Indian Journal of Communication Engineering and Systems (IJCES)
Vol.2.No.2 2014 pp 66-70.
Available at: www.goniv.com
Paper Received: 04-04-2014
Paper Accepted: 14-04-2014
Paper Reviewed by: 1. R. Venkatakrishnan 2. R. Marimuthu
Editor: Prof. P.Muthukumar

# TRUSTED CBCR SCHEME TO ENHANCE THE PERFORMANCE AND SECURITY IN MANET

**Mr. K. C. Prabu Shankar, V. Nesamalar**
Dept. of Information Technology.
St. Joseph's College of Engg. & Technology,
A. S. Nagar, Elupatti - Thanjavur, India.
kcprabushankar@gmail.com, nesam28@gmail.com

## ABSTRACT

The Mobile ad hoc networks (MANET) is a self-organized infrastructure less networks when compared to wired networks. The main challenge is to provide secure network services. Certificate revocation process provides secure network communications. The Certificate Authority (CA) issue certificates to all nodes. The certificates can be revoked from attackers and cut off from further network activities. The proposed cluster based certificate revocation with vindication capability (CCRVC) scheme can be used for quick and accurate certificate revocation. The falsely accused nodes are revoked to improve the reliability of the scheme. The threshold based mechanism is proposed to enhance the accuracy. This certificate revocation scheme is more effective and efficient to provide secure communications.

**Index Terms -** Warning list; Black list; Cluster member; Cluster head; Certificate revocation; Ubiquitous and Robust Access Control (URSA)

## I. INTRODUCTION

Mobile Ad Hoc Networks (MANET) is dynamic in nature consisting of cell phones, laptops, this can freely move in the network. MANET is used in various applications such as military, emergency communications and other real time applications by forward packets in limited transmission range. Security is an important requirement for network services. Implementing security [3], [4] protects networks against malicious nodes; the attacker can launch attack in network. Therefore, the MANET having more security attacks than wired networks. The certificate management scheme can be used for secure application which gives trusted public key infrastructure [5], [6]. It encompasses three components namely prevention, detection and revocation. Certificate Revocation [13], [14], [15], [16], [17], [18], [19] plays an important role in MANET. The certificates of the misbehaving nodes should be removed and immediately stopped from accessing the network.

## II. RELATED WORK

In a MANET, it is difficult to secure ad hoc networks because of limited protection, vulnerable attacks and dynamically changing networks. A different type of techniques has been proposed to improve network security. This section introduces existing approaches of certificate revocation such as voting-based mechanism and non-voting based mechanism.

### *A. Voting-Based Mechanism*

Voting-based mechanism means revoking certificates from malicious nodes with the help of neighboring nodes. The new nodes are getting certificates from neighbors. The attacker node certificates can be revoked basis on the neighbor's nodes votes. In URSA [16], every node performs one hop monitoring and exchanges that information with other neighbor nodes. When the number of negative votes exceeds, the certificates can be revoked from accused node and it cannot participate in network activities. The main thing is the node cannot communicate with others without having valid certificates. The drawback is it does not address false accusation from attacker nodes. In URSA, no certificate authority (CA) exists in the network, instead each node monitors the behavior of its neighbor nodes. The proposed system allows all nodes to vote together. The main difference from URSA is that nodes vote with variable weights in terms of reliability and trustworthiness. Based upon the neighbors vote, the certificate can be revoked from the accused node. Therefore, the accuracy can be improved and exchange of voting information is also high.

### *B. Non-Voting Based Mechanism*

In non-voting based mechanism [17], a cluster based certificate revocation scheme has been suggested. Here the nodes are coordinated and formed as clusters. This scheme maintains the Warning list and Black list which contains accuser node and accused node. The certificate authority (CA) maintains the control messages. It is responsible for issuing certificates to all nodes and revokes the certificates from accusation nodes. It removes the falsely accused nodes from the black list by its cluster head (CH). Therefore it takes minimum time for certificate revocation.

## III. CLUSTER-BASED SCHEME

This section introduces the proposed cluster-based revocation scheme, which can quickly revoke attacker nodes from neighboring node. This scheme maintains warning list and black list, in order to protect legitimate nodes from malicious nodes. Using the cluster head, falsely accused nodes are revoked. This scheme addresses only the issue of certificate revocation and does not address certificate distribution [7], [8].

### *A. Cluster Construction*

To construct the topology, the cluster based architecture is implemented. Here the nodes are combined to form a cluster. Each cluster consist cluster head (CH) with cluster members (CM). They are located in certain transmission range of CH. The certificate authority issues certificates to all nodes. After getting the certificate the nodes can join the network. The certificate authority is responsible for both distributing and managing certificates. The neighboring nodes often check the availability of the nodes using neighbor sensing protocols. It broadcasts a hello message and then it assumes that a new link is added to the network. If it does not receive a hello message within a certain period of time, it assumes that the node is disconnected from the network. The cluster head (CH) distributes CH Hello Packet (CHP) to neighboring nodes periodically. The CHP packet reaches to all the cluster members (CM) within their transmission range. If a new cluster member wants to join in that cluster, it accepts the CHP packets from the CH. Then the CM replies to the CH by sending CM Hello Packet (CMP). Afterward the cluster head will accept the CMP and it will join the cluster. The CH and CM make ensure the communication by sending CHP and CMP.

### *B. Certification Authority*

A trusted third party is said to be a certification authority, which can be used to provide the certificates for new nodes and revoking the certificates from the attacker nodes. The CA is responsible for maintaining WL and BL, which holds accusing and accused node respectively. The BL holds the accused nodes as an attacker and WL holds the corresponding accused node. The CA updates the two lists and it broadcasts that list to the whole network. After that malicious nodes can be identified easily and isolated from further network activities.

## IV. THRESHOLD–BASED MECHANISM

Conventional voting mechanisms set the threshold value K as a constant. This mechanism is mainly proposed to find whether the warned nodes are legitimate nodes or not. The constant value K has to be set. If the threshold value is set too big, it will take a long time to find that the warned node is a legitimate node because the method has to wait for more accusations to reach the verdict. If the threshold value is set too small, revoked malicious nodes can be released by other malicious nodes from the WL. To overcome these problems, optimum threshold value K is proposed based on the neighboring nodes.

## V. NODE CLASSIFICATION

Based on their behavior, the nodes can be classified as legitimate node, malicious node and attacker node. A node having valid certificates does not launch any attacks that is said to be legitimate node and it have secure communications. If a node not having valid certificates accesses the network with the help of any legitimate node then it is said to be a malicious node. If a node can launch attack and disrupt network communications then it is an attacker node. Further, the nodes can be categorized as normal node, warned node and revoked node. The normal node does not launch any attacks and it has high reliability, also it has the ability to accuse other nodes. The low reliability nodes are warned nodes that are placed in the warning list. The warning list contains a mixture of legitimate nodes and malicious nodes. The accused nodes are placed in BL that is said to be revoked nodes.

### *A. Certificate Revocation*

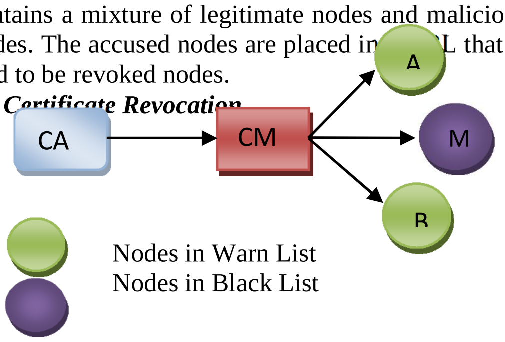

**Fig 1: Certificate Revocation**

In certificate revocation process, three stages are implemented namely accusing, verifying and notifying to revoke a malicious attacker's certificate. The nodes can be identified by neighboring nodes. The CA is responsible for maintaining the BL and WL and broadcast that list to all cluster members. The CM updates that two lists and check malicious nodes availability. It checks the local BL to match with any node. If it detects any detect any attacker node, its send an Accusation Packet (AP) to CA. The CA verifies the certificate validation of the accusing node. If it confirms then it put that node in to BL and revoked that node successfully. In between time, that malicious node is put in to WL. The CA updates the WL and BL and propagates that list to whole network.

