Novel Accuser Of Certificate Revocation In Mobile Adhoc Networks

Ms. Yogini R Joshi
Walchand Institute Of Technology
Solapur,India

Dr. Mrs. Sulabha Apte
Professor, CSE Department,
Walchand Institute of Technology,
Solapur, India.

Abstract

In Mobile Adhoc Network providing secure communication is a big challenge.because MANETs are infrastructureless and unreliable wireless networks.Therefore MANETs are susceptible to security attacks from malicious nodes. Certificate revocation is an important security component in MANETs.In this paper we discuss the Clustering based Certificate revocation scheme.This scheme is used for quick revocation of attacker's certificate and recovery of falsely accused certificates. The limitation of the above scheme is Normal nodes(The nodes which are able to accuse malicious nodes .) are decreases over time.To solve this problem we propose a new method by employing threshold based approach to restore nodes accusation ability.The proposed scheme enhance the effectiveness and efficiency of Clustering based certificate revocation schme.

1.Introduction

Mobile Adhoc network is a highly flexible network where nodes can freely move and join the network .MANETs are infrastructureless network.Therefore Mobile Adhoc networks are susceptible to various security attacks.The various methods have been developed for detecting the attacks from malicious nodes.but only detection and blocking of malicious node is not enough.because attacker can freely move in the network and can launch attack on different nodes. For the security of MANETs the attacker must be immediately removed from the network. Therefore we use certification system. Nodes in the network cannot communicate with each other without a valid certificate. Certificate authority (CA) is used for issuing and revoking certificates. CA digitally signs the valid certificate for each node. The attacker;s certificate successfully revoked by CA if there is enough accuation showing that it is an attacker.when the certificate of malicious node is revoked it is denied from all activities and isolated from the network. In many cases malicious node may make false accusation ,then the question arises in front of CA that the accusation is trustable or not. Therefore the certificate revocation method must be able to distinguish false accusation from valid ones.

2.Existing Techniques

Many Certificate Revocation techniques have been developed for Mobile Adhoc networks.

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.

The scheme proposed by G. Arboit et al. [2], referred to as the voting-based scheme, allows all nodes in the network to vote. As with URSA, no CA exists in the network, and instead each node monitors the behavior of its neighbors. The primary difference from URSA is that nodes vote with variable weight. The weight is calculated from a node's reliability which is derived from its past behavior. The higher its reliability is, the greater its weight will be. The certificate of a suspicious node can be revoked when the sum of the weights of the votes against the node reaches or exceeds a predefined threshold. By doing so, the accuracy of certificate revocation can be improved. However, since all nodes are required to participate during every Vote ,the communication overhead required to exchange voting information is quite high, thus increasing the time needed to revoke the certificate.

J. Clulow et al. [3] proposed the

decentralized suicidebased approach. In this approach, while the certificate revocation can be quickly completed with just an accusation, not only the certificate of the accused node but also accuser's certificate is revoked. In other words, at least one node has to sacrifice itself to remove an attacker from the network. This strategy

dramatically reduces both the time required to evict a node and the communication overhead of the certificate revocation procedures. However, owing to its suicide-based strategy, the application of this approach is limited. Also, the scheme does not provide a mechanism to differentiate falsely accused legitimate nodes from properly accused malicious nodes.

I.Clustering Based Certificate Revocation Scheme

In the Clustering based certificate revocation scheme cluster construction is decentralized and performed autonomously.In the following types of attacks such as Black hole ,flooding,and warm hole attackers ,nodes are assumed to be able to detect an attacker within their transmission range. When nodes join the network ,they are assumed as normal nodes.Nodes are differentiated into three types such as normal nodes which are highly trusted ,warned nodes with questionable trust ,and attacker nodes with no trust. The warned nodes placed in the warning list(WL)and attacker nodes placed in the black list(BL).The certificate of the node which is in the black list is revoked by certified authority(CA), means the node is isolated from network and denied from all activities in the network.The nodes listed in listed in warning list can communicate to other nodes but cannot become a cluster head(CH).
The WL and BL maintained by CA.
After the particular time period the CA broadcast the certificate information to all nodes in the network.In this scheme cluster

construction is decentralized.Each cluster consists of cluster head(CH) with several cluster members(CMs). Each Cluster member belongs to two different clusters.because the network topology changes due to mobility of the network. The CH will be able to detect any attack executed by one of it's cluster member. CH must be legitimate. Only normal nodes are allowed to become CH. The normal nodes accuse attacker by sending the attack detection packet(ADP) to CA.Then CA places the accused node in the black list,and accuser node in the warning list.The certificate of the node which is in black list is revoked by CA.The nodes in WL can communicate with other nodes in network,but cannot become CH. Sometimes the nodes are falsely accused .Cluster Head (CH) can detect the false accusation .

