Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

A Survey on Certificate Revocation Schemes in Mobile Adhoc Network

[1]N.Aravinthan and [2]K.Geetha
[1]M.Phil Research Scholar, [2]Assistant Professor
[1,2]Department Of Computer science, Bharathiar University, Coimbatore, TamilNadu, India

Abstract-- Mobile Adhoc NETwork (MANET) has become more popular in recent years because of its features like mobility and deployed nature. But, few natures like wireless and dynamic changes of topology launch different types of attack than the wired network. Hence, security is one of the major concerns should be considered to prevent MANET services from vulnerable attacks due to the presence of malicious nodes. Certificate revocation plays a major role in MANET for providing secure communication by revoking and removing the certificate of malicious nodes. There are various mechanisms developed in certificate revocation for removing malicious nodes from the network in an efficient manner. This paper provides detailed information about different mechanisms used for certificate revocation and compares them based on their output parameters.

Keywords-- *MANET, Certificate Revocation, Malicious Nodes*

I. INTRODUCTION

In MANET, one of the limitations is malicious nodes present in the network. Such nodes can easily corrupt the data in the routing path and finally resulted in malfunctioning of the network operations. Some of the malicious attacks launched in the network corrupted the information that is transmitted among nodes while other attacks might attempt to change the path that they are transmitted to prevent valid node to receive the correct packets. So security is considered as important concern in network topology, routing, and data traffic. Many research works have focused on the security of MANETs.

In Certificate management [1], trust vales are used for protecting services in the network and applications of network. Prevention, Detection, and revocation are the security solutions utilized for certificate management. Process of adding and removing the certificates of attacker nodes is called certification revocation scheme. This revocation scheme depends on voting based and non-voting based mechanism. In voting mechanism, certificate of attacker nodes was revoked by votes given by its non attackerneighboring nodes and in non voting, a given node is considered as attacker with a help of any other node having valid certificate. Thus the certificate of malicious nodes was detected and malicious nodes were removed from the network.

The remaining part of the work consists of following sections: section 2 explains the certificate revocation, section 3 provides the brief survey of the existing certificate revocation methodologies found in the literature. Section 4 concludes our work.

II. CERTIFICATE REVOCATION SCHEME

Certificate revocation is a process through which certificates of normal nodes and malicious nodes can be easily added or eliminated from the network. Certification plays the most significant part in protecting communication over network. Each node in the network has given the certificates by Certificate Authority (CA) and these certificates are enclosed with the digital signature for avoiding forging behaviour of nodes. Certificate issued by CA is tamper proof and it cannot be changed further. When Certificate of malicious node is detected and added to the Certificate Revocation List (CRL). CRL contains digitally signed list that has serial number of revoked certificates provided by CA. However, problem faced by CA is the false accusation. CA is a trusted node which sustains the public keys of all nodes deployed in the networks. It should be noted that, communication between nodes is allowed only with the help of valid digital certificates. So for effective communication, steps involved in certificate revocation are key generation, entity registration, certificate distribution, certificate archiving, certificate expiration and certificate revocation. Stages included in revoking the certificates are accusation of node, certificate verification of accused node and notification about certificate revocation of malicious node [2].

Revocation of certificate can be done by either voting based revocation mechanism or non-voting based revocation mechanism. The mechanism of removing the certificates of malicious attacker node with the help of votes obtained from valid neighbouring nodes is denoted as voting based revocation mechanism. The mechanism of detecting a malicious node through any node with valid certificate is represented as non-voting based revocation mechanism.

Initially, network was created with number of nodes in which both normal nodes and malicious nodes are included. Malicious node initiated attack on nearby nodes. After detecting this attack, accusation packet was forwarded from neighbour nodes of malicious node to CA. On receiving the accusation packet, CA verifies the certificate of accused node and if the accused node is confirmed as malicious node then added it certificate to the CRL. Revocation information was then disseminated to all other nodes for further secure communication. The flow diagram of certificate revocation process is shown in Figure1.

