature. A Mobile Ad Hoc Network is attractive for applications such as disaster relief, emergency operations, military services, vehicle network and so on. A MANET is characterized by having a dynamic, continuously changing network topology due to mobility of nodes. This feature makes it difficult to perform secure communication in a Mobile Ad Hoc Network compared with a conventional wired network. Implementing security is of prime importance in such networks. Among all security issues in MANETs, certificate management is a widely used mechanism.

Mobile Ad Hoc networks are vulnerable to various passive and active security [1] attacks that are launched by internal and external attackers. But because of special characteristics of MANETs, such as lack of any fixed infrastructure, mobility of nodes and limited bandwidth of wireless communication, establishing security in Mobile Ad Hoc Network is a challenging issue.

The ultimate goal of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack.

Since the nodes in a MANET are highly mobile, the topology changes frequently and the nodes are dynamically connected in an arbitrary manner. The rate of change depends on the velocity of the nodes. Consequently, the radio coverage of a node is small. The low transmission power limits the number of neighbor nodes, which further increases the rate of change in the topology as the node moves.

The example of MANET shown in Fig. 1, describes if node A wants to transmit data to node E (outside of its coverage area), it must transmit the data through the intermediate nodes, and they must collaborate forwarding the data until it reaches its destination (node E).

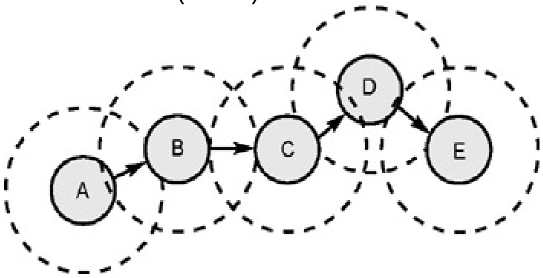


Fig. 1. Example of MANET

A. Approach

Certificate Revocation is an important task of removing the certificate from the attacker nodes in the network. If any node is compromised or misbehaved, it should be removed from the network by revoking the certificate. The reminder of this paper is organized as follows: In Section II, we give a brief overview of related works on certificate revocation techniques in MANETs.

Section III describes the structure of the proposed cluster-based scheme and introduces the certificate revocation process. In Section IV, describes the one-hop neighbor selection method provides high throughput. We devote Section 5, the performance evaluation of our scheme. Finally, we conclude the paper in Section VI.

II. RELATED WORK

It is difficult to provide secure mobile ad hoc networks, notably because of the vulnerability of wireless links, the limited physical protection of nodes, the dynamically changing topology, and the lack of infrastructure. In this section, we briefly introduce the existing approaches for certificate revocation, which are classified into two categories: voting- based mechanism and non-voting-based mechanism.

A. Voting-Based Mechanism

The certificate revocation of an attacker nodes are performed based on the votes from its neighbors. The number of negative votes exceeds a predefined number; the certificate of an accused node will be revoked. However, determining the threshold remains a challenge.

B. Non-Voting-Based Mechanism

In Non-Voting-Based mechanism, a malicious node will be decided by any node with a valid certificate. " Suicide for the common good" [2] strategy, where certificate revocation can be quickly completed by only one accusation. However, certificates of both the accused node and accusing node have to be revoked simultaneously. In other words, the accusing node has to sacrifice itself to remove an attacker from the network. Although this approach dramatically reduces both the time required to evict a node and communications overhead of the certificate revocation procedure due to its suicidal strategy, the application of this strategy is limited. Furthermore, this suicidal approach does not take into account of differentiating falsely accused nodes from genuine malicious attackers.

III. OVERALL APPROACH

A. Problem Statement

The significant advantage of the voting-based mechanism is the high accuracy in confirming the given accused node as a real malicious attacker or not. The decision process to satisfy the condition of certificate revocation [3] is, however, slows. Also, it incurs heavy communications overhead to exchange the accusation information for each other.

