IJCSE International Journal of Computer Science and Engineering Open Access
Research Paper Volume-2, Issue-1 E-ISSN: 2347-2693

Cluster Based Certificate Revocation of Attacker's Nodes in MANET

E.K. Neena[1*], C. Balakrishnan[2]

[1] *Department of computer science, S.A Engineering college, Chennai, India*, neenasathees@gmail.com
[2] *Department of computer science, S.A Engineering college, Chennai, India.*

www.ijcaonline.org

Received: 22/12/2013 Revised: 10/01/2014 Accepted: 18/01/2014 Published: 31/01/2014

***Abstract*—** Mobile ad hoc network (MANET) is a type of wireless ad hoc network. MANETs are very popular because of its infrastructure less network. Security is a major concern to provide protection between mobile nodes in hostile environment. Certificate revocation is one of the security components in mobile ad hoc networks (MANETs). Certificate revocation scheme, outperforms other techniques in terms of being able to quickly revoke attackers certificates and recover falsely accused certificates. The dynamic and wireless nature of mobile ad hoc network makes them more susceptible to many kinds of malicious attacks. Certificate revocation isolates the attackers from further participating in network activities. Certificates are issued and revoked by trusted party known as Certificate Authority. Certificate revocation invalidates the attacker's certificate which is essential in keeping the network more secured. Sometimes malicious node will try to remove legitimate nodes from the network by falsely accusing them as attackers. Therefore, the issue of false accusation must be taken into account in designing certificate revocation mechanisms. Clustering approach is able to quickly revoke certificates of accused nodes and also to explicitly distinguish false accusations. Here Warned nodes will also be involved in certificate revocation to make the scheme more efficient and reliable. Cluster based routing protocol is used for revocation of certificates that provides more security in mobile ad hoc network.

***Index Term*—** Certificate Revocation, Trusted Authority, Cluster Head, Regions.

I. INTRODUCTION

Mobile ad hoc network is vulnerable to many kinds of malicious attacks. Attacks on a wireless network can come from all directions and target at any node [1]. MANET is a self-configuring network without the help of a centralized infrastructure, often infeasible in critical mission applications like military conflict or emergency recovery. There is a rapid expansion in the field of mobile computing due to the available of inexpensive, wireless devices. Because of the dynamic nature, remote distribution and open medium of MANET make it vulnerable to various types of network attacks. In a wired network an adversary must gain a physical access to the network wires or pass through several lines of defense at firewalls and gateways. Mobile Ad hoc Network (MANET) is a collection of mobile nodes which consist of both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly [5]. Hence every node must be prepared for encounters with an adversary directly or indirectly. Mobile nodes and their infrastructure must be prepared to operate in a mode that trusts no peer. Here there is no well defined place where traffic monitoring or access control mechanisms can be deployed [1], [2]. 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 [3]. Security in mobile nodes must encompass these components such as prevention, detection and revocation for the certificate management. This Certification is considered as a prerequisite to secure network communications. Certificate revocation will enlist and remove the certificates of nodes that have been detected to launch attacks on the neighborhood [3]. Certificate revocation is a process that provides secure communications in MANET.

Corresponding Author: *E.K. Neena*

II. PRELIMINARIES

All the valid users are entered in the certificate revocation list (CRL). Trusted authority provides each user a unique public-key certificate if it is an authorized user. Trusted authority is a believable third party, under each trusted authority there will be many cluster heads available. The following sections describe user authentication scheme in detail, including the certificate generation, certificate update, and certificate verification.

A. Issue of Valid Certificate

User will be able to communicate with other members of same cluster or with the members of the other cluster only with the valid certificate. The user sends a request to trusted authority to issue the certificate. Only the trusted authority can issue the certificate to the requested user. Based on the personal information obtained during login the trusted authority verifies whether user is an authorized user or not. After verification done by the authority the certificate is issued to the valid user, if the user is not an

authorized user then the certificate is not issued by the trusted authority. All the other details regarding the user will be made available in the CRL, including the user id. This information is broadcast to other members of cluster group.