III. LITERATURE SURVEY

HuaqiangXu[3] proposed a scheme to revoke the certificate of malicious nodes in Hybrid MANET. In this approach, voting based mechanism was adapted in revocation process. Then the certificate of the malicious nodes was revoked by considering the weight of accused node based on acceleration strategy. This scheme also recovered the wrongly revoked nodes by utilizing vindication capability. But high accuracy was not obtained when false accusation was not considered. Rajaram Ayyasamy & Palaniswami Subramani[4] utilized shamir's secret sharing model along with their previous three phase scheme that consists of Routing Cum packet Forwarding(RCF) for packet monitoring, certification revival and certification revocation. RCF of packet monitoring detected the malicious nodes in both the routing as well as the packet forwarding in the network. The revocation of certificates of nodes was based on the trust values of each node. However, Flexibility is low while controlling and configuring certificates.

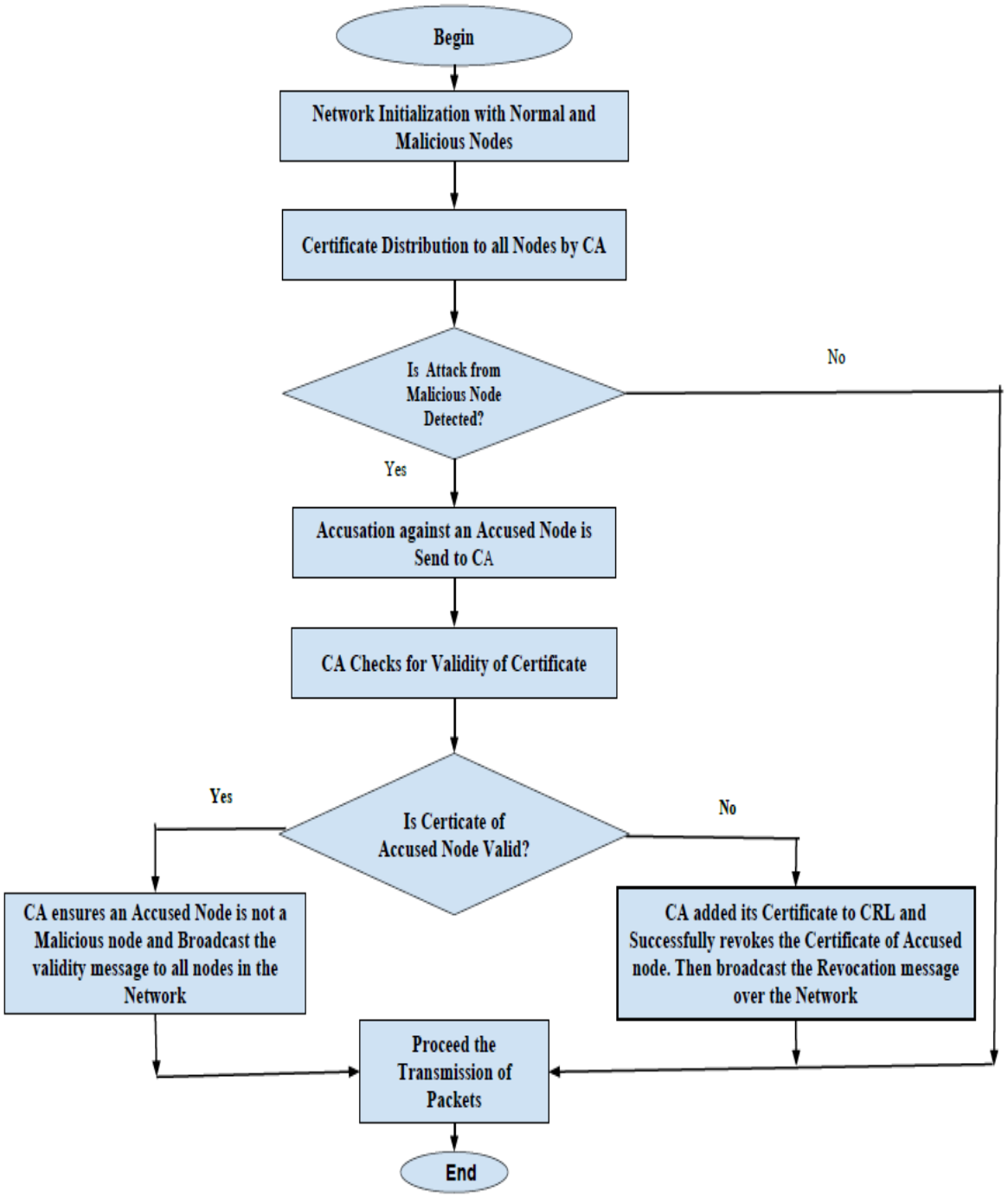

Figure 1: Certificate Revocation Process

Wei Liu et al [5] proposed Cluster-based Certificate Revocation with Vindication Capability(CCRVC) scheme for accurate detection of malicious nodes. In this scheme, cluster head solved the false accusation problem by restoring the falsely revoked nodes to the network. CCRVC revoke the attacker nodes by considering only one accusation from a neighboring node. This scheme minimizes the revocation time. The scheme supports only uniformly distributed mobile nodes. Ambarish A and Gowthamani R[6] developed a certificate revocation scheme which enriched the security level of MANET by Fuzzy Relevance Degree (FRD). This FRD technique chose the cluster head and forms the cluster based on the energyof transferring packets and velocity of nodes. FRD packet structure contains the field of identifier, FRD, level, hops and balance. After selecting the cluster head, traditional certificate revocation mechanism was processed to remove the attacker nodes from the network. This scheme enhanced the overall throughput of MANET.

Archana Devi et. al. [7] developed a scheme for revoking the certificate of malicious nodes from the network. The proposed scheme followed cluster based certificate revocation mechanism in addition with the vindication capability for minimizing the false accusation of nodes. It also improved the network security by adopting the technique based on cryptographic puzzle. The scheme resulted in better accuracy and reliability.Dieynaba Mall et. al. [8] proposed a secure and modified certificate revocation scheme using Public Key Infrastructure (PKI) management. In this modified scheme, each node generated certificate revocation list that consists of accusation information of its neighboring nodes and it was given by the matrix form. Then HEAP protocol was utilized which provides two shared keys for authenticating the transferred message. The advantage of this modified scheme is that, it offers lower overheads.

