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, February 2014

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

On 10th & 11th February Organized by

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

# Integral Component CCRVC Scheme for Enhancing Security in MANET

Mr.S.Herman Jeeva[1], Mr.D.Saravanan[2]

PG Scholar, Dept. of CSE, Pavendar Bharathidasan College of Engg and Tech, Tiruchirappalli, India[1]
Associate Professor, Dept. of CSE, Pavendar Bharathidasan College of Engg and Tech, Tiruchirappalli, India[2]

**Abstract— Mobile Adhoc Networks (MANETs) is the open network environment where nodes can join and leave the network freely. Therefore, the wireless and dynamic natures of MANETs is not secure than the wired networks. To overcome this problem, the Cluster-based Certificate Revocation is proposed with Vindication Capability (CCRVC) scheme. Each cluster consists of a Cluster Head along with some Cluster Members (CMs) located within the transmission range of their cluster Head. Before nodes join the network, they have to acquire valid certificates from the Certification Authority (CA) that is responsible for distribution and management of certificates to all nodes. The CA is also responsible of updating two lists, Warning list and Black list, which are used to hold the accusing and accused nodes information, respectively. Experimental results show that the proposed scheme is effective and efficient to provide secure communication.**

**Keywords— Mobile ad hoc networks (MANETs), certificate revocation, and security.**

## I. INTRODUCTION

In MANETs, certificate management is a widely used mechanism which serves as a means of conveying trust in a public key infrastructure [12], 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 [14], attack detection [2], [6] and certificate revocation [1]. Certification is a prerequisite 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 Adhoc 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 al l its activities immediately. In research, the fundamental security problem of certificate revocation is focused to provide secure communications in MANETs.

A Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme is proposed to the performance of MANET. The cluster-based architecture is presented 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 (certification authority), is deployed in the cluster-based scheme to enable each mobile node to preload the certificate, which is responsible for distributing and managing certificates of all nodes, so that nodes can communicate with each other unrestrainedly in a MANET. 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.

Voting-based mechanism is defined as the means of revoking a malicious attacker's certificate through votes from valid neighboring nodes. URSA [9] 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. [1] 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.

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. [4] 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. [10] 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.

The advantages and disadvantages between voting-based and non-voting-based mechanisms. 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 is slow. 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.

It is able to drastically simplify the decision-making process for rapid certificate revocation as well as reduce the communications overhead. 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. The significant performance emphasize the difference between voting-based and non-voting-based methods: the former achieves higher accuracy in judging a suspicious node, but takes a longer time, the latter can significantly expedite the revocation process. Cluster-based Certificate Revocation is proposed with Vindication Capability (CCRVC) scheme. Like the previously proposed cluster-based schemes [10], [8] clustering is incorporated in the proposed scheme, where the cluster head plays an important role in detecting the falsely accused nodes within its cluster and recovering their certificates to solve the issue of false accusation.

On the other hand, CCRVC inherits the merits of both the voting-based and non-voting-based schemes, in achieving prompt revocation and lowering overhead as compared to the voting-based scheme, improving the reliability and accuracy as compared to the non-voting-based scheme.

## II. THE PROBLEM

Since Wireless Adhoc network is self configured network, attackers cannot be easily identified. For enhancing network security various revocation techniques have been used. There are two types of mechanisms for certificate revocation, voting based mechanism and non-voting mechanism.

*Voting based mechanism*

In URSA, each node performs one-hop monitoring, and exchanges monitoring information with its neighboring nodes. Each node will be maintaining a predefined number as a threshold for getting negative votes. When the number of negative votes for a node exceeds the threshold value, the certificate of accused node will get revoked.

Then, the node will get isolated from network activities. However, when threshold value is assigned larger, then the accused node will be communicating with other nodes in network. Another risk is that, false accusation from malicious node is not addressed.

Arboit et al.[15] proposed that voting varies with the weights. The weight of a node is based on its reliability and trustworthiness, which is derived from its past behaviors. When the weighted sum from voters against the node exceeds a predefined threshold then the certificate will get revoked. All nodes are required to participate in each voting. By doing so, the accuracy of certificate revocation can be improved and communication overhead will be high.

*Non-voting based mechanism*

In "suicide for the common good" strategy, where certificate revocation can be quickly completed by only one accusation i.e., the certificates both the accused node and accusing node will be revoked simultaneously. This reduces both the time required to evict a node and communications overhead of the certificate revocation procedure. But the accuracy is degraded.