On the contrary, the non-voting-based method can revoke a suspicious misbehaved node by only one accusation from any single node with valid certification in the network. However, 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. Tremendous amount of research effort has been made in these areas, such as certificate distribution [4], attack detection [5] and certificate revocation [6].

In this paper, a Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme is used. A trusted third party, certification authority (CA), is deployed in the cluster-based scheme [7] to enable each mobile node to preload the certificate. The CA is also in charge of updating two lists, Warning List (WL) and Black List (BL), which are used to hold the accusing and accused nodes' information, respectively. Concretely, the BL is responsible for holding the node accused as an attacker, while the WL is used to hold the corresponding accusing node. The CA updates each list according to received control packets. Note that each neighbor is allowed to accuse a given node only once. Furthermore, the CA broadcasts the information of the WL and BL to the entire network in order to revoke the certificates of nodes listed in the BL and isolate them from the network.

B. Revoking Malicious Certificates

The revocation [8] procedure begins at detecting the presence of attacks from the attacker node. Then, the neighboring node checks the local list BL to match whether this attacker has been found or not. If not, the neighboring node casts the Accusation Packet (AP) to the CA. Note that each legitimate neighbour promises to take part inthe revocation process, providing revocation request against the detected node.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

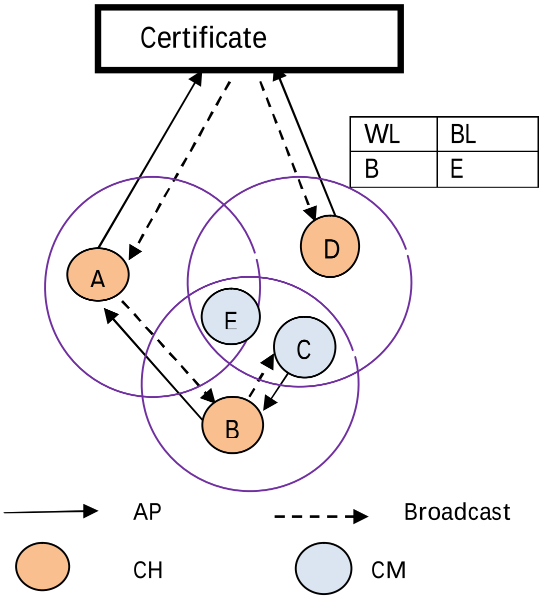
An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, January 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th Feburary Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering,Rasipuram,Tamilnadu, India

After that, once receiving the first arrived accusation packet, the CA verifies the certificate validation of the accusing node: if valid, the accused node is deemed as a malicious attacker to be put into the BL. Meanwhile, the accusing node is held in the WL. Finally, by broadcasting the revocation including the WL and BL through the whole network by the CA, nodes that are in the BL are successfully revoked from the network.



WL	BL
B	E

Fig. 2. Revoking a node's certificate

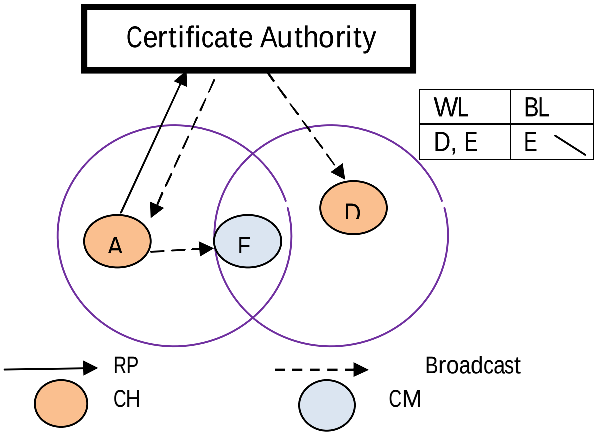
For example, a malicious attacker E widely launches attacks within one-hop transmission range, as shown in Fig. 2, the procedure of revocation is described in the following:

- Neighboring nodes B, C and D detect attacks from node E.
- Each of them sends out an accusation packet to the CA against E.
- According to the first received packet (e.g., from node D), the CA hold D and E in the WL and BL, respectively, after verifying the validity of node D.
- The CA disseminates the revocation message to all nodes in the network.
- Nodes update their local WL and BL to revoke E's certificate.

