ISSN: 2321-7782 (Online)
Volume 3, Issue 3, March 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

A Review on: Clustering Based Certificate Revocation Scheme for Malicious Nodes in MANET

Ruchita H. Bajaj[1]
Pursuing M.E. in CS-IT
HVPM COET
Amravati, India

Prof P.L. Ramteke[2]
B.E. and M.E. in CSE
Sipna College of Engg and Technology
Amravati, India

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 Vindication 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.***

Keywords: Mobile ad hoc networks (MANETs); certificate revocation; cluster; security; threshold.

I. 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, and 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 disrupt network security, is a primary concern. [8] 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 vulnerable 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.[9]

- *Internal Attacks*

In MANET, several different types of attacks that cause threat, due to their dynamic nature, each type of attack is different from another. Among them some are active and others are passive. Active attacks may be internal or external. The internal type of attacks launches attack inside of MANET, so it is dangerous when the node is considered as a trusted node at beginning .They directly leads to the attacks on nodes present in the network. It may broadcast wrong type of routing information to other nodes [3].

- *External Attacks*

External attacks try to cause congestion in the network, Denial of Services (DoS) [4].Some external attacks are modification attacks, dropping attacks, fabrication attacks and timing attacks.

Attacker directly threatens the availability and robustness of nodes. So, there is important issue to protect legitimate nodes from malicious nodes. This is achievable through the use of key management in which public key, secrete key is shared between the Certificate Authority (CA) and other nodes. CA signs certificates of nodes presents in the network. CA [5][6] plays an important role in enhancing the network security. It digitally signs a valid certificate for each node to ensure that nodes can communicate with each other in the network. In such type of network CA invalids the attacker certificate for keeping network secured. If there are much of accusers showing that it is an attacker, then attacker's certificate can be revoked. But, it is not possible to determine, is it accusations are false or true. So, there is needed to take it into account the issue of false accusations.

In this section, we enhances certificate revocation scheme. Network consisting of Certificate Authority, Cluster Heads and nodes.

- *Working of CA*

When CH want to join the network it request for the secret key to the CA ,then CA response secret key that is S2 mod N to the CH and after that CH joins the network by getting certificate. At the time of packet sending if any node is found as a malicious node then CA revokes the certificate of malicious node and also certificate recovery is done by CA.

- *Working of CH*

CA issues certificates to Cluster Members (CM) then CM discover CH after getting discover message from CM, CH responses hello discover message to CM. when there is need to send packets CH broadcasts R2 mod N to all CM and gives challenge to prove its identity. After accepting challenge it sends RS mod N to CH. If it is malicious node after referring ZKP algorithm then CH sends attack detection message to CA.

- *Certificate Revocation and Recovery*

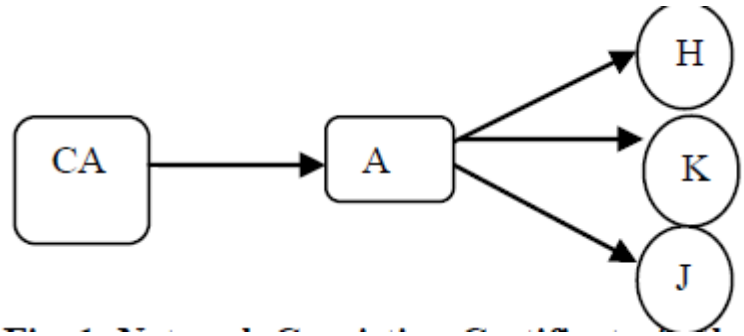

Fig.1 Network Consisting Certificate Authority and other normal nodes.

