Clustering Based Certificate Revocation Scheme for Malicious Nodes in MANET

Ms.T.R.Panke
* M.B.E.S.College of Engg, Ambajogai,India

Abstract- Certificate revocation is an important security component in mobile ad hoc networks. Owing to their wireless and dynamic nature, MANETs are vulnerable to security attacks from malicious nodes. Certificate revocation mechanisms play an important role in securing a network. When the certificate of a malicious node is revoked, it is denied from all activities and isolated from the network. The main challenge for certificate revocation is to revoke the certificates of malicious nodes promptly and accurately. In this paper, proposed scheme is based upon a clustering-based certificate revocation scheme, which outperforms other techniques in terms of being able to quickly revoke attackers' certificates and recover falsely accused certificates.

Index Terms- mobile Ad Hoc networks, certificate revocation, recovery, clustering

I. INTRODUCTION

Due to advances in wireless communications technologies, Mobile Ad hoc Networks (MANET) has attracted much attention. MANET is a highly flexible network where nodes can freely move and join, with no fixed infrastructure, and thus it is vulnerable to attacks by malicious users. Therefore, ensuring network security is one of the most important issues in MANET. With the increased focus on wireless communications, mobile ad hoc networks (MANETs) are attracting much attention in recent years. MANET is an infrastructure less mobile network formed by a number of self-organized mobile nodes; it is different from traditional networks that require fixed infrastructure. Owing to the absence of infrastructure support, nodes in MANET must be equipped with all aspects of networking functionalities, such as routing and relaying packets, in addition to playing the role of end users.

In MANET, nodes are free to join and leave the network at any time in addition to being independently mobile. Consequently, a mobile ad hoc network is vulnerable to many kinds of malicious attacks, and it is thus difficult to ensure secure communications . Malicious nodes directly threaten the robustness of the network as well as the availability of nodes. Protecting legitimate nodes from malicious attacks must be considered in MANETs. This is achievable through the use of a key management scheme which conveying trust in a public key infrastructure. These certificates are signed by the Certificate Authority (CA) of the network, which is a trusted third party that is responsible for issuing and revoking certificates.

The mechanism performed by the CA [2] plays an important role in enhancing network security. It digitally signs a valid certificate for each node to ensure that nodes can communicate with each other in the network. In such networks, a certificate revocation scheme which invalidates attackers certificates is essential in keeping the network secured. An attacker's certificate can be successfully revoked by the CA if there are enough accusations showing that it is an attacker. However, it is difficult for the CA to determine if an accusation is trustable because malicious nodes can potentially make false accusations. A 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.

II. EXISTING TECHNIQUES

In URSA [1], two neighboring nodes receive their certificates from each other and also exchange certificate information about other nodes that they know. Nodes sharing the same certificate information are regarded as belonging to the same network. In these networks, the certificate of a suspected node can be revoked when the number of accusations against the node exceeds a certain threshold. While URSA does not require any special equipment such as Certificate Authorities (CA), the operational cost is still high.

URSA proposed by Luo *et al*. [5] uses certified tickets which are locally managed in the network to evict nodes. URSA does not use a third-party trust system such as a CA. The tickets of the newly joining nodes are issued by their neighbors. Since there is no centralized authority, the ticket of a malicious node is revoked by the vote of its neighbors. In URSA, each node performs one-hop monitoring, and exchanges monitoring information with its neighbors which allow for malicious nodes to be identified. When the number of votes exceeds a certain threshold, the ticket of the accused node will be successfully revoked. Since nodes cannot communicate with other nodes without valid tickets, revoking a node's ticket implies the isolation of that node.

In contrast to URSA, DICTATE [2] employs a number of CAs to efficiently perform the publication and revocation of certificates. CAs monitor node behavior in order to detect attacks and share the certificate information with each other. If a CA identifies a malicious node, the certificate of the node is revoked by the CA and its information is shared among other CAs, thus resulting in the complete exclusion of the node from the network. However, the deployment of a sufficient number of CAs is not an easy task in MANETs.

In [3], the certificate of a node which has been accused by just one node will be revoked by every node. As a result, this scheme exhibits good performance in terms of promptness and low operating overhead. However, this scheme poses a controversial point that an accuser will be removed from the

network along with the accused node. This approach is fundamentally flawed, and so this scheme cannot be commonly used.

The method proposed in [4] introduces a time session to refresh the certificate information of each node. The accusation count is reset at the end of each session. Therefore, while this scheme is able to mitigate the damage caused by false accusations, the performance can be largely degraded by the increase of malicious nodes.