B. Certificate Update

User certificate is valid only during its lifetime. Each user can update the certificate instead of receiving a new certificate to extend the validity of it [7]. Before the validity dates of the certificate get expired, the user will send the certificate update request to the authority. After receiving the update request message, the authority verifies whether the request message is really from the authorized user or not. When the request obtained is from valid user, the authority sends the response message by updating the certificate. After obtaining the response message, user can continue its work within the network.

C. Verification of Certificate

Trusted authority verifies the certificate by the available data among it when the user enters into the cluster and makes the communication with the other nodes. Before user joins the group, it sends a request to the authority via a secure channel. After being authenticated by the trusted authority, users become a new legitimate member and get its certificate from trusted authority. They then exchange their certificates with other user of same cluster to verify each other's legal identity. Whenever the user leaves the cluster the certificate of that particular user become invalidates. This makes the communication between authorized nodes and malicious nodes can be easily identified.

III. RELATED WORK

Various types of certificate revocation techniques have been proposed to enhance network security. Providing security to MANET is a challenging one due to their dynamically changing topology, limited physical protection of nodes, the vulnerability of wireless links, and the lack of infrastructure [3]. Certified tickets are locally managed in the network to evict nodes. The tickets of the newly existing nodes are issued by their neighbors. There is no centralized authority; therefore the ticket of a malicious node is revoked by the vote of its neighbors. Upon receiving such a ticket renewal request, a neighboring node checks its records, generated by its chosen neighborhood monitoring mechanism during the latest monitoring period. The monitoring period is typically about the same order of magnitude of the average time that a node remains within the one-hop communication range [6]. Every node performs one-hop monitoring, [3], [4] and exchanges monitoring information with its neighbors which allow for malicious nodes to be identified. When the number of votes increases a certain threshold level, the ticket of the accused node will be successfully revoked. Nodes will not be able to communicate with other nodes without valid tickets and hence revoking a node's ticket implies the isolation of that node.

The existing proposals are generally attack-oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart such threats. Because the solutions are designed with certain attack models in mind, they work better in the presence of designated attacks but it may collapse under the unanticipated attacks [2].

Generally nodes vote in variable size. The nodes weight is calculated in terms of the reliability and trust worthiness of the node that is obtained from its past behaviors, the number of accusations against other nodes and that against itself from others [3]. If the reliability is stronger, then the weight acquired will be greater for the nodes. The accuracy can be improved for the certificate revocation when the weighted sum from voters against the node exceeds a predefined threshold level [3], [4]. Every node are required to participate in voting mechanism, therefore communications overhead used to exchange voting information is very high, and it increases the revocation time as well. Simultaneously certificates of both the accused node and accusing node have to be revoked. In other words, the accusing node also sacrifices itself to remove an attacker from the network. The research on MANET security is still in its early stage.

In Cluster-based certificate revocation scheme [3], where nodes are self-organized to form clusters. There are number of cluster authorities (CAs) to efficiently perform the publication and revocation of certificates. A trusted certification authority is responsible to manage and maintain the control messages, consist of accuser and accused node in the warning list (WL) and blacklist (BL). The certificate of the malicious node can be revoked by any single neighboring node. In addition, it can also handle 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 minimum time to complete the process of handling the certificate revocation. The significant advantage of the voting mechanism is the high accuracy in confirming the given accused node as a real malicious attacker or not [3], [4]. The decision process to satisfy the condition of certificate revocation is slow. Also, it observes heavy communication overhead during the exchange of accusation information among each other. Cluster head detect the falsely accused nodes within its cluster and recovering their certificates to solve the issue of false accusation. Cluster based routing protocol is used in order to inherits the advantage of the voting based mechanism and to overcome the communication over head due to the exchange of the voting information.

IV. PROPOSED SYSTEM

All Nodes together form clusters and each cluster consists of a Cluster Head (CH) Along with several Cluster Members (CMs) that are located within the communication range of their CH. Each CM in the cluster belongs to two different clusters in order to provide robustness against changes in topology due to mobility [4], [6]. It should also be noted that because the clusters overlap, a node within the communication range of a CH is not necessary part of its cluster. Clustering information is not used for routing purpose; it is only used for managing certificates.

