An Improved Approach for MANET Security using Cluster Based Certificate Revocation

Gayathri Mohan[1], Renjana Ramachandran[2]

[1]*Student, Dept. of Computer Science and Engineering,*
Mangalam College of Engineering, Ettumanoor, Kerala, India.

[2]*Assistant Professor, Dept. of Computer Science and Engineering,*
Mangalam College of Engineering, Ettumanoor, Kerala.

Abstract— **Mobile ad hoc networks (MANETs) got attention due to their frequent change in topology and easy deployment capability. Unlike other wireless networks, MANETs are more vulnerable to various types of security attacks. To guarantee secure network services is the major challenge associated with any MANET. In order to have secure network communications, one important action mostly being carried out is certificate revocation of malicious nodes inside the MANET. The proposed system uses an improved strategy while considering the false accusation against normal nodes. The proposed system maintains three important lists White List (WL), Intermediate List (IL) and Black List (BL) based on the communication among nodes within a certain transmission range. The Intermediate List (IL) is introduced in the proposed system to set a threshold before moving a node to Black List (BL). The proposed system in most cases is able to remove attackers from further participating in network activities. The results show that proposed system is able to give improved Delivery Probability than existing CCVRC scheme.**

Keywords*— *MANETs, Security Attacks, Certificate Revocation, Intermediate List(IL), CCVRC Scheme

I. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is a collection of several mobile nodes (devices) that communicate through wireless links with limited transmission range. Radio waves support the communication within MANET. There are directly communicating nodes which are in the same radio range and other nodes require the help of intermediate nodes to route their packets. There is no fixed infrastructure and MANETs are fully distributed. Fig.1 shows the example of a typical Mobile Ad-hoc network (MANET) with five nodes.

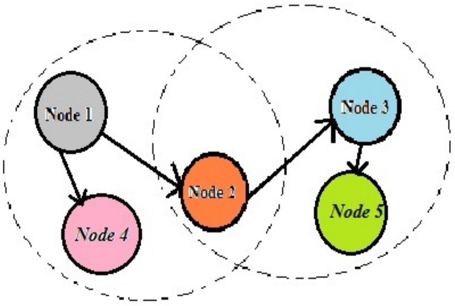


Fig.1 Example of a MANET

In Fig.1 Node1 and Node3 is not in the same range however they can communicate each other via Node2. Here Node2 acts as a router to forward packets between Node1 and Node3.

A. Characteristics of MANETs

a) Nodes are Mobile

All nodes within a MANET are free to move inside a reachable bandwidth and they are having routing capability to deliver packets to other nodes.

b) Rapidly Changing Network Topology

Network topology is highly dependent on the relative locations and connections between nodes in the network. Thus the resulting topology will be dynamic in nature.

c) Easily Deployable

The network deployment is very easy as the network topology is rapidly changing.

A MANET is a decentralized network in which all network activities like the finding the topology and delivery of messages are handled by the nodes themselves, i.e., the mobile nodes are associated with the task of routing packets. MANETs are more sensitive to various types of security attacks [6] [3] due to their frequently varying wireless nature. To guarantee secure network services is a major challenge associated with any MANET [7]. In order to have secure network communications, certificate revocation is an important task.

Certificate Revocation is a phase associated with Certificate Management which is a widely accepted method to provide trustworthy public key infrastructure [9] for both application security and network service security. In the process of certificate management the three phases needed are: prevent, detect and revocate.

Several works have been originated which suggests how to remove malicious attacks in the network. It is important that any attack should be identified as soon as possible.

Certificate revocation is a major task where listing and removing the certificates of nodes that have been detected to launch attacks on the neighbourhood, is done. A node should be removed from the network and cut off from all its activities immediately when it is found as misbehaved. [1]

This work focuses on false accusation among nodes and limiting the entry to Black List (BL) with a threshold value. It is expected that the proposed work can handle all the delicate attacks for MANETs and develop a good application prototype.

II. RELATED WORKS

Security is one of the major issues related to MANETs that requires attention. Due to sensitive wireless links, the dynamically changing topology, and the lack of infrastructure, there is difficulty in securing a MANET. There are various Certificate Revocation techniques exist in concern with ensuring security to MANETs. This section briefly describes some of the existing Certificate Revocation techniques.

