

TRUST BASED MALICIOUS NODE DETECTION & CERTIFICATE REVOCATION BASED ON CLUSTER HEAD FOR MANET

Ms.L.Muthumari,
PG Scholar,
Department Of Computer Science
and Engineering
Dhanalakshmi college of Engg.,
Tambaram Tamil Nadu
smss91227@gmail.com

Mr. Y.Sharmasthvali,
Asst.Prof.
Department Of Computer Science
and Engineering
Dhanalakshmi college of Engg.,
Tambaram. Tamil Nadu
vali566@gmail.com

Mr. S. Sivakumar,
Asso.Prof.
Department Of Computer Science
and Engineering
Dhanalakshmi college of Engg.,
Tambaram. Tamil Nadu
sivas.postbox@gmail.com

Abstract— Mobile adhoc network (MANET) is an infrastructure less network where the nodes can move easily. The main aim of this paper is to provide security in the network. In this paper, we propose Trust and certificate based Malicious Node detection and also improve certificate revocation based on cluster head for mobile adhoc network. Cluster head plays an important role in detecting falsely accused nodes. The reliability will be increased based on single node accusation and based on the optimum threshold value the malicious node can be identified easily and it can be isolate from the network. Instead of nodes directly send accusation message to Certificate Authority (CA), it will confirm with cluster head, then cluster head will decide whether accusation is correct or not. Then cluster head pass the message to CA. In the trust based scheme, if the trust value falls below the trust threshold value, then the particular node is marked as malicious node and the certificate revoked and isolated from the network. The performance of our scheme is measured by simulation method.

Index Terms— Mobile adhoc networks (MANETs), Certificate revocation, Cluster Head, Trust Handler, Trust table, Certificate Authority.

1 INTRODUCTION

Due to their tremendous growth of mobile adhoc network in recent years, the growth of usage of the mobile reaches the hike due to the mobility, topology, cost, accommodation etc. Generally mobile network forward the packet to the destination within its transmission range. In adhoc networks, multichip packet delivery is achieved and they perform two network operations. They are adhoc routing and packet forwarding. The existing ad hoc routing protocols are Ad Hoc On Demand Distance Vector (AODV), Dynamic Source Routing (DSR) and wireless MAC protocols, such as 802.11, they assume a trusted and cooperative environment. So, malicious attacker will become a router and it will disrupt the normal network operations by disrupting all the protocol specifications. To secure an ad hoc network, we consider the following attributes: availability, confidentiality, integrity, authentication, and non-repudiation.

There are two basic things for protecting the MANET, They are Proactive and Reactive. The Proactive approach will prevent the attack before attack takes place by

adopting various cryptographic techniques. The reactive approach will detect the attacks that happened in the network and it will react accordingly. The complete security in Manet must integrate both the approaches and it must have all the three components such as prevention, detection and reaction. For example the proactive approach will enable all the routing protocols and states, while the reactive approach will ensure the protection of packets while forwarding. As a result missing a single component will degrade the strength of overall security solution.

In a mobile during transmission of nodes, security is important because in a wireless service due to their property, the type of security attacks is more. Implementing such a type of security is very crucial thing in a network. Due to the property of MANET in mobile nodes they are implementing the functionality of all features beginning from transmission until to reach destination, they themselves act as the end user and router, they easily join and leave the network freely. In final, due to the presence of node in hostile environment, the attackers act freely to authorize the service. This feature of wireless network make more vulnerable than the wired network. To manage the security problem, certification in an Manet is widely used to provide the conveying component in a public key infrastructure. Certification is a predefined (or) authority to the node which is simply recognizes the node in the network communication. In certification, generally they Encompassed three components (i) prevention (ii) detection (iii) Revocation, in such a case any attacks can be easily identified. In this certificate revocation it is an important task of recognizing and deleting the nodes which is found to be vulnerable to the attacker. In a general certificate, it encompasses the data as like digital signature (or) verification to verify whether the node is belonging to it or not. To avoid the tampering and forging in mobile adhoc network, in this we focus of general problem of certificate list to provide secure communication in adhoc network.