## III. CONTRIBUTION

Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme is proposed. In that, Cluster head plays an important role in detecting the falsely accused nodes within its cluster and recovering their certificates to solve the issue of false accusation.

On the other hand, CCRVC inherits the merits of both the voting-based and non-voting-based schemes, in achieving prompt revocation and lowering overhead as compared to the voting-based scheme, improving the reliability and accuracy as compared to the non-voting-based scheme. Cluster-based revocation scheme revokes 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. Here, the focus is 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.

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.

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.

Based on their reliability nodes are classified as normal node, warned node, and revoked node.

*Normal 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.

*Warned Node:* 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.

*Revoked Node*: The accused nodes that are held in the blacklist are regarded as revoked nodes with little reliability. Revoked nodes are considered as malicious attackers deprived of their certificates and evicted from the network.

## IV. SYSTEM DESIGN

The system design involves the different steps involved in the proposed Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme. The entire process is summarized in the Fig.2 which gives a clear cut idea about the proposed method.

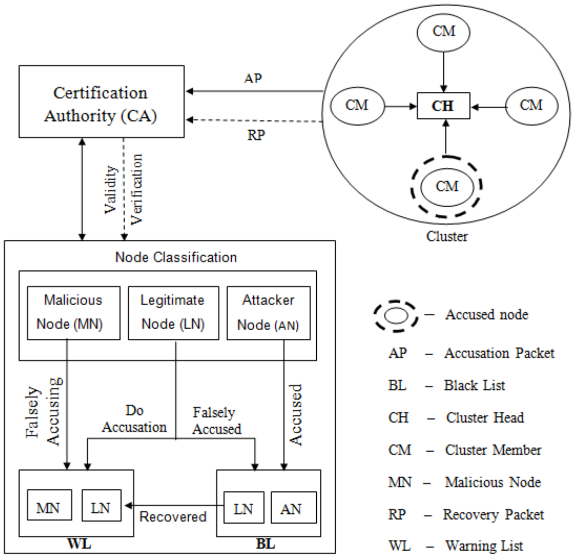

Fig. 1. System Architecture

Process:

When the neighboring nodes detect attacks from any one node then each of the nodes sends out an accusation packet to the certificate authority (CA) against attacker node.

According to the first received packet, the CA holds neighboring node and attacker node in the Warning List (WL) and Black List (BL)., respectively, after verifying the validity of neighboring node the CA disseminates the revocation message to all nodes in the network.

After receiving the revocation message nodes update their local WL and BL to revoke attacker's certificate. Meanwhile, CH updates their WL and BL and determines that one of the nodes was framed. Then some of the nodes send recovery packet to the CA to revive the falsely accused node.

Upon receiving the first recovery packet, the CA removes the falsely accused node from the BL and holds both the falsely accused node and normal node in the WL and then disseminates the information to all the nodes. At last the nodes update their WL and BL to recover the falsely accused node.

## V. SYSTEM IMPLEMENTATION

### Simulation of AODV Protocol

Creation of nodes and transmission of packets between those nodes is done using Normal Network with AODV protocol. The parameters such as end to end delay, throughput, packet delivery ratio, energy spent are calculated.

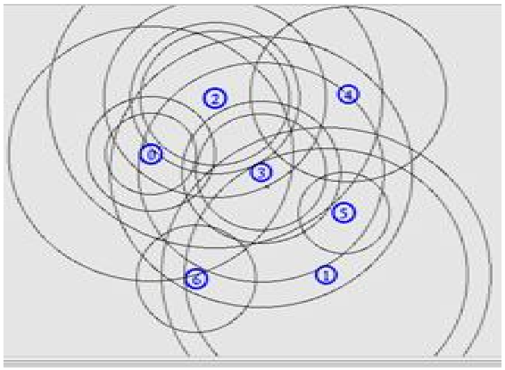

Fig. 2. Creation of nodes

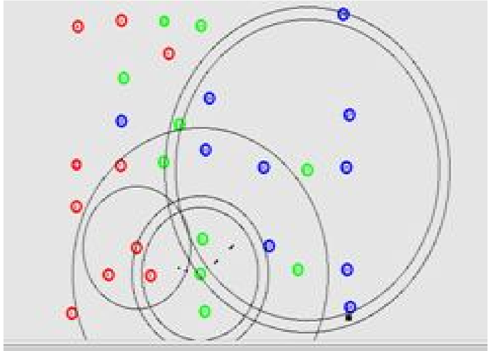

Fig. 3. Transmission of packets using AODV protocol

### Simulation of DoS Attack

DoS Attack is implemented, during packet transmission, which shows the performance degradation. And also parameters such as end to end delay, throughput, packet delivery ratio, energy spent are calculated.