A. Voting Based Mechanism

In voting-based mechanism it is possible only to revoke a framed attacker's certificate based on the votes from the normal nodes who are the neighbours of framed attacker node. In the scheme proposed by Arboit et al. [4] all nodes in the MANET can vote together. There is no central Certification Authority (CA) exists in the network, instead of CA each node is having the duty to monitor the behaviour of its neighbouring nodes. In this scheme the nodes in the network vote with different weights. The weight of a node is calculated in terms of reliability and trustworthiness that is derived from its past behaviours like acquisition of this node towards others as well as acquisition from other nodes against that node. Node having high weight is more reliable. When the weighted sum from voters against a node exceeds a predefined threshold then the certificate of an accused node is revoked. Thus the accuracy of certificate revocation can be improved. Since all nodes are required to participate in each voting, the communication overhead for voting information exchange is quite high, so revocation time also increases.

B. Non-Voting Based Mechanism

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. According to this strategy certificates of both the accused node and accusing node have to be revoked simultaneously. The suicidal approach limits the use of this scheme in applications, even though this approach reduces both the time required for removal of a node and for communication overhead. It fails to differentiate falsely accused nodes from genuine malicious attackers so that accuracy is degraded.

Park et al. [2] proposed a cluster-based certificate revocation scheme, in which the nodes are self-organized to form clusters. The scheme has a trusted Certification Authority (CA) who is responsible to manage control messages; CA can hold the accuser and accused node in the warning list (WL) and blacklist (BL), respectively.

Any single neighbouring node can revoke the certificate of a malicious node. 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 less mean time to complete the process of handling the certificate revocation.

C. Cluster Based Certificate Revocation

Cluster-based Certificate Revocation with Vindication Capability scheme (CCVRC) adopts the merits of both voting-based and non-voting based mechanisms and revoke malicious node's certificate and solve the problem of false accusation. An accused node can be revoked based on accusation details provided by a single node, and reduce the revocation time as compared to the voting-based mechanism. In addition, a cluster-based model is used to restore falsely accused [2] nodes by the CH, thus there is an improvement in accuracy when compared to the non-voting based mechanism.

The CCVRC scheme adopts a new method to release and restore the legitimate nodes, and to improve the number of available normal nodes in the network. But if there is a situation that any node is being framed by one or more nodes in the very beginning stage where the MANET is just created then the cluster head do not have any trusty details to inform the CA to release the framed node this makes the limitation of CCVRC scheme.[1]

III. PROPOSED SYSTEM

For a MANET every action like data transfer or even a topology change occurs within a transmission range. It is crucial to have secured transmission through every wireless links within the MANET. The proposed system provide an improvement to the existing CCVRC scheme by introducing a new withholding list known as Intermediate List(IL). Before getting into the acquisition maintenance let's peep into the overall strategy followed in proposed scheme.

A. C*luster Formation*

Before the entire MANET gets clustered into several clusters every node in the MANET should get authentication certificate issued by the Certification Authority (CA).

The several steps for cluster formation are:

Step 1: When a node joins the probability to declare itself as cluster head CH) is P.

Step 2: To check the presence of neighbouring nodes every node periodically broadcast Hello Messages, if others reply, a new link is formed.

Step 3: If there is no reply within a certain time period the link is broken and with a small time delay Step 2 starts again.

Step 4: If a node proclaims itself as a CH it sends CH Hello Packet (CHP) to know its neighbours within its transmission range.

Step 5: All nodes who receive CHP within the transmission range of CH send back Cluster Member Packet (CMP) to join with the CH.

Step 6: All nodes keep a touch with CH in time period Rt.

Step 7: Every node can be a member of different clusters to have a robust topology and when a CM moves out of the transmission range of its current CH and if it do not get any CHP within a time of 2 Rt, then it declare itself as a CH and sends CHP to form a new cluster. [1]

B. Trust Value for Every Communication

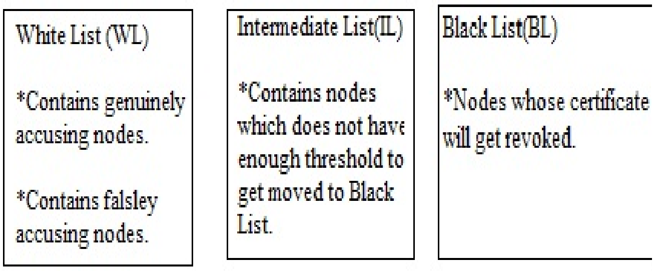
Step 1: The clustering algorithm should repeat at a specific time interval T.

Step 2: Every node should inform it's Cluster Head (CH) with a Trust Value (TV), every time when it is communicating with any other node. TV is the node's experience when it is communicating with other node. The

TV should be a value based on predefined threshold **p**. For example Node A communicates with Node F and there is an attack from Node H which will cause a decrease in the TV of F.
Step 3: CH notifies the TV of every node to CA periodically and in certain time interval CA broadcasts TV related information to every node in the network.
Step 4: If a node gets least TV for more than a predefined no. of times, is found as malicious node and CA broadcasts a message to everyone that the node is revoked.