2. RELATEDWORKS

Recently researches have much attention to MANET regarding Security issues. It is very difficult to secure adhoc networks because of the lack of infrastructure and wireless link in the network. There are various kinds of Certificate revocation techniques to enhance the network security. In this section, the existing approaches for certificate revocation are going to be classified.

2.1 Existing System

The existing system deals with the cluster construction and the cluster based revocation scheme which revoke the attacker nodes by one accusation from a neighboring node. By framing the cluster architecture the Cluster head will revive the falsely revoked nodes from the network.

Before joining the network, all the nodes need to get certificates from the certificate authority and how the malicious node can be identified in the network. Each node will be performing only one hop.

2.2 Cluster Construction

The security design for Manet is concerned with securing the network functionality, to deliver the packets between mobile nodes. Its main aim is to ensure that the routing message transform between the nodes is consistent and the packet forwarding is based on the reliability. The essential component in it are Cluster Head (CH), Cluster member (CM) and Cluster Authority (CA). Generally, in this topology nodes cooperate to form a cluster. In a cluster if the nodes want to join the network, they need to certify from the certificate Authority. The certificate authority which is Responsible for broadcasting the message to all nodes and it controls all the nodes in the network. Generally the cluster will be formed within the transmission range. In a cluster, the nodes will start joining the network as will initialize as cluster members. The cluster members form a cluster due to the availability of the link, and transmission range. If they are beyond the transmission range the link is disconnected.

In this model, if a node is initiated as a Cluster Head it allows to propagate a message as cluster head packet (CHP). This message will be notified by neighbor nodes. The nodes within its transmission range, can accept CHP and they replay to their respective cluster Head. When the nodes join the network, they must communicate periodically to all nodes. If a cluster member goes out of its range, then the link will be disconnected and they will be isolated from the network. We can assume that the nodes are within one hop count, so that if the nodes are beyond the one hop count, they cannot communicate with the cluster head and it will be disconnected from the network. All nodes must be in one hop range and if they are beyond the network, they can form a new cluster and they can join the network.

2.3 Role of Certificate Authority

Certificate Authority (CA) is a trusted third party that issues Digital Certificates and public-private key pairs. The role of the Certificate Authority (CA) is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. A Certificate Authority (CA) can be a trusted third party that is responsible for physically verifying the legitimacy of the identity of an individual or organization before issuing a digital certificate.

Certificate Authority (CA) Verifies the identity: The Certificate Authority (CA) essentially validates the identity of the entity who requested a digital certificate before distributing it.

Certificate Authority (CA) maintains Certificate Revocation List (CRL): The Certificate Authority (CA) sustains Certificate Revocation List (CRL). A certificate revocation list (CRL) is a list of digital certificates which are not valid and have been invalid and therefore should not be relied by anyone.

CA is in charge of updating two lists, Whitelist and Blacklist, which hold reproving and suspect nodes information respectively. BL is in charge of holding node accused as an attacker, WL is in charge of holding reproving node.

2.4 Reliability Node Classification

According to the behavior of nodes in the network, three types of nodes are legitimate, malicious and attacker nodes. **Legitimate node** is defined as the secure node in the network for communication. That will detect the attacker node correctly and revoke the certificates of the malicious node. The **malicious node** will revoke the malicious attackers and will not execute the function of network. The **attacker node** will be considered as the special malicious node and it will disturb the normal behavior of the network and it will not provide secure Communication.