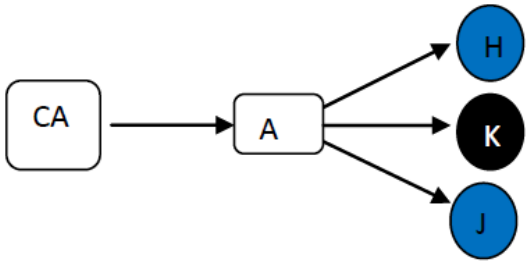

Fig.2 Certificate Revocation

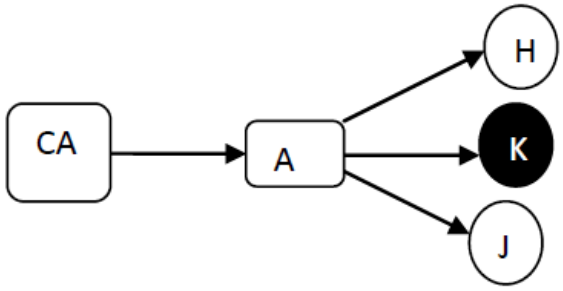

Fig.3 Certificate Recovery

Fig 2. and Fig 3. Shows examples of certificate revocation and recovery. Here CA Broadcasts messages to all nodes. In Fig 1 A, H.K, J are found as normal nodes. But in Fig 2 node K launches attacks on H,J that is detected by both of nodes H,J.So,H,J are placed into Warn List and malicious node K is placed into Block List, by which certificate revocation of malicious node K is done. At last nodes H and J are released from Warn List and placed into White List, due to which normal nodes are increased. Here certificate revocation scheme is enhanced that is described. The false accusers are detected and placed into Block List and normal nodes are released from Warn List.

II. Literature Review and Related Work

In URSA [1], two neighboring nodes receive their certificates from each other and also exchange 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 suspected node can be revoked when the number of accusations against the node exceeds a certain threshold. While URSA does not require any special equipment such as Certificate Authorities (CA), the operational cost is still high.

Recently, researchers pay much attention to MANET security issues. It is difficult to 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. 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.

The main disadvantages of non-voting-based method are slow decision process to satisfy the condition of certificate revocation and also it sustains heavy communications overhead to exchange the accusation information for each other. Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme is proposed [2], [3]. In this, clustering plays a major role, where the cluster head is to detecting the falsely accused nodes within its cluster and regaining their certificates to solve the issue of false accusation. CCRVC achieves immediate revocation and lowering overhead as compared to the voting-based scheme and when compared to the non-voting-based scheme improves the reliability and accuracy.

Several different types of certificate revocation techniques have been developed for mobile ad hoc networks. The most popular method is a simple certificate control approach by using a Certificate Revocation List (CRL) [2] which is managed by a single CA or shared among multiple CAs. A digital certificate which is valid for a certain time period is assigned to each node by the CA. The CA revokes the certificates of suspicious nodes and adds them to the CRL.

Nodes can be accused by any node with a valid certificate and the updated CRL is broadcasted throughout the entire network. URSA proposed by H. Luo et al. [3] uses certified tickets which are locally managed in the network to evict nodes. URSA does not use a third-party trust system such as a CA. The tickets of the newly joining nodes are issued by their neighbors. Since there is no centralized authority, the ticket of a malicious node is revoked by the vote of its neighbors. In URSA, each node performs one-hop monitoring, and exchanges monitoring information with its neighbours which allow for malicious nodes to be identified. When the number of votes exceeds a certain threshold, the ticket of the accused node will be successfully revoked. Since nodes cannot communicate with other nodes without valid tickets, revoking a node's ticket implies the isolation of that node. Although URSA is robust for false accusation attacks, there is still a remaining issue in coping with collusion attacks by multiple malicious attackers. The scheme proposed by G.

Arboit et al. [4], referred to as the voting-based scheme, allows all nodes in the network to vote. As with URSA, no CA exists in the network, and instead each node monitors the behavior of its neighbours. The primary difference from URSA is that nodes vote with variable weight. The weight is calculated from a node's reliability which is derived from its past behaviour. The higher its reliability is, the greater its weight will be. The certificate of a suspicious node can be revoked when the sum of the weights of the votes against the node reaches or exceeds a predefined threshold. By doing so, the accuracy of certificate revocation can be improved. However, since all nodes are required to participate during every vote, the communication overhead required to exchange voting information is quite high, thus increasing the time needed to revoke the certificate .J. Clulow et al. [5] proposed the decentralized Suicide based approach. In this approach, while the certificate revocation can be quickly completed with just an accusation, not only the certificate of the accused node but also accuser's certificate is revoked. In other words, at least one node has to sacrifice itself to remove an attacker from the network. This strategy dramatically reduces both the time required to evict a node and the communication overhead of the certificate revocation procedures. However, owing to its suicide-based strategy, the application of this approach is limited. Also, the scheme does not provide a mechanism to differentiate falsely accused legitimate nodes from properly accused malicious nodes.

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

A. 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. URSA [14] proposed by Luo et al. uses a voting-based mechanism to evict 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.

In URSA, 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. Determining 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. Another critical issue is that URSA does not address false accusations from malicious nodes.

The scheme proposed by Arboit et al. [9] allows all nodes in the network to vote together. As with URSA, no Certification Authority (CA) exists in the network, and instead 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 accusations 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 revoked when the weighted sum from voters against the node exceeds a predefined threshold. 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.

B. 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 Clulow et al. [8] proposed a fully distributed "suicide for the common good" 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. As a consequence, the accuracy is degraded.