Kannan and Dinesh [9] introduced a scheme for detecting malicious nodes in MANET based on clustering based certificate revocation. This scheme contains warned list and block list to prevent non malicious nodes. Initially nodes were categorized into clusters and certificates were provided by certificate authority to each node. Based on the threshold based mechanism, nodes were classified into malicious, attacker and non malicious nodes. Then certificate of malicious nodes was revoked by the certificate authority. This scheme shows better result in terms of revocation time, efficiency and reliability. Gowsalyaa et. al.[10] addressed about the problem on MANET due to the presence of malicious and attacker nodes. They have used public key infrastructure based certificate revocation scheme which makes the use of both voting and non-voting based mechanism.In this scheme, Certificate authority provides certificate for each node presented in the cluster along with public key to provide secure communication against attacker nodes in the network. They concluded that their proposed scheme minimized the communication overhead.

Megala and Arunadevi [11] developed a Hybrid Cubes based Certificate Encryption (HCCE) scheme by following three phases such as accusing, verifying and notifying of the nodes. In HCCE, additional information of nodes was combined by identifying the value of encryption key according to the orthogonal latin square. This proposed scheme improved the security level of MANET. But the scheme requires new programs to detect the attacks occurred in the network. Sungwookkim [12] presented weighted votingbased revocation scheme to detect and remove the certificate of malicious nodes from the network. Cluster head sends the accusing message to all nodes in the cluster and each node play a part in voting based mechanism. Cluster head received the votes and forwarded it to the certificate authority. Then the certificate authority removed the certificate of accused node from the network and broadcasted the information to all nodes in the cluster. They concluded that the proposed scheme minimized the false revocation of nodes and found that ther exits a significant improvement in the accuracy of the revocation system. Comparison of Various Certificate Revocation Schemes found in the literature is tabulated in the table 1.