In the voting based scheme [3], [6], if the number of nodes, which have accused a particular node, exceeds the predefined threshold, the accused node is removed from the network by having its certificate revoked. This scheme takes into account of the false accusations, i.e. each accusation has a different weight according to the accuser's reliability. However, this scheme has two problems, a large amount of operational traffic
and a long revocation time, because the opinion of every node in the network is needed for each node to decide whether to revoke the certificate of the malicious node or not.

III. NODE CLUSTERING

By classifying nodes into clusters, the proposed scheme allows each Cluster Head (CH) to detect false accusation by a Cluster Member (CM) within the cluster. Node clustering provides a means to mitigate false accusations.

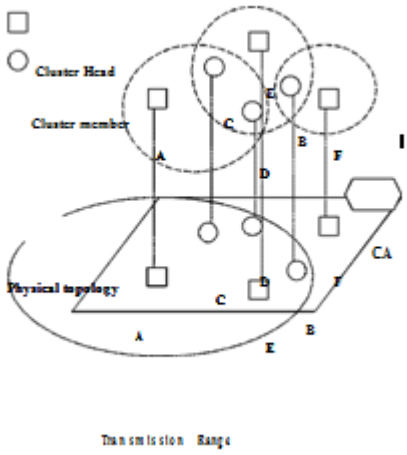

Fig.1. Node clustering

Fig. 1 shows an example of how clusters are constructed in the proposed scheme. While each cluster consists of one CH and CMs lying within the CH's transmission range, some nodes within the transmission area of the CH might not be the member of the cluster and can be the CM of another cluster. For example, in Fig. 1, node B does not belong to the cluster headed by node A while it is located within the transmission area of node A. Only normal nodes having high reliability are allowed to become a CH. Nodes except CHs join the two different clusters of which CHs exist in the transmission range of them. By constructing such clusters, each CH can be aware of false accusations against any CMs since each CH knows which CM executes attacks or not, because all of the attacks by a CM can be detected by any node, of course including the CH, within the transmission range of the CM. The reason why each node except CH belongs to two different clusters is to decrease the risk of having no CH due to dynamic node movement. To maintain clusters, CH and CMs frequently confirm their existence by exchanging messages, i.e., the CH periodically broadcasts CH Hello packets to the CMs within its transmission range, and each CM replies to the CH with the CM Hello packet.

IV. CLUSTERING- BASED CERTIFICATE REVOCATION SCHEME

In this, clustering-based certificate revocation scheme which was originally proposed in [4]. Although a centralized CA manages certificates for all the nodes in the network, cluster construction is decentralized and performed autonomously. Nodes cooperate to 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 belongs to two different clusters in order to provide robustness against changes in topology due to mobility. It should be noted that because the clusters overlap, a node within the communication range of a CH is not necessary part of its cluster.

The aim of using clusters is to enable CHs to detect false accusations. Requests for the 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 most types of attacks, such as flooding attack , black hole attack , wormhole attack and sybil attack , can be detected by any node within the communication range of the attacker. In other words, a CH will be able to detect any attack executed by one of its CMs, implying that a CH can identify whether a CM is malicious or not.

In order for clustering-based certificate revocation to work, CHs must be legitimate. Nodes can be classified into three different categories, normal nodes which are highly trusted, warned nodes with questionable trust, and attacker nodes which cannot be trusted. Only normal nodes are allowed to become CHs and accuse attackers by sending. Detection Packets (ADPs) to the CA. Nodes in the Warning List (WL) cannot become CHs or accuse attackers, but they can still join the network as CMs and communicate without any restrictions. Nodes classified as attackers are considered malicious and completely cut
off from the network. The reliability of each node is determined by the CA as follows.

The CA maintains both a Black List (BL) and a Warning List. When the CA receives an ADP from an accuser, the accused node is regarded as an attacker and is immediately registered in the BL. The BL includes nodes which are classified as attackers and have had their certificates revoked. The accuser of the attacker is then listed in the WL because the accuser might actually be making a false accusation. However, falsely accused nodes will be restored quickly by their CHs. We consider false accusation and false recovery as an act of misbehavior, and define nodes that do such act as misbehaving nodes.