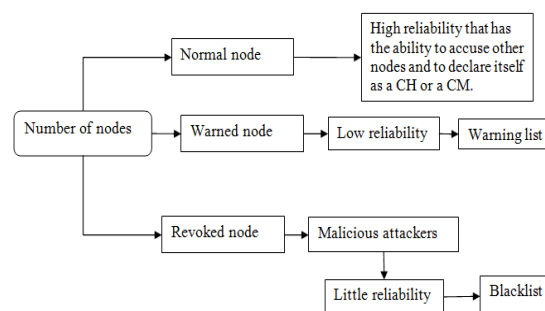


Fig.1. Classification of Nodes

2.5 Certificate Revocation

In MANET, authorization plays a vital role to reach complete network security. Management issue of certificate revocation in wired network is somewhat easy related to the MANETs. In wired network, when the certificate of a malicious node gets revoked then the certificate authorities add the information about the revoked node in to certificate revocation lists (CRLs) otherwise transmission the CRLs to each and every node current in the network.

2.6 Revoking malicious certificates

The protection of certificate message exchange a part of network layer security solution for MANET. There is certain possibility for malicious node to revoke valid nodes in the network. In order to revoke, we initially consider three stages for Certificate revocation process. Generally they are (i) accusing (ii) verifying (iii) notifying. The main goal is to find the attacker node. The two lists maintained are Whitelist (WL) and Blacklist (BL), where if the message is linked through cluster member by cluster Head, then initially neighbor node will check the Local list of Blacklist to verify whether attacker is there or not. If not, neighboring node will cast the accusation packet to cluster Authority. When the CA receives the accusation packet, it will check the certificate validation of accusing node. If valid, accused node will be considered as a malicious attacker and they can be maintained in the BL. The accusing node will be in WL. At last, by broadcasting of messages by the CA, nodes that are in the BL are successfully eliminated from the network.

2.7 Coping with false Accusation

An easy way to identify attackers is to gather various information on attackers from nodes in the network. However, in this approach, it is tough to distinguish valid accusations made by legitimate nodes from false accusations made by malicious nodes. The amount of traffic in order to exchange messages on attackers and the valid time to gather the information will improve as the network size becomes larger. The certificate revocation scheme which can cancel the certification of attackers in a short time with a small amount of operating traffic.

The false accusation of a malicious node against a valid node to the CA will lower the accuracy and robustness of our scheme. To overcome this problem, the aim of forming clusters is to enable the CH to check false accusation and restore the falsely accused node within its cluster. Each CH can identify all occurrences from its CMs, and direct to the CA to recover the certificate of the falsely defendant node can be accomplished by its CHs by delivery of Recovery Packets (RPs) to the CA. After receiving the recovery packet from the CH, the CA can remove the falsely accused node from the BL. The

CA will spread the information or packets of the WL and BL to all the nodes in the network and the nodes update their BL and WL from the CA even if there is a false accusation. If the CH does not check any attacks from a concern accused member mentioned in the BL from the CA, the CH will be aware of the presence of false accusation against its CM. Then, the CH will send a recovery packet to the CA, in order to revive the cluster member from the network. When the CA get the recovery packet and check the validity of the sender, the falsely accused node will be removed from the BL and held in the WL. Then, the CA propagates this information to all the nodes for the overall network.

3 PROPOSED WORK

The proposed work mainly focus on how to Detect and eliminate the Malicious Node. It mainly depends upon the two schemes (i) Trust and certificate based Malicious Node Detection management Scheme (ii) Reliability.

3.1 Trust and certificate based Malicious Node Detection

This research mainly depends upon the Trust management scheme, which explains about the trust in MANETs and routing on the basis of trust. It uses trust values for forwarding a packet or information by maintaining a trust token for each node. If the trust token value falls below a trust threshold, then the particular node is marked as malicious node and the certificate will be revoked, isolated from the Network, so the performance will be increased in the network.

All the nodes while communicating with other nodes, the trust value of all of the communicating nodes are calculated and they are maintained in the trust table of that node with field name like direct trust value and one more total trust value of the corresponding node. Then some time the neighbor nodes may move out of the cluster due to their mobility and they will come back to that cluster to form again a network, then the trust value is calculated and that network entry is also updated in that table. Every change in the network will be updated.