### *B. Recovering false accusation*

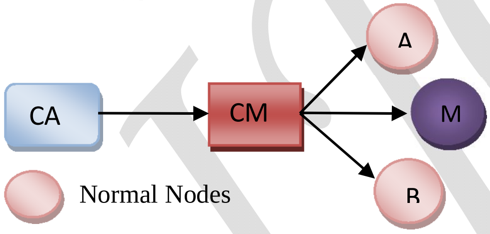

**Fig 2: Certificate Recovery**

Sometimes the legitimate node may address as an malicious node and the CA put that node in to BL and disseminates to all CH and CM. The CH is responsible for detecting false accusation node against legitimate node and restores that node within its cluster. CH can detect attacks from CM then and revoked it. If the legitimate node is identified as malicious node that will be added to the BL and propagates to all nodes. The CH updates and detects any node as falsely accused, it send a Recovery Packet (RP) to the CA. The CA validates that recovery packet and restores that node in to cluster and updates the BL.

## VI. PERFORMANCE EVALUATION

This section discusses the simulation results using Qualnet4.0 network simulator. The simulation helps to improve the performance of the scheme in terms of efficiency. In particular, the proposed scheme is simulated to verify its efficiency in revoking attacker nodes.

### *A. Simulation Setup*

Many devices (mobile phones, laptops, PDA) can be used to construct a MANET in a particular area. These devices are randomly moved and communicate with neighboring nodes. A MANET is simulated with 50-100 normal nodes in Qualnet4.0 simulator and ad hoc on-demand distance vector (AODV) is used as an IP routing protocol. The node movements are followed by random way-point mobility pattern, in which each node moves to a randomly selected location at different velocities from 1 to 10m/s. The simulation parameters are shown in Table 1. The transmission range is set to be 250m. An attacker node periodically launches attacks every 5 seconds that can be detected by other nodes.

### *B. Simulation Results*

*i) The detection performance*

Here, the detection performance is analyzed to verify the efficiency of the method. Fig. 3 shows comparative results of previous method versus our method. This simulation shows that detection time gets reduced. For simulation, 60 normal nodes are considered.

**TABLE 1**
**SIMULATION PARAMETERS**

| Parameter | Value |
|---|---|
| Number of nodes | 50-100 |
| Node Placement | Random |
| Node transmission range | 250m |
| Mobility model | Random-Waypoint |
| Node speed | 1-10m/s |
| Simulation time | 500s |
| Routing protocol | AODV |

The malicious nodes are changes as 15,30,45,60. The detection time is simulated and it was reduced by the new method. As the number of malicious nodes increases detection time varies between previous method and the proposed method. The detection time is reduced fast compared with the previous method. Also falsely accused nodes are released from WL after certificate revocation.

ii) Impact of mobility

To evaluate the detection performance of the scheme, the impact of mobility on the detection is studied. Here the mobility changes are simulated in MANET. Fig. 4 shows the detection time as the node mobility changes. Here the threshold value is equal to 2 and mobility is set to be 1m/s, 2m/s, 5m/s, 10m/s. The results show that the detection time decreases as the node mobility increases.

*iii) Security analysis*

In the proposed scheme, a CH can recover the falsely accused node certificate from black list and revoking the malicious node certificate by certificate revocation process and it never access the network further so the mobile network allowing only authenticated nodes and get secured. Here simulate the users get communicated with full security. To enhance the security, threshold-based mechanism is used. Here the threshold value is considered as 5, 10, and 15 having constant movement in mobile network. When threshold becomes large, the detection time increases. Fig. 5 shows that all users having full security in mobile network.