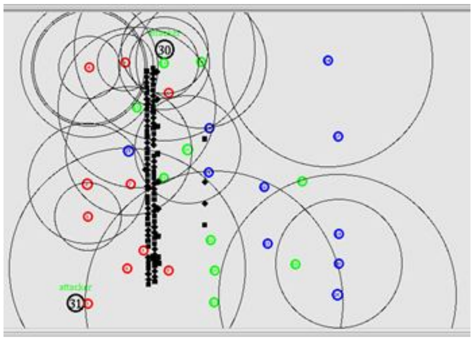

Fig. 4. Dropping of packets

Simulation of CCRVC Scheme

Transmission of packets between the nodes is done using proposed Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme to avoid attack and to increase network performance. The parameters such as end to end delay, throughput, packet delivery ratio, energy spent are calculated.

Result Analysis

Comparison between AODV, ATTACK and CCRVC is done on various parameters.

## VI. CONCLUSION AND FUTURE ENHANCEMENT

A major issue, certificate revocation of attacker nodes is addressed, which in turn ensures a secure communications in MANET. Cluster-based certificate revocation with vindication capability scheme is a combination of merits of both voting-based and non-voting based mechanisms, which revokes malicious certificate and solves the problem of false accusation. In this scheme the revocation time is reduced as compared to the voting-based mechanism. In addition, the cluster-based model is adopted to restore falsely accused nodes by the CH, which improves the accuracy as compared to the non-voting based Mechanism.

A new incentive method is used to release and restore the legitimate nodes, and to improve the number of available normal nodes in the network for ensuring the efficiency of quick revocation. Thus the 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] Arboit G., Crepeau C., Davis C.R. and Maheswaran M. (2008) "A Localized Certificate Revocation Scheme for Mobile Adhoc Networks," Adhoc Network, vol. 6, no. 1, pp. 17-31.

[2] Bounpadith Kannhavong, Hidehisa Nakayama,Yoshiaki Nemoto, and Nei Kato. (2007) "A survey of routing attacks in mobile Adhoc networks".

3] Camp T., Boleng J. and Davies. (2002) "The survey of mobility models for Adhoc network research," Wireless Communication and Mobile Computing, vol.2, no. 5, pp. 483-502.

[4] Clulow J. and Moore T. (2006) "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.

[5] Hegland A.M., Winjum E., Rong C. and Spilling P. (2006) "A survey of key management in Adhoc networks," IEEE Communications Surveys and Tutorials, vol 8, no. 3, pp. 48-66.

[6] Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour, Yoshiaki Nemoto and Nei Kato. (2009) "A Dynamic Anomaly Detection Scheme for AODV- Based Mobile Adhoc Networks".

[7] Jie Lian, Kshirasagar Naik, Gordon B. and Agnew. (2004) "A Framework for Evaluating the Performance of Cluster Algorithms for Hierarchical Networks".

[8] Liu W., Nishiyama H., Ansari N. and Kato N. (2011) "A Study on Certificate Revocation in Mobile Adhoc Network," Proc. IEEE Int'l Conf. Comm. (ICC).

[9] Luo J., Kong P., Zerfos S., Lu and Zhang L. (2004) "URSA: Ubiquitous and Robust Access Control for Mobile Adhoc Networks," IEEE / ACM Trans. Networking, vol. 12, no. 6, pp. 1049-1063.

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

[11] Sakarindr P. and Ansari N. (2007) "Security services in group communications over wireless infrastructure, mobile Adhoc, and wireless sensor networks," IEEE Wireless Communications, 14(5), pp. 8-20.

[12] Yang H., Luo H., Ye F., Lu S. and Zhang L. (2004) "Security in mobile adhoc networks: challenges and solutions," IEEE Wireless Communications,11(1), pp. 38-47.

[13] Yang H., Shu J., Meng X. and Lu S. (2006) "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 261-273.

[14] Zhou L., Cchneider B. and Van Renesse R. (2002) "COCA: A Secure Distributed Online Certification Authority," ACM Transactions on Computer Systems, Vol.20, No.4, pp.329-368.

[15] Zhou L. and Haas Z. J. (1999) "Securing Adhoc networks," IEEE Network Magazine, pp. 24-30.