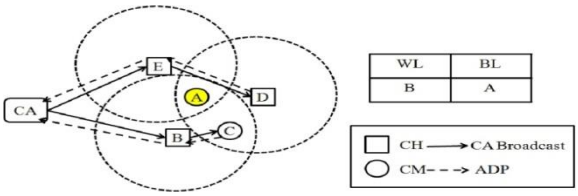

Fig.2. The procedure of certificate revocation

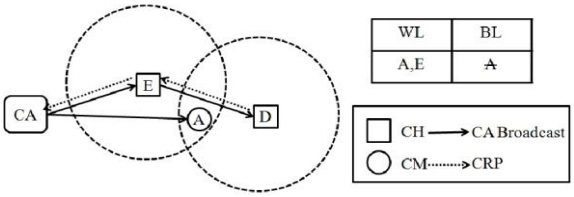

Fig.3. The procedure of certificate recovery

Fig.1 and Fig.2 shows examples of certificate revocation and recovery procedures. As shown in Fig.1, node A is a malicious node and launches attacks on its neighbors, i.e. nodes B, C, D and E. Its neighbors detect the attacks and send ADPs to the CA to accuse node A. Upon receiving the first ADP from node B, the CA puts it into the WL as an accuser and node A into the BL as an attacker. It then broadcasts the information contained in the WL and BL to the entire network. Fig.2 shows the procedure of certificate recovery. When node E and D, which are the CHs of node A, are informed that node A is listed in the BL, if they have never detected any attacks coming from A, the accusation as a false one. They will then send a CRP to the CA to recover node A's certificate. Upon receiving the first arrival CRP from node E, the CA removes the falsely accused node A from the BL, and enlists it into the WL along with node E. After the broadcast of the updated WL and BL, the certificate of node A will be recovered successfully.

V. ADVANTAGES

The proposed certificate revocation scheme for ad hoc networks, that provide some measure of protection against malicious accusation succeeding in causing the revocation of certificates of trustworthy, well-behaving nodes.