The aim of using clusters is to enable CHs to identify false accusations. Requests made to CA to recover the certificates of falsely accused nodes can only be made from CHs. A CH will send a Certificate Recovery Packet (CRP) to the CA to recover an accused node, only in the case where it is a CM in its cluster. This is based on the fact that attacks can be detected by any node within the communication range of the attacker. This implies that a CH will be able to detect any attack executed by one of its CMs, specifies that a CH can identify whether a CM is malicious or not. Since the CA regularly broadcasts certificate information on nodes which have been accused as malicious nodes, CHs will be able to detect false accusations against their CMs by comparing this information with their own local observations.

A. Path finding

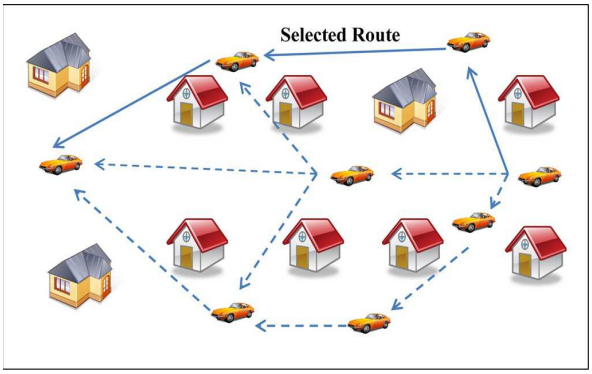


Fig.1. Path selection

Fig.1 shows path is selected and the data is forwarded among the path to reach the destination quickly. Mostly Data will be forwarded among cluster member within the same cluster region, or members belong to other cluster group. Once the path has been found by using the cluster based routing protocol, data can be transmitted through the path and finally data reaches the destination.

Data passed through the path may or may not reach the destination. Once data reaches the destination then there is no attacker available in the path. If the data does not reaches the destination then there is an attacker available in the path.

B. Attacker Node

In MANET, malicious node can easily disrupt network operations by violating routing. The attacker node will send the unrelated message continuously to the other node and make an attack to authorized node. This will make the authorized node not to perform its function properly. The attacker node can be detected by using the attacker detection methodology.

The data will be transmitted from the sender node to the receiver node. If the receiver node is an attacker node, then the receiver node will send continuously acknowledgement to the sender node and affect the sender node. These are referred as replay attack and can be detected by using the attack detection method.

C. Certificate Revocation List

As clients leave the system, the certificates should be made as invalid even though the certificate lifetime has not expired. Certificate revocation processes use a CRL that is periodically generated by the authority and distributed to all the participants via an overlay network with pull or push transfers [8]. The CRL distribution overlay is established on the media data transmission network. This CRL consist of index that stores the unique id of the certificate.

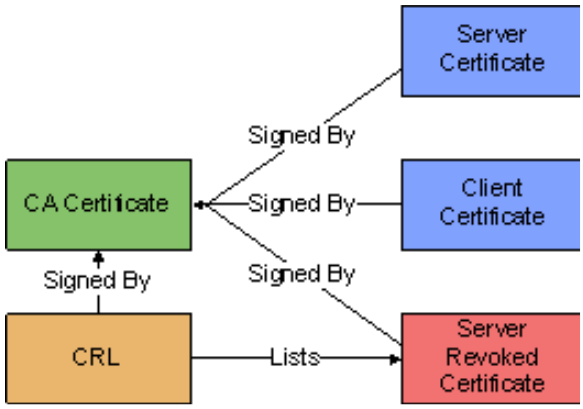


Fig.2.Certificate revocation

Fig.2 shows there is a certificate authority which is a trusted third party, these authority will sign the certificate for the server, client. There is also certificate revocation list which contains the list of the members and their information. In certificate revocation process, any node in network is trying to do some malicious activity and if it is detected by some other node , then detector will intimate

about the accused node to destination, claiming that nodes as accuser.