C. *Functioning of Certification Authority*

The certification authority is a trusted third party; it is maintained in the cluster-based scheme so that each node will have a valid certificate. The CA can also update three lists, White List (WL), Intermediate List (IL) and Black List (BL). WL contains the detail of accusing nodes, IL contains the detail of nodes that got accused but not have enough votes to get moved to BL. BL contains the exact detail of nodes to get revoked.


White List (WL)

*Contains genuinely accusing nodes.

*Contains falsley accusing nodes.

Intermediate List(IL)

*Contains nodes which does not have enough threshold to get moved to Black List.

Black List(BL)

*Nodes whose certificate will get revoked.

Fig. 2 Lists maintained by CA.

D. *Need of Intermediate List (IL)*

IL is introduced in the proposed system to solve the problem associated with the BL maintenance in CCVRC scheme. It is not possible for a CH to claim that a node is trusty and not malicious if that node does not have any communication history. In order to get rid of the situation the proposed scheme maintains IL and every accused node with single accusation is put into the IL and if the accused node gets a predefined no. of accusations (set as threshold t) then only it is moved to BL. In necessary situations (When routing link cannot be made without a node in IL) the nodes in the IL can be a part of routing in the network.

E. *Certificate Revocation*

Steps for Revoking Malicious Certificate:
Step 1: When a node, for example - Node A claims and informs CA that Node F is malicious.
Step 2: CA puts Node A in WL and Node F in IL (initially).
Step 3: When votes against F exceeds threshold t then F is moved to BL.
Step 4: CA broadcasts the current status of WL, IL and BL to all nodes, on getting the broadcast message every node updates its WL, IL and BL.
Step 5: CA successfully revoke Node F's certificate.
Step 6: Until a node is in IL it can communicate in case of necessity.

IV. Experimental setup

We consider a simulated environment to construct a mobile ad hoc network. It simulates a realistic environment that there are many laptops, PDAs, Mobile phones etc. These devices move randomly and communicate with their neighboring devices in the network. All nodes are termed as a separate device in the MANET and transmission range is fixed to 250 m. The scheme uses AODV routing [10] and in every situation initially a link is possible by including the normal nodes only, if not possible, with an IL node if the link is feasible then that specific IL node can also be a part of routing. It is assumed that each node could move to a randomly selected location with different velocities from 1 to 10 m/s. The probability **P** that the newly joining node becomes a CH is 0.3. CH and CMs are sensing each other with Hello packets in every time interval Rt (set to 15s) by which the clustering algorithm runs and obtains new CH and CMs. The minimum Trust Value (TV) probability for a node is set to 0.4. The graph shows improvement in delivery probability when compared with existing CCVRC scheme, for no. of nodes from 50-100.

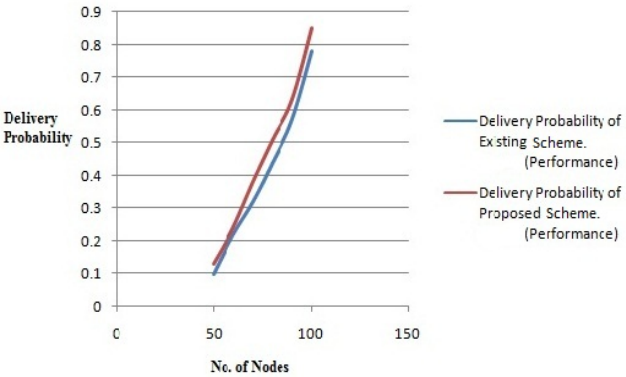


Fig. 3 Graph showing the Delivery Probability (comparison between Proposed Scheme and Existing Scheme).

V. Conclusion

The proposed system introduces extra security concern than the existing Certificate Revocation schemes with a good recoverability from false accusation. The proposed scheme improves the delivery probability by reducing the chance to get revoked through a false accusation.

Acknowledgment

We take this opportunity to thank all people who helped us for the study and preparation of this paper.

References

[1] K. Park, H. Nishiyama, N. Ansari,N. Kato and Jie Yang "*Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks*" IEEE Trans. on Parallel and Distributed Systems, vol. 24, no. 2, Feb. 2013.

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

[3] 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.

[4] 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, pp. 17-31, Jan. 2008.

[5] 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.

[6] 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.

[7] 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.

[8] 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, July 2006.

[9] 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.

[10] J. Kong, X. Hong, Y. Yi, J.-S. Park, J. Liu, and M. Gerla, "*A Secure Ad-Hoc Routing Approach Using Localized Self-Healing Communities*," Proc. Sixth ACM Int'l Symp. Mobile Ad hoc Networking and Computing, pp. 254-265, 2005.