# Review On Certificate Revocation Of Mobile Ad Hoc Networks

[1]M.Srividya, [2]K.Radhika, [3] D.Jamuna

## ABSTRACT

**Certificate revocation is an important security component in mobile ad hoc networks (MANETs). Owing to their wireless and dynamic nature, MANETs are vulnerable to security attacks from malicious nodes. 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, we build upon our previously proposed scheme, 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. However, owing to a limitation in the schemes certificate accusation and recovery mechanism, the number of nodes capable of accusing malicious nodes decreases over time. This can eventually lead to the case where malicious nodes can no longer be revoked in a timely manner. To solve this problem, we propose a new method to enhance the effectiveness and efficiency of the scheme by employing a threshold based approach to restore a node's accusation ability and to ensure sufficient normal nodes to accuse malicious nodes in MANETs. Extensive simulations show that the new method can effectively improve the performance of certificate revocation.**

**Index terms- mobile ad hoc networks, certificate revocation, recovery, clustering**

## 1. INTRODUCTION

A Wireless Ad Hoc Network is a group of low capacity computing devices(laptops, PDAs etc) connected through wireless links. These devices are generally mobile with frequent location changes. Communication between the devices can be established anywhere, in a decentralized manner with-out the support of an established infrastructure. The purpose of ad hoc networks is to enable the mobile device users to share resources, provide services to each other or simply establish a network for communication and information exchange. Ad hoc networks have a number of applications where infrastructure free communication is required. These applications include emergency relief, military operations, on-demand conferencing and home networking. Like any communication network, the true potential of wireless ad hoc networks cannot be exploited without considering and adequately addressing the security issues.

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 serves as a means of 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 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. Our previous scheme, which is based on a clustering approach, outperforms other techniques in terms of being able to quickly revoke certificates of accused nodes and also to explicitly distinguish false accusations. However, it has a shortcoming in that its performance degrades as the number of detected attacker's increases.

## 2 CERTIFICATE REVOCATION

Any data with a digital signature could be called a certificate. Certificates are tamperevident (modifying
the data makes the signature invalid) and unforgeable (only the holder of the secret, signing key can produce the signature). These properties make certificates useful in conducting secure electronic transactions.

When a certificate is issued, its validity is limited by an expiration date. However, there are circumstances (such as when a private key is revealed, or when a key holder changes affiliation or position) where a certificate must be revoked prior to its expiration date.

Security requirements of wireless ad hoc networks are similar to that of other networks. They can be briefly summarized as follows:

*Access control:* The need to restrict access of network re- sources to legitimate authorized entities.
*Authentication:* Guarantee of the authenticity of the network peers and traffic source; that is, provides some assurance that a given network node is actually who it claims to be, and that any given network traffic actually ordinated from the source it proports to originate from.
*Confidentiality:* Provides assurance that data in its un-obfuscated form will be restricted to legitimate entities that have the authority to access the data.
*Availability:* Network resources should be available to authorized entities without excessive delays.

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.

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 Attack 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.

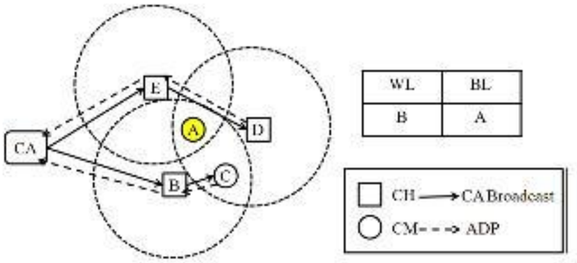

Figure 1. The procedure of certificate revocation

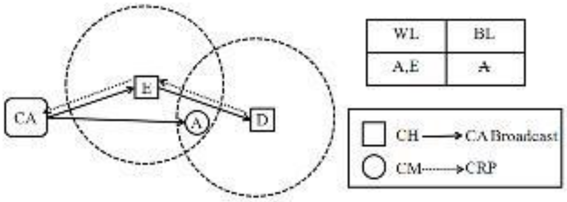

Figure 2. The procedure of certificate recovery

Fig. 1 and Fig. 2 show 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, they will recognize this 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.

## 2.1 CERTIFICATE REVOCATION TREES

Certificate Revocation Trees (CRT) enable the verifier of a certificate to get short proof that the certificate leaves corresponding to a set of statements about certificate serial number X issued by a CA, CAx.The set of statements is produced from the set of re-voked certificates of every CA. It provides the information whether a certificate X is revoked or not (or whether its status is unknown to the CRT issuer).

There are two types of statements: specifying ranges of unknown CAs, and, specifying certificates range of which only the lower certificate is revoked. For instance, if CA1 revoked two certificates, X1 < X2, than one of the statements is:

if CAx = CA1 and X1 _X <X2 then X is

Revoked iff X = v

To produce the CRT, the CRT issuer builds a binary hash tree with leaves corresponding to the above statements. A proof for a certificate status is a path in the hash tree, from the root to the appropriate leaf (statement) specifying for each node on the path the values of its children. The main advantages of CRT over CRL are that the entire CRL is not needed for verifying specific certificate and that a user may hold a succinct proof of the validity of his certificate. The main disadvantage of CRT is in the computational work needed to update the CRT. Any change in the set of revoked certificates may result in re-computation of the entire CRT

## 3 CONCLUSION

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, 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.

## 5.REFERENCES

1.Yi-an Huang and Wenke Lee, A Cooperative Intrusion Detection System for Ad Hoc Networks, in Proceedings of the 1st ACM Workshop on Security of Ad hoc andSensor Networks, Fairfax, Virginia, 2003, pp. 135 –147.

2. Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki Data_integrity.

3.P. Papadimitratos and Z. J. Hass, Secure Routing forMobile Ad Hoc Networks, in Proceedings of SCSCommunication Networks and Distributed SystemsModeling and Simulation Conference (CNDS), San Antonio, TX, January 2002.

M.Srividya Pursuing M.Tech from Jaya Prakash Narayan college of engineering Mahabubnagar, Andrapradesh . Her areas of interest include study in mobile adhoc networks.

K.Radhika(MTECH) working as Associate professor in Jaya Prakash Narayan College of Engineering, mahabubnagar, Andrapradesh. Her areas of interest include Wireless networks, Information Security currently focusing on IP Networks .

Prof.D.Jamuna ,M.Tech, (,Ph.D). Professor & HOD. At Jaya Prakash Narayan College of Engineer ing, mahabub nagar, Andra pradesh. M.Tech. degree in SE from School of Information Technology, JNTU, Hyd and Pursuing Ph.D from Rayalaseema University, Kurnool. Her areas of interest include Wireless networks, Information Security currently focusing on IP Networks