Table 1: Mechanism and parameters of Various Recovation Schemes

Sl.No	Author	Mechanism Used	Parameters
1	Xu H., Wang R., Jia Z	Lightweight certificate revocation scheme, wrong revocation recovery mechanism	Impact of Malicious nodes: Revocation Accuracy= 98.5% Number of accusations: 4 Revocation time: 50 sec
2	Ayyasamy R., Ssubramani P	Shamir's secret sharing model	Based on 100 nodes: Packet delivery Ratio: 0.82 Delay: 13 sec Overhead (packets): 90000
3	Liu W., Nishiyama H., Ansari N., Yang J., Jato N	Cluster based revocation scheme, Vindication mechanism	Number of accusation: CCRVC: 22 Non voting: 76 Revocation time (sec): CCRVC: 40 Non voting: 230
4	Ambarish A., Gowthamani R	Fuzzy Relevance Degree for cluster head selection	Throughput
5	Devi A.T., Petchiappan K., Balasubadra K	CCRVC scheme, cryptographic puzzles technique	Accuracy : 91%
6	Mall D., Konate K., Pathan A.K	PKI, HEAP as authentication scheme	Storage overhead Computational overhead Communication overhead: 185
7	Kannan M., Dinesh E	CCRVC, threshold based mechanism	Packet delivery ratio: 0.95 Revocation time: 30 sec
8	Megala D., Aruna Devi P	CCRVC, Public Key Infrastructure	Packet delivery ratio: 97% Communication overhead: 192
9	Gowsalyaa M., Karthick N., keerthana S., Durga R	Hybrid cubes certificate encryption	Number of accused nodes: 12 Revocation time (sec): 25
10	Kim S	Clustering, weighted voting scheme	For 300 nodes: Revocation accuracy: 95% Normalized revocation time: 60 sec false revocation : 30% malicious nodes revocation: 98%

CONCLUSION

Detecting and removing malicious nodes from the network is the most difficult task in MANET. This paper reviews certificate revocation scheme for the effective elimination of the malicious nodes in MANET. This paper also described about various techniques which includes certificate revocation mechanism. These techniques are compared based on their parameters such as packet delivery ratio, revocation time, overhead, delay and accuracy. The comparison result proved that, weighted voting gaming technique with certificate revocation scheme shows effective result than other existing revocation schemes.

References

[1] Kim S., (2016). Effective certificate revocation scheme based on weighted voting game approach. IET Information Security, 10(4), 180-187.

[2] Attokaren A G. & Mujeebudheen Khan A. I., (2014). Survey on Certificate Revocation Scheme for Mobile Ad Hoc Networks. International Journal of Computer Science and Information Technologies (IJCSIT), 5(3), 3410-3415.

[3] XuH.,Wang R., & Jia Z., (2016). A Lightweight Certificate Revocation Scheme for hybrid Mobile ad hoc Networks. International Journal of Security and Its Applications, 10(1), 287-302.

[4] AyyasamyR. & Subramani P., (2012). An enhanced distributed certificate authorityscheme for authentication in mobile ad hoc networks. Int. Arab J. Inf. Technol., 9(3), 291-298.

[5] Liu W., Nishiyama H., AnsariN.,Yang J. & Jato N., (2013). Cluster-based certificate revocation with vindication capability for mobile ad hoc networks. IEEE transactions on parallel and distributed systems. 24(2), 239-249.

[6] Ambarish A. & Gowthamani R (2014). Secure Cluster Formation and certificate revocation of adversary nodes in mobile adhoc network. International Journal of Innovative Research in computer and communication Engineering. 2(1), 4082-4087.

[7] Devi A.T., Petchiappan K. & Balasubadra K., (2015). Huddle Based Certificate Revocation with Vindication Capability in Large Scale Wireless Networks. International Journal on Applications in Information and Communication Engineering. 1(4), 35-38.

[8] Mall D., Konate K. & Pathan A.K., (2014). SECRET: A Secure and efficient Certificate revocation Scheme for Mobile Ad Hoc Networks. ISBAST.

[9] Kannan M. & Dinesh E., (2014). Improving QoS in Cluster Based Certificate Revocation for Mobile Ad Hoc Network. International Journal of Innovative Research in Science, Engineering and Technology. 3(3), 992-997.

[10] Megala D. & Aruna Devi P., (2014). Secure hybrid cubes certificate encryption revocation with capability for Mobile ad hoc networks. International Journal of advanced research in computer science and software Engineering. 4(12), 633-638.

[11] Gowsalyaa M., Karthick N., Keerthana S., & Durga R., (2014). Certificate Revocation using Public Key Infrastructure for MANET's. . International Journal of advanced research in computer Engineering & Technology. 3(3), 1032-1035.

[12] Kim S., (2016). Effective certificate revocation scheme based on weighted voting game approach. IET Information Security, 10(4), 180-187.