Once trusted authority receives the complain, it forward the accuser name to all cluster heads to know it is malicious or not. And all cluster heads forwards that information to all nodes except to accuser and complained node. So now all nodes checks with their buffer whether this node previously performed malicious activity or not [3], [4]. Once cluster heads receives all replays, it sends total number of attack counts and non attack counts to trusted authority. Now trusted authority will have all nodes replies about that accuser. If maximum number of nodes tells that, accused node is attacker, then that node is added to black list and intimated to all nodes through cluster heads. Else if none of the attackers count is more, the node in black list will be released and intimated node will be added to list.

V. SYSTEM ARCHITECTURE

Network topology is formed with trusted authority, regions, cluster members (nodes), cluster heads. First trusted authority is formed and regions were created to some coverage area. Trusted authority is considered as a trusted third party [3], [7]. Each node created by assigning some name and range. According to its range nodes forms different clusters. Cluster head election is based upon their battery, memory, mobility. All the cluster heads can communicate with all the cluster members present in the region. Cluster head will intimate all the information regarding the region, cluster member to the trusted authority.

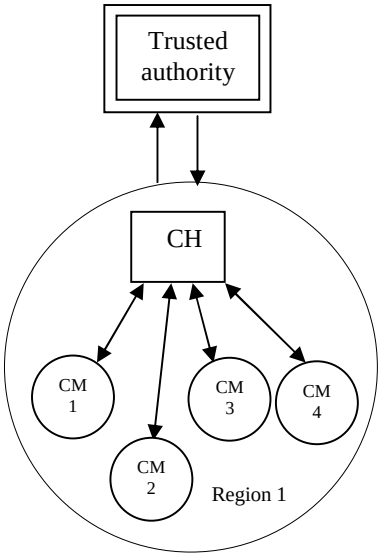


Fig.3. Trusted authority and cluster groups

Fig.3 shows there is a Trusted Authority, and there is a Cluster Head, all the Cluster Members are connected to the Cluster Head. This Fig.3 explains only one region; likewise there will be many regions available.

Revocation time is an important factor for measuring the performance of the revocation scheme; it defined as the time from an attacker node's launching the attack until its certificate is revoked. Generally In MANET, mobile nodes are assumed to be uniformly distributed over a coverage area so as to satisfy the binomial distribution B(n,q) which denotes the probability of number of nodes existing in a special area [3].

VI. CLUSTER-BASED ROUTING PROTOCOL

Due to the limited transmission range of wireless network, multiple "hops" are needed to exchange data across the entire network. To facilitate communication within the network, a routing protocol identifies routes between the nodes. The goal of an ad hoc network routing protocol is efficient route establishment between a pair of nodes so that messages may be delivered in a timely manner. The construction of route should be done with a minimum of overhead and bandwidth consumption. Cluster based routing protocol for MANET uses clustering's structure to decrease average end-to-end delay and improve the average packet delivery ratio.

Cluster Based Routing Protocol works efficiently for finding the shortest path among the nodes. Nodes are available at different regions. Some nodes will be common to both the region. This common node is represented as gateway node. This gateway node will act as an intermediate node. Whenever the data is transmitted between two regions they pass through this intermediate node only.