The trust agent will perform the subsequent task and the Computation. Node x want to evaluate the trust value on node y termed as

$$dt_{xy} = p_s / p_r$$

Where dt_{xy} is the direct trust value of x and y.

p_s is the packet sent from the node x.

p_r is the packet receive from the node y.

To calculate the direct trust on node, the direct trust table is maintained.

Direct Trust Table

Node ID	Packet send	packet received	Dropped	Direct Trust

3.2 TrustHandler

The trust handler will enable all the incoming and outgoing ALARM messages. Incoming ALARMS can be updated from any node. So, the source of an ALARM has to be examining for trustworthiness before Starting a reaction. This conclusion is made by seeing at the trust level of the reporting node. The outward ALARMS are initiated by the node itself after having practiced, looked, or in receipt of a report of malicious node activities. The receivers of these ALARM messages are called friends, which are maintained in a friends list by each node. The ALARM should be created even when the last Trust value is low. After ending of the Final Trust Value, by keeping this value, it could say that, they are a partial Identification of Malicious node. It was obtained by using Trustworthy Mechanism. After recognizing the trust, it will trigger the alarm to its neighbor nodes to avoid confusion in the network. The trust table will update the trust records of each node to find the trustworthiness of an incoming alarm. The friend list will be maintaining all the list of nodes to which the node has to send alarms when it checks if there is any badactivity.

In this method the trust is maintained only when it is needed. Therefore, each node will have the direct trust value of all remaining nodes as well as the indirect trust or recommended trust value. Nodes with less trust values will be considered as MALICIOUS node. An alarm is created by the Trust Manager to show that the node's malicious behavior to other valid nodes in its range, thus isolating the less trusted nodes and forming a secure system. No unsecure nodes can cause unprotected and danger to the nodes. Trust values of each node are measured and information transmission is done by the nodes which have highest trust values. These trust values are measured dynamically time to time and updated. Hence the packets or information are sendsecurely.

3.3 Reliability

The second scheme is, in order to identify the malicious node, the CA will classify node as high reliable or low reliable. If an accusation request comes from high reliable, than immediately the CA will disseminate the message to all nodes and it will be isolated from the network. Otherwise, the CA will waits for accusation message from another node, if both the nodes will send the same message, then the CA will check the reliability and it will be isolated from thenetwork.

In the existing system, all the nodes in the network directly communicated to the Certificate Authority. So, the high communication overhead occurs in the network. Automatically the accusation detection time is high in the network. In this scheme, instead of sending all theinformation

directly to CA, they can send their information or packet to the Cluster Head. The cluster Head will check the node whether it is malicious or valid node based on the past behavior of the nodes and its reliability, if the node is deemed as malicious node, then automatically it will send to the Certificate Authority. Only if the node is coming from the CH, the CA will revoke the certificate of the node and it will broadcast the information to overall network.so, automatically the CA will detect the false accusation correctly and the communication overhead will be reduced. The traffic will be reduced and the network performance will be improved.

4 PERFORMANCE EVALUATION

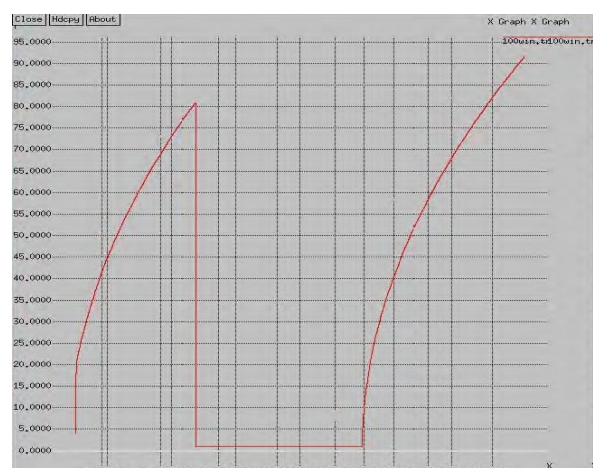
In this Paper, we present simulation results conducted in the network simulator, Qualnet 4.0. To measure the performances of our proposed scheme, we run simulations to check its efficiency in removing the malicious node from the network and cancelling the attacker nodes' certificates, and compare them with the existing schemes; also the revocation time can be reduced. Then, we also evaluate the accuracy of releasing legitimate nodes in our scheme.