Park et al. 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 blacklist (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 blacklist by its cluster head (CH). It takes a short time to complete the process of handling the certificate revocation.

III. Model of the Cluster Based Scheme

In this section, we introduce the model of 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 blacklist, 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 the network. On the other hand, we focus on the procedure of certificate revocation once a malicious attacker has been identified, rather than the attack detection mechanism itself. Each node is able to detect its neighboring attack nodes which are within one-hop away [8].

A. *Cluster Construction*

We present the cluster-based [2] 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.

While a node takes part in the network, it is allowed to declare itself as a CH with a probability of R. Note that neighbor sensing protocols, such as periodical broadcast of hello messages, are effective approaches used in routing protocols to check the availability of links between neighboring nodes. A new link is detected if a node receives a new hello message. Otherwise, the link is considered disconnected if none of the hello messages is received from the neighboring node during a time period.

In this model, if a node proclaims itself as a CH, it propagates a CH Hello Packet (CHP) to notify neighboring nodes periodically. The nodes that are in this CH's transmission range can accept the packet to participate in this cluster as cluster members. On the other hand, when a node is deemed to be a CM, it has to wait for CHP. Upon receiving CHP, the CM replies

with a CM Hello Packet (CMP) to set up connection with the CH. Afterward, the CM will join this cluster; meanwhile, CH and CM keep in touch with each other by sending CHP and CMP in the time period Tu.

We note that each CM is assumed to belong to two different clusters in order to provide robustness against changes in topology. In case a CM moves out of the transmission range of its CH, it has to search for other CHP to participate in a new cluster. Especially, if the node does not receive any CHP for a certain period of time 2Tu, namely, there is no CH within its one-hop range, it will declare itself as a CH and propagate CHP to form a new cluster. On the other hand, in case a CH has no CM in its neighborhood range, but if there are other CHs in its neighborhood, this node assigns itself as a CM to communicate with two of the CHs.

B. *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 Blacklist, 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. This will be detailed in the threshold mechanism described in Section 4. 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.

C. *Reliability-Based Node Classification*

According to the behavior of nodes in the network, three types of nodes are classified according to their behaviors: legitimate, malicious, and attacker nodes. A legitimate 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 legitimate 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 or a CM. Moreover, we should note that normal nodes consist of legitimate nodes and potential malicious nodes. Nodes that are listed in the warning list are deemed as warned nodes with low reliability. Warned nodes are considered suspicious because the warning list contains a mixture of legitimate nodes and a few malicious nodes (see Section 3.2). Warned nodes are permitted to communicate with their neighbors with some restrictions, e.g., they are unable to accuse neighbors any more, in order to avoid further abuse of accusation by malicious nodes.

IV. EVALUATION

In this section, simulation results for our method proposed. For this results, Java language is used,50 normal nodes are used,10-50 malicious nodes are used.

A. Impact of mobility

To evaluate the detection performance of the scheme, we studied the mobility on the detection time. Fig 4. shows the detection time as the mobility changes. In this simulation threshold is equal to 2 is used and mobility is set to be 1m/s,2m/s,5m/s and 10m/s .From this results, the detection time reduces as the node mobility increases.

B. Impact of Threshold

The simulation measures the impact of the threshold value on the detection performance.Here threshold values are considered as 5,10,15 having constant movement at 10m/s in the mobile network. As shown in Fig 5,when threshold becomes large, the detection time increases,

C. The detection performance

Fig 3. Shows comparative results of previous method in which nodes in Warn List are not released versus our method. For this result we have taken 20 normal nodes and malicious nodes are changes as 5,10,15,10.As number of malicious nodes are increases detection time varies fastly in previous method but there is just slight change in detection time of our method , also whatever the nodes present in Warn List are released after certificate revocation of malicious node.

V. 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 vindication 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 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.

Particularly, we have proposed a new incentive method to release and restore the legitimate nodes, and to improve the number of available normal nodes in the network. In doing so, we have sufficient nodes to ensure the efficiency of quick revocation. 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 malicious 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. 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.
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 Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002.
6. 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.

7. 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.
8. 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.
9. 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.

AUTHOR(S) PROFILE

Ruchita H. Bajaj received the B.E degree in CSE stream at H.V.P.M College of Engineering and Technology in 2012. And pursuing M.E degree in CS&IT stream H.V.P.M College of Engineering and Technology, Amravati. Area of Interest is Cloud Computing.

Prof. P. L. Ramteke received the B.E and M.E. degree in CSE stream at Govt. College of Engineering and Technology. He is member of various Technical Institutions of India like ISTE, IEI and IAPT, published various research papers in International Journals.