Certificate Revocation Using Public Key Infrastructure For MANET's

Gowsalyaa.M[1],Karthick.N[2],Keerthana.S[3],Durga.R [4]

[1,2,3]Department of Computer Science And Engineering
[4]Assistant professor
SNS College of Technology,
Coimbatore- 641 035, Tamil Nadu, India.

Abstract---**The mobile Ad Hoc networks (MANETs) having wireless and dynamic nature. MANETs are more susceptible to security attacks rather than wired networks. So they are vulnerable to security attacks from malicious node due to which it is important to detect malicious nodes to avoid attacks. In this paper certificate Authority (CA) provides it's secret key to all nodes (normal). When node want to send data to other nodes Cluster Head (CH) broadcast R2mod N to all nodes and it gives challenge to that node whether it sending same data, if it sends RS mod N to CH with its secrete key which is provided by CA, then CH compares its data with itself data. If it is same, then it considers it is as a normal node otherwise as malicious node. Here CA should be legitimate. Finally if node is found as a malicious then revocation of certificate is done for that malicious node and other normal nodes are released due to which the number of normal nodes will increase in mobile network and it get secured from susceptible attacks.**

I.INTRODUCTION

In wired/wireless infrastructure networks, a trusted third party, known as Certification Authority (CA), is needed to certify users' digital certificate that contains users' public key and identity. It is needed to provide a secure communication among users and ensure some security requirements, such as; authentication, confidentiality and integrity of transited data. In classical Public Key Infrastructure (PKI), a Registration Authority (RA) is used to collect and analyze users' requests before forwarding them to a CA to certify, issue and renew user's digital certificate. In Mobile Ad hoc Networks (MANETs), a decentralized certificate authority approach is proposed, due to MANET characteristics, as a solution to avoid single point of failure, MANET attacks and consider nodes' mobility. To handle these requirements, a distributed clustering algorithm is proposed to cluster nodes based on a set of trusted nodes that belong to a confident community. A head cluster is selected among trusted nodes to play the role of CA.

A system based on the distribution of the certification authority among specific nodes by using the threshold cryptography scheme with several threshold levels to offer nodes flexibility in selecting an appropriate security level for a given application. With this approach the fault tolerant and hierarchical key management services are ensured. Unfortunately, the approaches based on threshold cryptography have some drawbacks: Firstly, then nodes must be initialized by a trusted authority which is responsible for introducing the partial secret of CA role. On the other hand, an external administration is necessary to configure the system and establish the architecture. Secondly, the number k must be a trade-off between availability and robustness, it must be frequently updated. Thirdly, the system overloads the network since the node must send at least k requests instead of sending only one request to obtain a certificate or revocation (i.e.,k−1 messages are needed).A few work tried to introduce the fully CA distribution without using the threshold cryptography. In these systems, each user is able to generate a certificate for other users. Certificates are stored and distributed by the users themselves. In this system, each user maintains a local certificate repository. When two users want to check the public keys of each other, they merge their local certificate repositories to find appropriate certificate chains. Several work introduce the cluster concept for security in MANETs particularly for the CA distribution. The distribution

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET

of the CA service by using threshold cryptography and introduce the cluster structure. The cluster concept is adopted to provide the CA service and proactive secret shared update protocol. A distributed architecture divides the network into clusters and distributes the CA in each cluster to secure the network.

II. Related And Research Work

It is difficult to secure mobile ad hoc networks, notably because of the vulnerability of wireless links, the limited physical protection of nodes, the dynamically changing topology, and the lack of infrastructure. Various kinds of certificate revocation techniques have been proposed to enhance network security in the literature. Certificate revocation, which are classified into two categories: voting-based mechanism and non-voting-based mechanism.

Voting-Based Mechanism:

The so-called voting-based mechanism is defined as the means of revoking a malicious attacker's certificate through votes from valid neighboring 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 previous studies each node performs one-hop monitoring, and exchanges monitoring information with its neighboring nodes .Since nodes cannot communicate with others without valid certificates, revoking the certificate of a voted node implies isolation of that node from network activities. In some existing approaches there is no Certification Authority (CA) exists in the network, and instead each node monitors the behavior of its neighbors.