VI. RESULTS

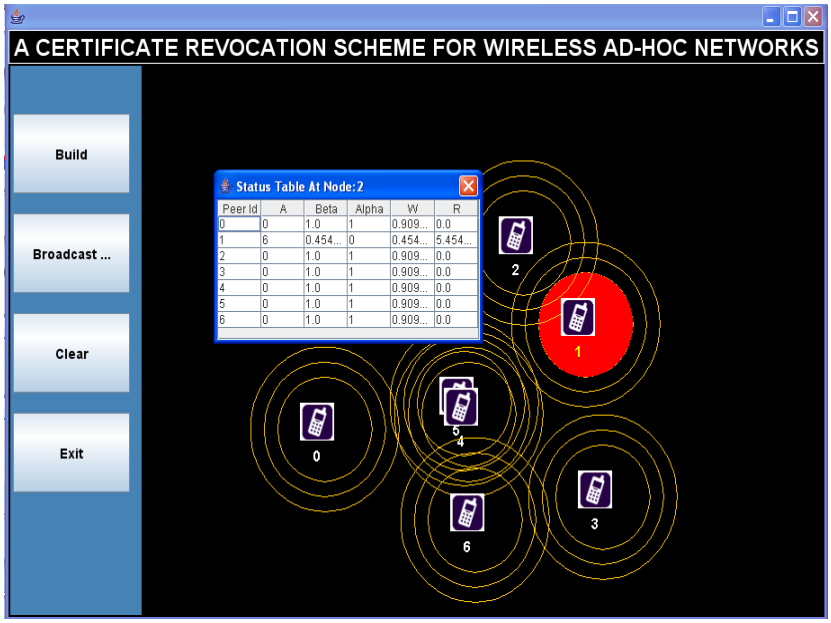

Fig.4.status table of node

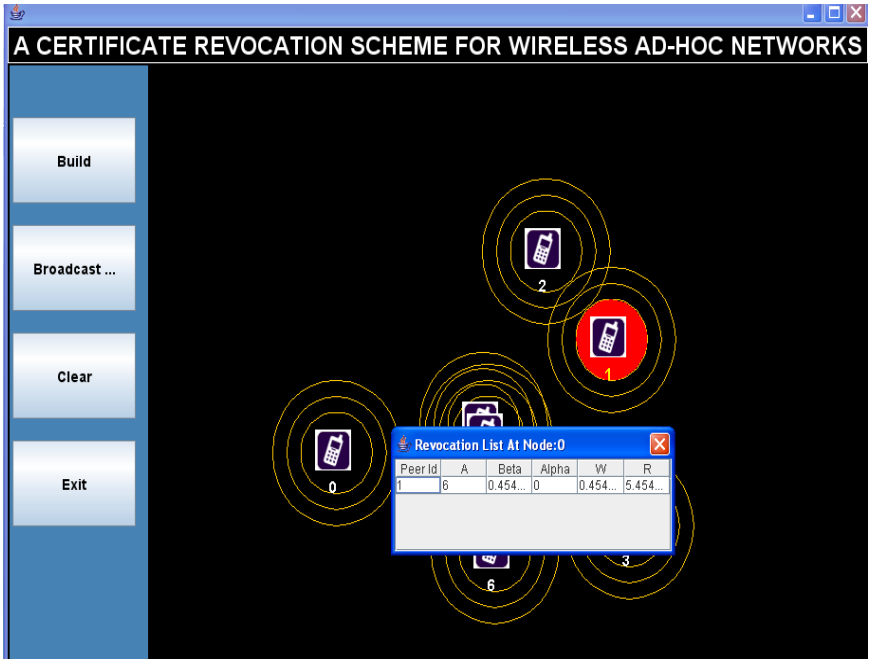

Fig.5.Revocation List

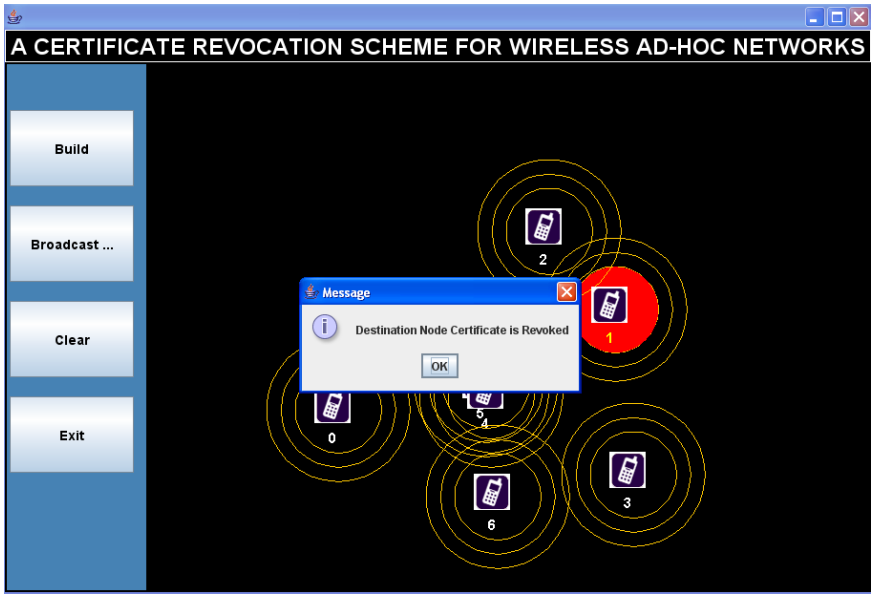

Fig.6.Error Message

The fig.4 shows the certificate of the specified node where the certificate contains the Serial no of certificate,issue time and expiration time etc.The fig.5 shows the dialog box asking for the data to be send for the destination node.Here each node be able to communicate with each other in a secure way.In the fig.6 or results specify the move option at the node which enables the movement one node dynamically to another node.Here the figure shows the node 6 initial position.

VII. CONCLUSION AND FUTURE WORK

In this paper, we have enhanced our previously proposed clustering-based certificate revocation scheme which allows for fast certificate revocation. In order to address the issue of the number of normal nodes being gradually reduced, we have developed a threshold based mechanism to restore the accusation function of nodes in the WL. The effectiveness of our proposed certificate revocation scheme in mobile ad hoc networks has been demonstrated through extensive simulation results**.**

Our future work includes doing further explorations to evaluate our protocol through security analyses and simulations to access its robustness and its cost in terms of overhead and throughput. We intend to present the results of the further investigations in another publication.

REFERENCES

[1] T.Panke,"Review of Certificate Revocation in Mobile Ad Hoc Networks,"International Journal of Advances in Management,Technology & Engineering Sciences,ISSN:2249-7455,vol.II,Issue 6(V),March 2013.

[2] Y.Joshi,T.Panke,"Study of Certificate Revocation in Mobile Ad Hoc Networks,"National Conference Entitled Fostering Management and I.T.for Gen-Next,ISBN:978-81-920972-1-3.

[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] J.Clulow and T. Moore, "Suicide for the Common Good: A New Strategy for Credential Revocation in Self-organizing Systems," ACM SIGOPS Operating Systems Reviews, vol. 40, no. 3, pp.18-21, Jul. 2006.

[5] J.Clulow and T. Moore, "Suicide for the Common Good: A New Strategy for Credential Revocation in Self-organizing Systems," ACM SIGOPS Operating Systems Reviews, vol. 40, no. 3, pp.18-21, Jul. 2006.

[6] H.Chan, V. D. 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, pp.233- 247. Oct.-Dec. 2005.

[7] 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.[6] 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.

AUTHORS

First Author – Ms.T.R.Panke, M.B.E.S.College of Engg, Ambajogai, India, tejupanke@gmail.com, 8149235191