CH send the certificate recovery packet (CRP) to CA.Then CA remove the recoverd node from black list and registered it into warning list.The Cluster head (CH) which send CRP is also placed in warning list.
Following Fig.1 and Fig.2 shows examples of certificate revocation and certificate recovery procedure.

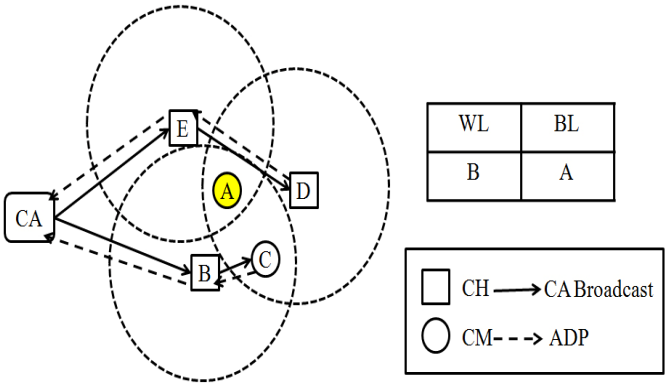

Figure 1. The procedure of certificate revocation

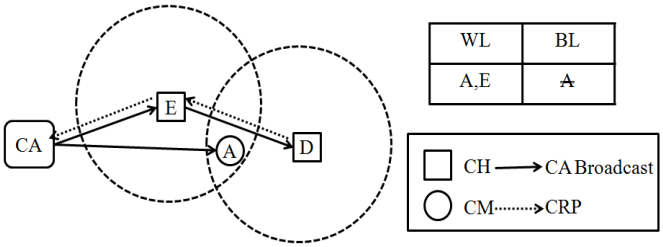

Figure 2. The procedure of certificate

recovery

In Fig.1 node A is malicious node and launches attacks on its neighbours i.e. nodes B,C,D,E. The neighbour send ADP,s to CA to accuse node A. When CA receives first ADP from node B,CA puts it into WL.and node A is registered in BL.The database maintained by CA is updated and CA broadcast the information to the network. Certificate Recovery procedure shown in Fig.2. The CH,s E and D get information that the node A is accused .After long time period if the node E and D never detect the attack from A. They conclude that this accusation is false. Then E and D will send a CRP to CA to recover node A's certificate. When CA receives CRP from E then CA removes A from BL and enlist into the WL along with E.
The advantages of certificate revocation scheme are quick revocation, small overhead, and it resolves the problem of false accusation .But the limitation of the

scheme is ,when the number of malicious nodes increases the number of normal nodes decreases in the network.

3.Proposed Scheme

The clustering based certificate revocation scheme have the following limitation that the normal nodes in the network decreases over time. We propose a method to release nodes from the WL based on a threshold in order to increase the number of normal nodes in network. Nodes in the WL are of two types legitimate nodes and misbehaving nodes. We need to distinguish between

legitimate and misbehaving nodes. In the clustering based approach the CA receives first ADP and ignores other accusation by other nodes against the same accused node. In threshold based approach a counter is assigned to each accused node and CA receives accusation upto the counter equal to k. If the counter equals k ,the accused node is recognized as an attacker then the certificate of that node is revoked. The accuser is considered as legitimate node and it is removed from WL. In this way the no. Of normal nodes increases in the network.