C. False Accusation

The CA disseminates the information of the WL and BL to all the nodes in the network, and the nodes update their BL and WL from the CA even if there is a false accusation. Since the CH does not detect any attacks from a particular accused member enlisted 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 to the CA in order to vindicate and revive this member 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 held in the WL. Furthermore, the CA propagates this information to all the nodes through the network.



WL	BL
D, E	E ╲

Fig.3. Dealing with False Accusation

Fig. 3 illustrates the process of addressing false accusation as follows:

- The CA disseminates the information of the WL and BL to all nodes in the network.
- CH A and D update their WL and BL, and determine that node E was framed.
- A and D send a recovery packet to the CA to revive the falsely accused node E.
- Upon receiving the first recovery packet (e.g., from D), the CA removes E from the BL and holds D and E

in the WL, and then disseminates the information to all the nodes.

- The nodes update their WL and BL to recover node E.

IV. ONE-HOP NEIGHBOR SELECTION METHOD

In the real world, most of the nodes have a selfish behavior, being unwilling to forward packets for others in order to save resources. In our proposed system, finds the attacker node in the network and revoke the certificate. The attacker node will typically not cooperate in the transmission of packets, seriously affecting network performance.

Therefore, detecting these nodes and select alternative path is essential for network performance. So we find out alternative path (not in the attacker node between source to destination) from source to destination communication. We modeled its performance using one-hop neighbor selection method.

Here mentioned two comparisons such as attacker node is one of the hop nodes between source to destination communication, and select best path that it doesn't have any attacker node. Throughput will be high in the best path compared to normal path because attacker node hack the data or drop the data through communication.

V. SIMULATION SETUP

In this section, we are going to revoke the certificate of malicious nodes using CCRVC scheme.

A. Simulation Parameter

We simulate this MANET environment within 500 m by 500 m terrain in NS2 simulator for 802.11b, running Dynamic Source Routing (DSR) as the routing protocol. The devices are deployed in a random uniform distribution, and each device is seen as a node which has the fixed transmission range as 200m.

The random way-point mobility pattern is used to model node movements. Each node is assumed to move to a randomly selected location at different velocities from 1 to 8 m/s. The probability R that the newly joining node becomes a CH is 0.4.

Parameter	Value
Node placement	Uniform distribution
Trans. range	200m
Node speed	1m/s-8m/s
CH chosen probability, R	0.4
Simulation Time	500s

B. Results

Fig. 4 clearly demonstrates that it can effectively reduce the number of nodes listed in the WL, i.e., the number of available nodes in the network has been improved by using the CCRVC scheme. We can see that the number of nodes listed in the WL is almost equal to the number of attacker nodes. Actually, almost all the malicious nodes are successfully kept in the WL.

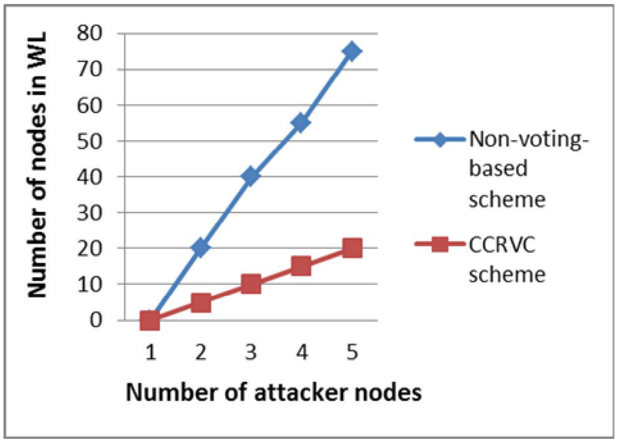


Fig. 4. The number of nodes in WL.