4.1 Deriving the optimalThreshold

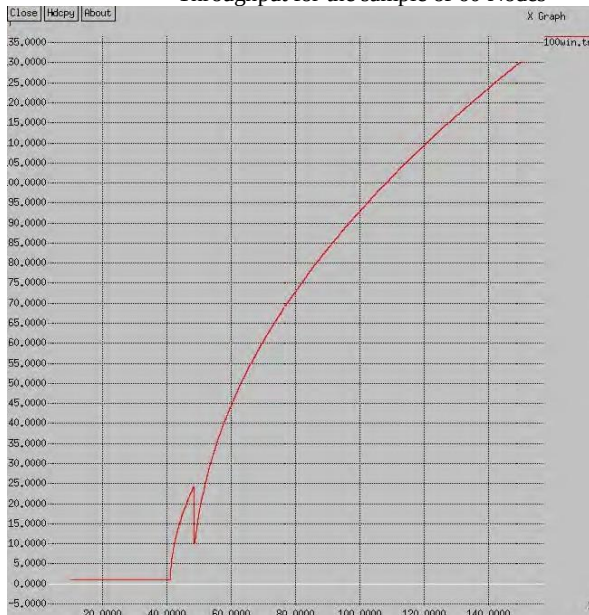
In this simulation, we prove the optimum threshold value in comparison with the numerical result. We set 50 nodes in the network, which contains five malicious nodes and five attacker nodes. The trust table is maintained and updated, and the threshold value is calculated.

4.2 Throughput for Proposed System

In the projected system, as the malicious nodes are recognized in the first level of broadcast and malicious nodes are isolated with increase in the level of throughput. The removal of malicious node ID in the trusted node table make the malicious nodes isolate. After the complete isolation, the trusted nodes will send the packets by having the certificates.



Throughput for the sample of 60 Nodes



4.3 Summary

In summary, the simulation results will show the performance of this scheme: 1) the threshold is the optimum value to differentiate the legitimate nodes from malicious nodes 2) the proposed scheme performs the trust and certificate based malicious node detection and it maintains a trust table for revoking the malicious node 3) the trust Handler will enable the incoming and outgoing messages by the ALARM messages 4) It performs increased accuracy in removing valid nodes

5. CONCLUSION

In this paper, we have discussed a major issue to guarantee the communications for mobile ad hoc networks, for the certificate revocation of attacker nodes. By comparing with the existing algorithms, we propose an Enhanced cluster based certificate revocation based on cluster head scheme combined with the merits of cluster based certificate revocation to cancel malicious certificate and solve the problem of false accusation. This scheme will cancel an accused node based on a single node's accusation, and it will decrease the revocation time as compared to the existing mechanism. Also we have implemented the cluster-based model to recover the falsely defendant nodes by the CH, thus improving the correctness.

Particularly, we have proposed a new method that is trust and certificate based malicious node detection. If the trust value is below the threshold value, then the node is considered as malicious node and it will be isolated. Release and restore the legitimate nodes, and thus increasing the number of normal nodes in the network. We have sufficient nodes to ensure the efficiency of quick revocation. The results have explained that, in comparing with the existing methods, our proposed scheme is more effective and efficient in cancelling certificates of malicious attacker nodes, reducing revocation time, and increasing the accuracy and reliability of certificate revocation.

REFERENCES

- [1] Wei Liu, Student Member, IEEE, Hiroki Nishiyama, Member, IEEE, "Cluster-Based Certificate Revocation with Vindication Capability for Manet", IEEE Communications on equivalent and distributed systems, VOL. 24, NO. 2, FEBRUARY 2013.
- [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] 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.
- [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, pp. 8-20, 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, pp. 48-66, Third Quarter 2006.
- [6] 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.