4. DFD Diagram

Fig.3 Fields of profile table

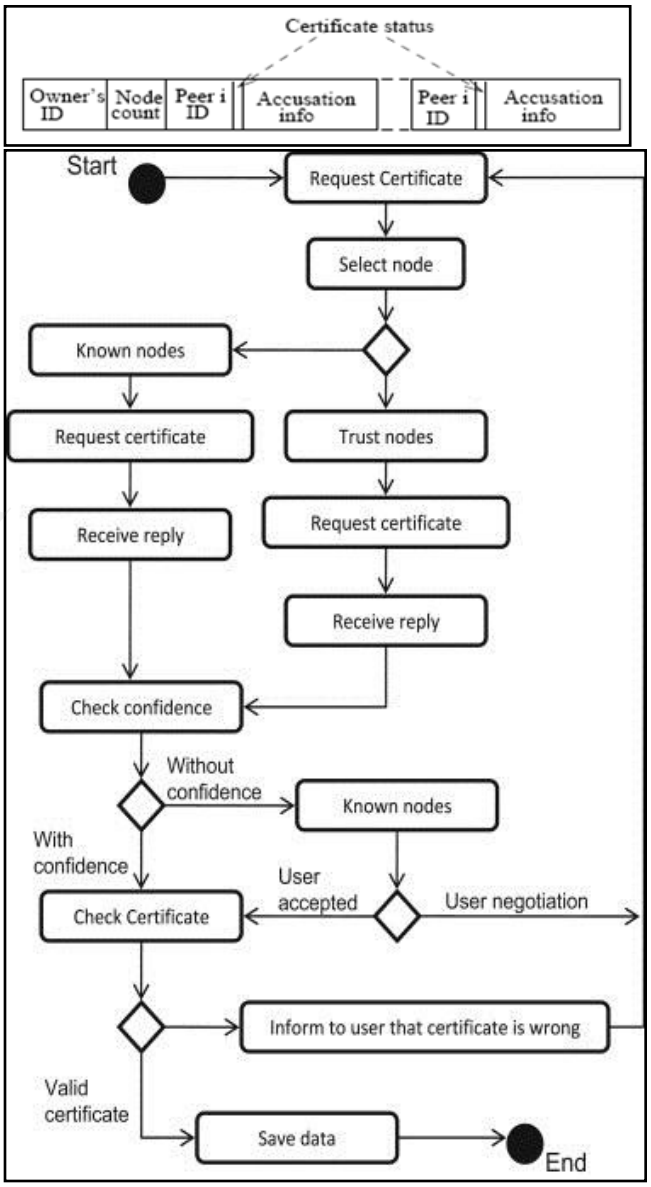

Fig.4 Diagram for certificate issuing

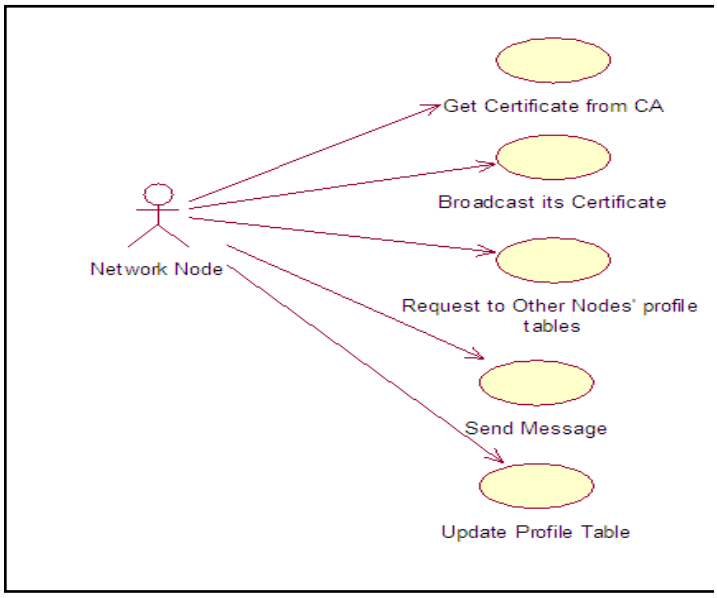

Fig.5 Usecase diagram for network node

5. Conclusion

In this paper, we have enhanced our 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 will 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 will be demonstrated through extensive simulation.

6. References

[1] Wei Liu, Hiroki Nishiyama, Nirwan Ansari, Nei Kato, "A study on Certificate Revocation in Mobile AdHoc Networks" IEEE ICC 2011

[2] K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate revocation to cope with false accusations in mobile ad hoc networks," *Proc. 2010 IEEE 71st Vehicular Technology Conference: VTC2010-Spring*, Taipei, Taiwan, May 16-19, 2010.

[3]F. Nait-Abdesselam, B. Bensaou and T. Taleb, "Detecting and avoiding wormhole attacks in wireless ad hoc networks," IEEE Commun. Mag., vol. 46, no. 4, pp.127-133, Apr. 2008.

[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]R.A. Raja Mahmood and A.I. Khan, "A survey on detecting black hole attack in AODV-based mobile ad hoc networks," Int'l Symp. High Capacity Optical Networks and Enabling Technologies, pp.18-20, Nov.2007.

[6]P. Sakarindr and N. Ansari, "Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless sensor networks," IEEE Wireless Communications, 14(5), pp. 8-20, 2007.

[7]A.M. Hegland, E. Winjum, C. Rong, and P, Spilling, "A survey of key management in ad adhoc networks", IEEE Communications Surveys and Tutorials, vol 8, no. 3, pp. 48-66, 2006.