Non-voting mechanism:

However ,certificates of both the accused node and accusing node have to be revoked simultaneously. Although this approach 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.

III. Existing Work

The model of the proposed cluster-based revocation scheme, which can quickly revoke 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.

A trusted third party, certification authority, is deployed in the cluster-based scheme to enable each mobile node to preload the certificate. 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.

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 unrestrainedly in a MANET.

As a solution to release nodes from the WL, we should first consider the two cases for nodes to be listed in the WL. As shown in Fig. 1, the first case is that a legitimate node correctly accuses an attacker node, thus resulting in the accusing node and accused node being listed in the WL and BL, respectively; the other case is the enlisting of a malicious node in the WL because it sends false accusation against a legitimate node. Hence, nodes in the WL may be legitimate nodes as well as malicious nodes.

Therefore, to improve the reliability and accuracy, nodes must be differentiated between legitimate nodes and malicious nodes so as to release legitimate nodes from the WL and withhold malicious nodes in the WL.

IV. Model Of Cluster Based Scheme

Node deployment:

The module in the implementation is generating mobile nodes. The number of mobile nodes will be initiated in the topography with the node properties such as node id, initial bandwidth and RREQ, RREP etc.,The first module utilizes the .tcl language with standard MANET parameters such as wireless physical channel type, with 35 nodes, and one CA.

Cluster Architecture:

This module presents the cluster-based architecture 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

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET

from the CA, which is responsible for distributing and managing certificates of all nodes, so that nodes can communicate with each other unrestrainedly in a MANET.

Certificate revocation and Node classification:

The module implements the overall all process of the proposed cluster based node detection scheme.

This performs the following tasks

a. Classification:

According to the behavior of nodes in the network, three types of nodes are classified according to their behaviors:

A legitimate node is deemed to secure communications with other nodes. It is able to correctly detect attacks from malicious attacker nodes and accuse them positively, and to revoke their certificates in order to guarantee network security.

A malicious node does not execute protocols to identify misbehavior, vote honestly, and revoke malicious attackers. In particular, it is able to falsely accuse a legitimate node to revoke its certificate successfully.

The so-called attacker node is defined as a special malicious node which can launch attacks on its neighbors to disrupt secure communications in the network.

b. Key verification

For every transaction the proposed protocol contacts the certification authority. And verifies the keysfor node identification.

c. Black and whitelist management:

Once the keys verified by the CA, the node will be listed in BL or WL based on the keys.

V. PROPOSED WORK

Clustering is incorporated in the proposed scheme, where the cluster head plays an important role in detecting the attacker node and the falsely accused nodes within its cluster and recovering their certificates to solve the issue of false accusation.

The proposed 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. Our scheme can quickly revoke the malicious device's certificate, stop the device access to the network, and enhance network security.

Some of the advantages that can be identified using the proposed work is that it is fast and accurate such that it can reduce the communication overhead between each of the nodes.The attacker node provides the deactivation and isolation of the communication between each of the nodes in the network.This work also identifies the falsely accused nodes such that the data can be send to the destination node without the changing of the data provided to be sent through the network.

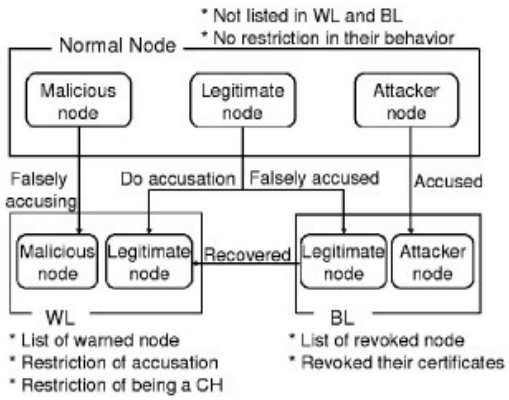

Fig 1.The classification of nodes

VI. SIMULATION SETUP

In this section, we present simulation results conducted in the network simulator. To evaluate the performances of our proposed Cluster Based Certificate Revocation using Public Key Infrastructure scheme, we run simulations to verify its efficiency. The cluster formation of the nodes are provided and the various types of attackers hack the message and lead to the packet loss in the communication of the nodes. In this simulation we mention the efficiency of providing the public key to the nodes in the network and the probability of identifying the attackers can enter the cluster in the given range.