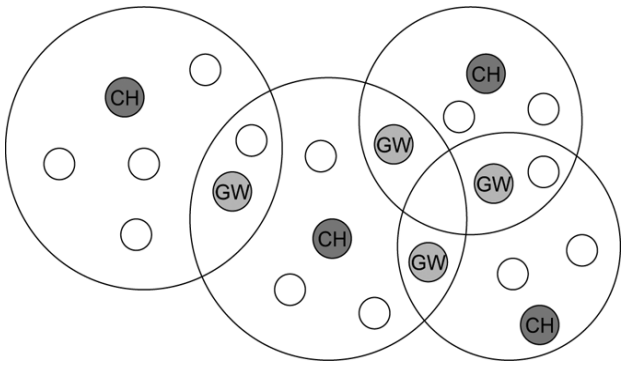


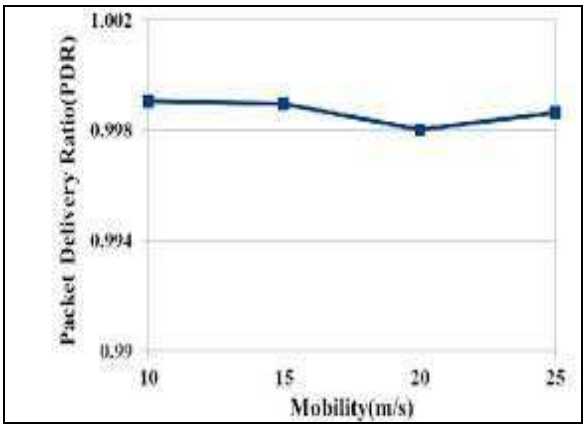
Fig.4. Cluster Head and gateway nodes

Fig.4 shows there is availability of cluster head at each region which maintains the information of other nodes. There is also gateway node in regions. These gateway nodes will act as an intermediate node between the regions. By using these gateway nodes shortest path can be fond easily for the data transmission by using the cluster based routing protocol.

As analyzed above, the number of normal nodes is decreasing over time. When m = 0, i.e., no normal nodes within an attacker's transmission range, then the probability is

$$Pr(m = 0) = e^{-\theta\rho S} \quad (1)$$

From (1), the probability Pr(m=0) greatly increases with the decrease of density ρ; the efficiency of detecting malicious attackers is significantly reduced. In other words, the probability Pr(m=0) must be reduced to guarantee a certain number of nodes in the network to revoke malicious attackers quickly. Consequently, the legitimate nodes should be released from the WL and be restored of their accusation function to increase the number of available normal nodes in order to enhance the robustness and reliability against the decreasing number of normal nodes over time.



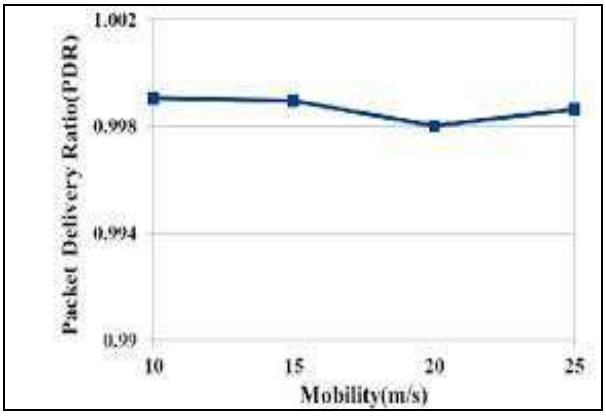


Fig.5. packet delivery

Fig.5 shows as MANET represent all the moving object, There will be some delay or failure of packet delivery in MANET. This ratio has been analyzed and is represented above. Some of the packet may be transmitted between the legitimate node and some of the packet may be transferred between the malicious node to the legitimate node. There is probability of delay in delivering the packets or failure in delivery in both the cases.

VII. CONCLUSION

Secure communications for MANET, is a major issue and has been addressed by using the proper certificate revocation of attacker nodes. The proposed 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. Cluster-based model is used to restore falsely accused nodes by the cluster head, thus improving the reliability of certificate revocation.

REFERENCES

[1]. Yongguang Zhang, Wenke Lee, "Security in Mobile Ad-Hoc Networks" Springer-Verlag US., pp 249-268, 2005.

[2]. 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.

[3]. Weiliu, Nirwan Ansari,"cluster-based certificate revocation with vindication capability for mobile ad hoc networks," ieee transactions on parallel and distributed systems, vol. 24, no. 2, february 2013.

[4]. Priti Rathi, Parikshit Mahalle, "Certificate Revocation in Mobile Ad Hoc Networks," International Journal of Application or Innovation in Engineering & Management, Volume 2, Issue 1, January 2013.

[5]. 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, pp. 261-273, Feb. 2006.

[6]. 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, pp. 1049-1063, Oct. 2004.

[7]. LIU Xuening, YIN Hao, LIN Chuang, DU Changlai, "Efficient User Authentication and Key Management for Peer-to-Peer Live Streaming Systems", tsinghua science and technology issnll1007-0214ll13/18llpp234-241 volume 14, number 2, april 2009.

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