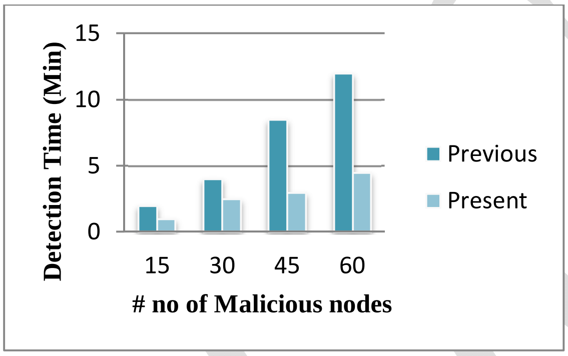

Fig. 3 Previous method versus our method

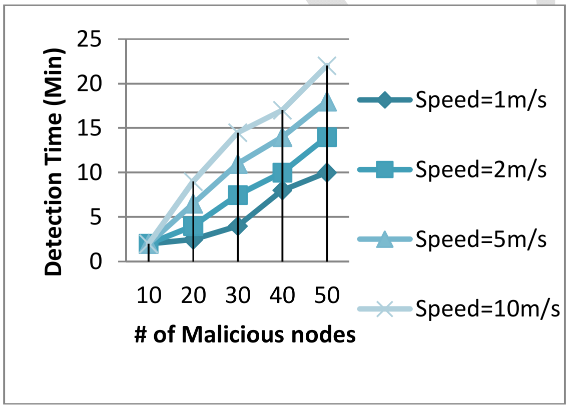

Fig. 4 Impact of mobility

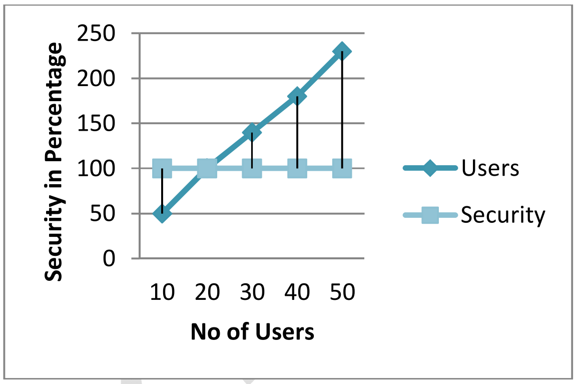

Fig. 5 Impact of security

## VI. CONCLUSION

This paper focuses on the secure network communication in MANET. Certificate revocation process ensures that the communication is secure. The proposed CCRVC scheme can be used to revoke the malicious certificate and restore false accusation node. The revocation time is reduced by single node accusation and improving the accuracy by restores the falsely accused node using CH. Therefore this scheme increases the normal node in MANET. To enhance the accuracy threshold-based mechanism is used.

## REFERENCES

[1] T. R. Panke and B.M.Patil "Improved Certificate Revocation method in Mobile ad hoc network" International Journal of Computer applications (0975 – 8887) Volume 80 – No 12, October 2013).

[2] Wei Liu, Hiroki Nishiyama, Nirwan Ansari and Nei Kato "A Study on Certificate Revocation in Mobile Ad Hoc Networks"

[3] 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, Feb. 2004.

[4] 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, Oct. 2007.

[5] 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, 3rd Quarter 2006.

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

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

[8] 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, July 2005.

[9] 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, Apr. 2005.

[10] 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, Oct. 2007.

[11] 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, June 2009.

[12] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Network: Analysis & Defenses," Proc. Third Int'l Symp. Information Processing in Sensor Networks, 2004.

[13] S. Micali, "Efficient Certificate Revocation," Massachusetts Inst. Of Technology, Cambridge, MA, 1996.

[14] C. Gentry, "Certificate-Based Encryption and the Certificate Revocation Problem," EUROCRYPT: Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques, 2003.

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

[16] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks," IEEE/ACM Trans. Networking, vol. 12, no. 6, Oct. 2004.

[17] G. Arboit, C. Crepeau, C.R. Davis, and M. Maheswaran, "A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks," Ad Hoc Network, vol. 6, no. 1, Jan. 2008.

[18] 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, July 2006.

[19] C. Bettstetter, G. Resta, and P. Santi, "The Node Distribution of the Random Waypoint Mobility Model for Wireless Ad Hoc Networks,"IEEE Trans. Mobile Computing, vol. 2, no. 3, July-Sept. 2003.

[20] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," Wireless Comm. and Mobile Computing (WCMC) Special Issue on Mobile Ad Hoc Networking: Research, Trends, and Applications, vol. 2, no. 5,2002.