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET

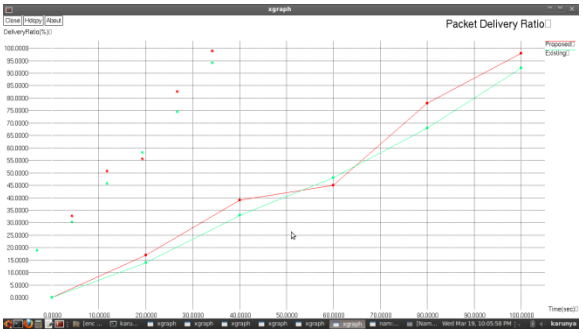

Fig 2.Packet Delivery Ratio

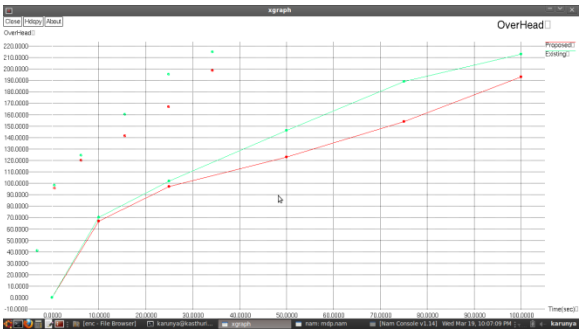

Fig 3.Cluster Overhead with time ratio

VII. Conclusion

In this paper, we have addressed a major issue to ensure secure communications for mobile ad hoc networks, namely, certificate revocation of attacker nodes. In contrast to existing algorithms, we propose a certificate revocation with public key infrastructure combined with the merits of both voting-based and non-voting based mechanisms to revoke malicious certificate and solve the problem of false accusation. The scheme provides the certificate authority in which the public key is distributed to all the cluster nodes.

The malicious nodes can be identified with the certificates provided by the certificate authority in such a way that the legitimate nodes can be made as the active and the other nodes as the deactiveone.Hence our proposed scheme is to provide the reduction in communication overhead.

Acknowledgment

We take immense pleasure in expressing our humble note of gratitude to our project guide **Mrs.R.Durga**, Assistant Professor, Department of Computer Science and Engineering, SNS College of Technology, for her remarkable guidance and useful suggestions, which helped us in completing the paper before deadline.

References

[1] Wei Liu,Student Member ,IEEE ,Hiroki Nishiyama,Member ,IEEE, NirwanAnsari,Fellow,IEEE,Jie Yang ,and NeiKato,Senior Member ,IEEE"Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks"IEEE Transaction on Parallel and Distributed System,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]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.

[4]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.

[5] Mrs. Priti Rathi1, Mr. Parikshit Mahalle2 1,2Department of Computer Engineering, Smt. KashibaiNavle College of Engineering,, India "Certificate Revocation in Mobile Ad Hoc Networks" International Journal of Application or Innovation in Engineering & Management Volume 2,Issue 1, January 2013

[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. 2009.

[7]Jason J. Haas, Yih-Chun Hu, and Kenneth P. Laberteaux, "Efficient Certificate Revocation List Organization and Distribution," IEEE Journal on selected areas in communications, Vol.29 , No.3, March 2011.

[8] C. Gentry, "Certificate-Based Encryption and the Certificate Revocation Problem," EUROCRYPT: Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques, pp. 272- 293, 2009.

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET