www.ijiarec.com

ISSN:2348-2079

Volume-5 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Cluster based certificate revocation For mobile ad hoc networks

[1]Mrs.C. Navamani MCA., M.Phil., M.E., Assistant Professor,
[2]Ms. N. Aasifa Final M.C.A,
Department of MCA, Nandha Engineering College (Autonomous), Erode - 52.
E-Mail-ID: navamanimca@gmail.com, aasifa2315@gmail.com

Abstract — Mobile Ad hoc Networks (MANETs) have attracted much attention due to their mobility and ease of deployment. However, the wireless and dynamic natures render them more vulnerable to various types of security attacks than the wired networks. The major challenge is to guarantee secure network services. To meet this challenge, certificate revocation is an important integral component to secure network communications. In this paper, we focus on the issue of certificate revocation to isolate attackers from further participating in network activities. For quick and accurate certificate revocation, we propose the Cluster-based Certificate Revocation with Justification Capability (CCRVC) scheme. In particular, to improve the reliability of the scheme, we recover the warned nodes to take part in the certificate revocation process; to enhance the accuracy, we propose the threshold-based mechanism to assess and vindicate warned nodes as legitimate nodes or not, before recovering them. The performances of our scheme are evaluated by both numerical and simulation analysis. Extensive results demonstrate that the proposed certificate revocation scheme is effective and efficient to guarantee secure communications in mobile ad hoc networks.

.Index Terms—Mobile ad hoc networks (MANETs), certificate revocation, security, and threshold

1. INTRODUCTION

Mobile Ad hoc Networks (MANETs) have received increasing attention in recent years due to their mobility feature, dynamic topology, and ease of deployment. A mobile ad hoc network is a self-organized wireless network which consists of mobile devices, such as laptops, cell phones, and Personal Digital Assistants (PDAs), which can freely move in the network. In addition to mobility, mobile devices cooperate and forward packets for each other to extend the limited wireless transmission range of each node by multihop relaying, which is used for various applications, e.g., disaster relief, military operation, an emergency communications.

Security is one crucial requirement for these network services. Implementing security is therefore of prime importance in such networks. Provisioning protected communications between mobile nodes in a hostile environment, in which a malicious attacker can launch attacks to interrupt network security, is a primary concern. Owing to the absence of infrastructure, mobile nodes in a MANET have to implement all aspects of network functionality themselves; they act as both end users and routers, which relay packets for other nodes. Unlike the conventional network, another feature of MANETs is the open network environment where nodes can join and leave the network freely. Therefore, the wireless and dynamic natures of MANETs expose them more susceptible to various types of security attacks than the wired networks.

Among all security issues in MANETs, certificate management is a widely used mechanism which serves as a means of conveying trust in a public key infrastructure to secure applications and network services. A complete security solution for certificate management should encompass three components: prevention, detection, and revocation. Tremendous amount of research effort has been made in these areas, such as

certificate distribution attack detection and certificate revocation. Certification is a requirement 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 interfering and forging in mobile ad hoc networks. Many research efforts have been dedicated to mitigate malicious attacks on the network. Any attack should be identified as soon as possible. Certificate revocation is an important task of enlisting and removing the certificates of nodes that have been detected to launch attacks on the neighborhood. In other words, if a node is compromised or misbehaved, it should be removed from the network and cut off from all its activities immediately. In our research, we focus on the fundamental security problem of certificate revocation to provide secure communications in MANETs.

2 RELATED WORK AND MOTIVATION

Recently, researchers pay much attention to MANET security issues. It is difficult to secure mobile ad hoc networks, notably because of the susceptibility of wireless links, the limited physical protection of nodes, the dynamically changing topology, and the lack of infrastructure. Various kinds of certificate revocation techniques have been proposed to enhance network security in the literature. 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.

2.1 Voting-Based Mechanism

The so-called voting-based mechanism is defined as the means of revoking a malicious attacker's certificate through votes from valid neighboring nodes.

The certificates of newly joining nodes are issued by their neighbors. The certificate of an attacker is revoked on the basis of votes from its neighbors. Each node performs one-hop monitoring, and exchanges monitoring information with its neighboring nodes. When the number of negative votes exceeds a predetermined number, the certificate of the accused node will be revoked. Since nodes cannot communicate with others without valid certificates, revoking the certificate of a voted node implies isolation of that node from network activities. Defining the threshold, however, remains a challenge. If it is much larger than the network degree, nodes that launch attacks cannot be revoked, and can successively keep communicating with other nodes. The scheme proposed by all nodes in the network to vote together no Certification Authority (CA) exists in the network, and instead each node monitors the behavior of its neighbors. By doing so, the accuracy of certificate revocation can be improved. However, since all nodes are required to participate in each voting, the communications overhead used to exchange voting information is quite high, and it increases the revocation time as well.

2.2 Non-Voting Based Mechanism

In the non-voting-based mechanism, a given node deemed as a malicious attacker will be decided by any node with a valid certificate. 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. Proposed a cluster-based certificate revocation scheme, where nodes are self-organized to form clusters. In this scheme, a trusted certification authority is responsible to manage control messages, holding the accuser and accused node in the warning list (WL) and block list (BL), respectively. The certificate of the malicious attacker node can be revoked by any single neighboring node. In addition, it can also deal with the issue of false accusation that enables the falsely accused node to be removed from the block list by its Cluster Head (CH). It takes

a short time to complete the process of handling the certificate revocation.

3. MODEL OF THE CLUSTER-BASED SCHEME

The proposed cluster-based revocation scheme, which can quickly revoke attacker nodes upon receiving only one accusation from a neighboring node. The scheme maintains two different lists, warning list and block list, in order to guard against malicious nodes from further framing other legitimate nodes. Moreover, by adopting the clustering architecture, the cluster head can address false accusation to revive the falsely revoked nodes. Owing to addressing only the issue of certificate revocation, not certificate distribution, the scheme assumes that all nodes have already received certificates before joining network.

3.1 Cluster Construction

The cluster based architecture to construct the topology. Nodes cooperate to form clusters, and each cluster consists of a CH along with some Cluster Members (CMs) located within the transmission range of their CH. Before nodes can join the network, they have to acquire valid certificates from the CA, which is responsible for distributing and managing certificates of all nodes, so that nodes can communicate with each other unrestrainedly in a MANET. The nodes that are in this CH's transmission range can accept the packet to participate in this cluster as cluster members.

3.2 Function of Certification Authority

A trusted third party, certification authority, is deployed in the cluster-based scheme to enable each mobile node to preload the certificate. The CA is also in charge of updating two lists, WL and Block list, 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. 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.

3.3 Reliability-Based Node Classification

According to the behavior of nodes in the network, three types of nodes are classified according to their behaviors: valid, malicious, and attacker nodes. A valid node 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. A malicious node does not execute protocols to identify misbehavior, vote honestly, and revoke malicious attackers. In particular, it is able to falsely accuse a valid node to revoke its certificate successfully. The so-called attacker node is defined as a special malicious node which can launch attacks on its neighbors to disrupt secure communications in the network. In our scheme, these nodes can be further classified into three categories based on their reliability: normal node, warned node, and revoked node. When a node joins the network and does not launch attacks, it is regarded as a normal node with high reliability that has the ability to accuse other nodes and to declare itself as a CH.

3.4 Certificate Revocation

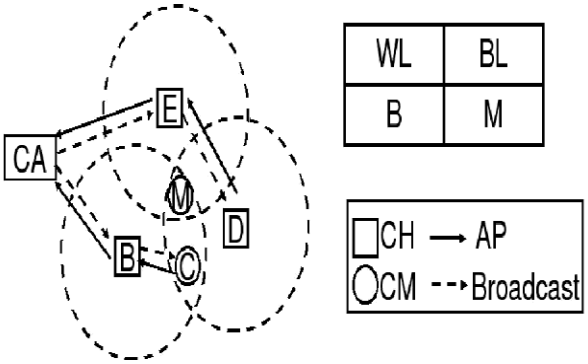
3.4.1 Procedure of Revoking Malicious Certificates

The process of certificate revocation. To revoke a malicious attacker's certificate, we need to consider three stages: accusing, verifying, and notifying. The revocation 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, which the format of accusation packet is each legitimate neighbor promises to take part in the revocation process, providing revocation request against the detected node. 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 message including the WL and BL through the whole network by the CA, nodes that are in the BL are successfully revoked from the network.

3.4.2 Coping with False Accusation

The false accusation of a malicious node against a valid node to the CA will degrade the accuracy and robustness of our scheme. To address this problem, one of the aims of constructing clusters is to enable the CH to detect false accusation and restore the falsely accused node within its cluster. Since each CH can detect all attacks from its CMs, requests for the CA to recover the certificate of the falsely accused node can be accomplished by its CHs by sending Recovery Packets (RPs). Upon receiving the recovery packet from the CH, the CA can remove the falsely accused node from the BL to restore its legal identity. The sequence of handling false accusation is described hereafter. First of all, 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. Then, the CH sends a recovery packet to the CA in order to vindicate and recover 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.



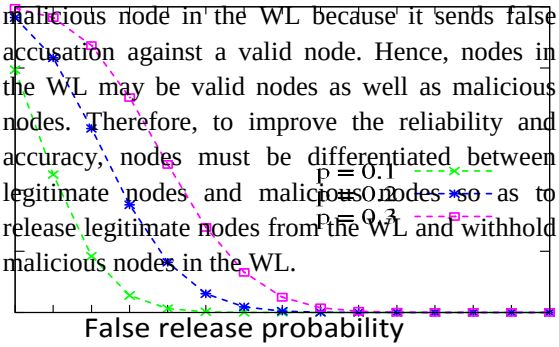
4. WL Management

4.1 Normal Nodes Depreciation

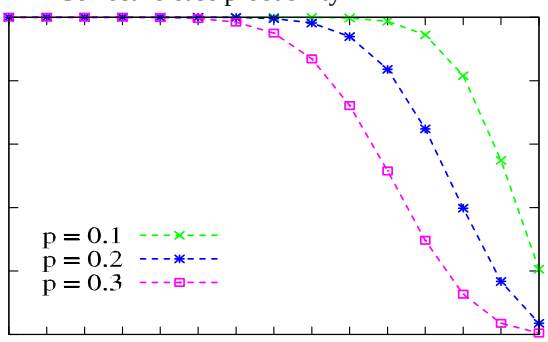
Nodes enlisted in the WL by certificate revocation lose the function of accusation since the CA does not accept accusation packets from nodes enlisted in the WL in order to prevent further damage from malicious nodes. Thus, as the number of malicious nodes increases, an increasing number of normal nodes are listed in the WL. Subsequently, there will not be enough normal nodes to accuse the attacker nodes over time. Such scenario will affect the reliability of the scheme. Intuitively, if there are sufficient normal nodes around malicious attackers, the scheme is efficient in revoking attackers rapidly. On the contrary, if no normal node is available around an attacker node which is launching attacks to the neighborhood, the scheme cannot detect and revoke this attacker immediately until a normal node roams into the attacker's transmission range.

4.2 Node Releasing

Legitimate node correctly accuses an attacker node, thus resulting in the accusing node and accused node being listed in the WL and BL, respectively; the other case is the enlisting of a malicious node in the WL because it sends false accusation against a valid node. Hence, nodes in the WL may be valid nodes as well as malicious nodes. Therefore, to improve the reliability and accuracy, nodes must be differentiated between legitimate nodes and malicious nodes so as to release legitimate nodes from the WL and withhold malicious nodes in the WL.



Correct release probability



5. PERFORMANCE EVALUATION

We present simulation results conducted in the network to demonstrate the optimal threshold K, we design the experiment to measure Pf and Pc in comparison with those of numerical results, and observe the impact of different threshold values. To evaluate the performances of our proposed CCRVC scheme, we run simulations to verify its efficiency in releasing legitimate nodes from the WL and revoking attacker nodes' certificates, and compare them with the existing schemes. In particular, we are interested in the revocation time to evaluate the efficiency and reliability of certificate revocation in the presence of malicious attacks. Furthermore, we also estimate the accuracy of releasing legitimate nodes in our CCRVC scheme.

5.1 Simulation Setup

We consider a realistic environment, where there are many devices (mobile phones, laptops, PDAs, etc.) to construct a mobile ad hoc network within a certain area (campus, station, etc.). These devices move randomly and communicate with their neighboring devices in the network. 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 10 m/s.