Revocation time is an important factor for evaluating the performance of the revocation scheme. Revocation time is defined as the time from an malicious node's launching the attack until its certificate is revoked.

To evaluate the impact of different numbers of attacker nodes on the revocation time, 50 legitimate nodes are considered in the network, while the number of malicious nodes is varied from 1 to 19. Fig. 5 presents how the revocation time changes with different numbers of malicious nodes between the existing schemes (i.e., voting-based scheme) and the CCRVC scheme.

Note that as the number of attacker nodes is not larger than the number of legitimate nodes, the results always converge because there are enough legitimate nodes to revoke attackers' certificates within finite time in our simulation. Obviously, the voting-based scheme requires longer revocation time than that of our proposed scheme.

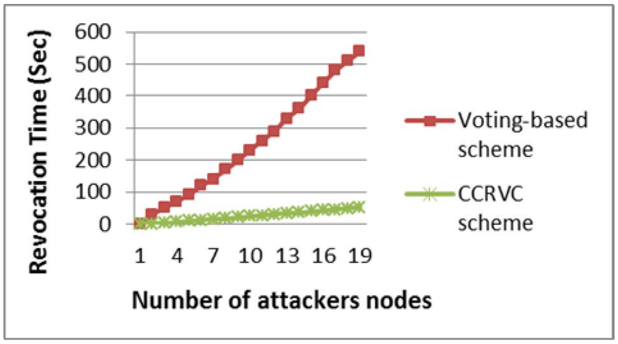


Fig: 5. Revocation time

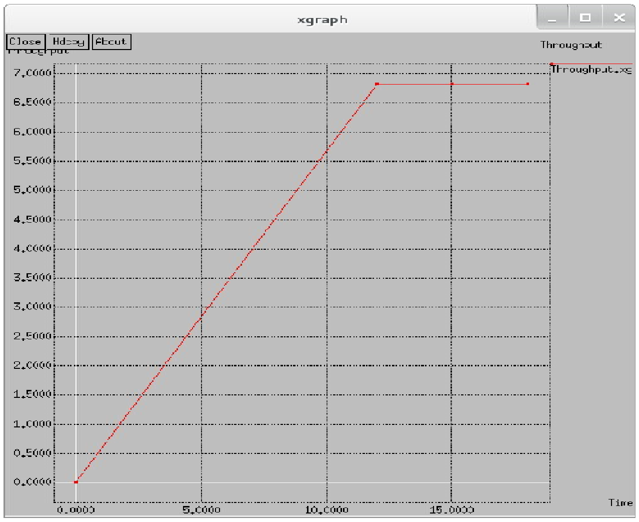


Fig 6. Throughput

Throughput is high in the best path compared to normal path because attacker node hack the data or drop the data through communication.

IV.CONCLUSIONS

The proposed 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. 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.

The extensive results have demonstrated that, in comparison with the existing methods, our proposed CCRVC scheme is more effective and efficient in revoking certificates of 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. 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, July2006.

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

4. L. Zhou, B. Cchneider, and R. Van Renesse, "COCA: A Secure Distributed Online Certification Authority," ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002.

5. P. Yi, Z. Dai, Y. Zhong, and S. Zhang, "Resisting Flooding Attacks in Ad Hoc Networks," Proc. Int'l Conf. Information Technology: Coding and Computing, vol. 2, pp. 657-662, Apr.2005.

6. S. Micali, "Efficient Certificate Revocation," Massachusetts Inst. Of Technology, Cambridge, MA, 1996.

7. J. Lian, K. Naik, and G.B. Agnew, "A Framework for Evaluating the Performance of Cluster Algorithms for Hierarchical Networks,"IEEE/ACM Trans. Networking, vol. 15, no. 6, pp. 1478-1489,Dec. 2007.

8. 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.