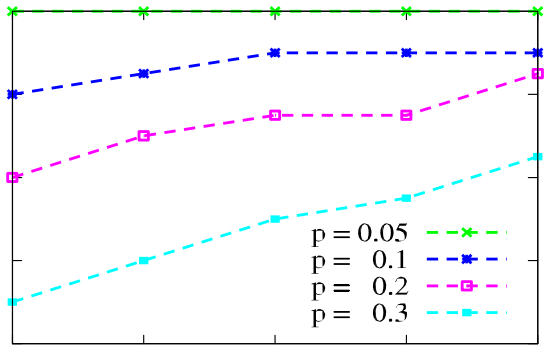
5.2 Deriving the Optimal Threshold K

We prove the optimum threshold value in comparison with the numerical result. We set 80 nodes in the network, which contains eight malicious nodes and eight attacker nodes. The simulation results of Pf and Pc demonstrate that they are close to the mathematically analyzed results. To determine the optimal value of K, which enables our scheme to achieve the maximum accuracy, plot in the value of is the maximum when the threshold K is set to 8. As a consequence, the optimal threshold K is equal to N/2, which is indeed consistent with the mathematical analysis.

5.3 Comparing the Effectiveness of Certificate Revocation

The threshold method is able to release nodes from the WL, to evaluate the effectiveness of our CCRVC scheme; we first observe the change of the number of nodes in the WL according to different number of malicious nodes. In this experiment, we deploy 100 nodes in the network, where both the number of malicious and attacker nodes are set to 5, 10, 15, and 20 for each simulation run, respectively. Revocation time is an important factor for evaluating the performance of the revocation scheme. Revocation time is defined as the time from an attacker 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 valid nodes are considered in the network, while the number of attacker nodes is varied from 10 to 50.

Number of warned nodes



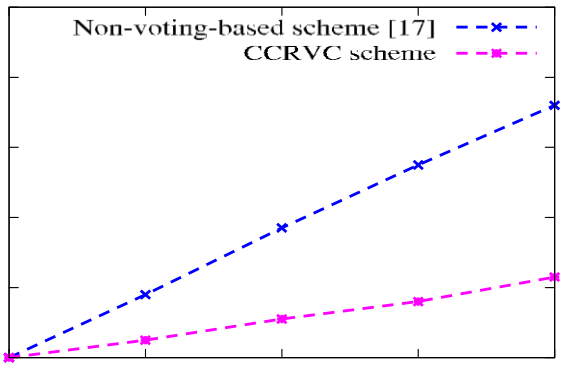
5.4 Accuracy of Releasing Nodes

The accuracy of releasing nodes from the WL by using our proposed CCRVC scheme, we first define the accuracy as

Accuracy ¼ 1 _ Rfalse _ Run released

Where R false denotes the probability of the falsely released nodes and Run released means the probability of the unreleased valid nodes (legitimate nodes enlisted in the WL have not been correctly released). The node density varies from 60 to 100 nodes=km2. Both of the malicious nodes and attacker nodes are set to account for 5, 10, and 15 percent of the total number of nodes in the simulation, respectively. The accuracy continues to improve with the increase of the node density.

Number of attacking node



6. CONCLUSION

In this paper, we have addressed a major issue to ensure secure communications for mobile ad hoc networks, namely, certificate revocation of attacker nodes. In contrast to existing algorithms, we propose a cluster-based certificate revocation with evidence capability scheme combined with the merits of both voting-based and non-voting based mechanisms to revoke malicious certificate and solve the problem of false accusation. The 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 accepted the cluster-based model to restore falsely accused nodes by the CH, thus improving the accuracy as compared to the non-voting based mechanism. Particularly, we have proposed a new incentive method to release and restore the valid nodes, and to improve the number of available normal nodes in the network. In doing so, we have satisfactory nodes to ensure the efficiency of quick revocation.

REFERENCE

[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] P. Sakarindr and N. Ansari, "Security Services in Group Communications Over Wireless Infrastructure, Mobile Ad Hoc, and Wireless Sensor Networks," IEEE Wireless Comm., vol. 14, no. 5, pp. 8-20, Oct. 2007.

[3] 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.Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002.

[4] 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[4] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, Nov./Dec. 1999.

[5] L. Zhou, B. Cchneider, and R. Van Renesse, "COCA: A Secure Distributed Online Certification Authority," ACM Trans. Computer. 3, pp. 233-247, July 2005.

[6] 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.

[7] 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.

[8] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, "A Dynamic Anomaly Detection Scheme for Aodv Based Mobile Ad Hoc Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 5, pp. 2471-2481, June 2009.

[9] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Network: Analysis & Defenses," Proc. Third Int'l Symp. Information Proces