A Survey on Certificate Revocation In Mobile Ad-hoc Networks

Honey mol C.S

M.E Student ,Department of CSE

Fatima Michael College of Engineering & Technology, Madurai

honeymolcs@gmail.com

Abstract-The term MANET (Mobile Ad –hoc Networks) refers to a multi-hop packet based wireless network composed of set of mobile nodes that can communicate and move at same time, without using any kind of fixed wired infrastructure. The wireless and dynamic natures render them more vulnerable to various types of security attacks than the wired networks. The major challenge is to guarantee secure network services, so we use certificate revocation as an important integral component to provide secure network communication. In this paper, a cluster based certificate revocation scheme is present which are build upon our previously proposed scheme, which outperforms other techniques in terms of being able to quickly revoke attacker's certificate and improve falsely accused certificates. The limitation of above scheme is, the number nodes to accuse malicious node decrease over time. To solve the above problem we proposed new method based on threshold to ensure sufficient normal nodes to accuse malicious nodes in MANET.

Keywords: certificate revocation, clustering, certificate authority, certificate recovery, threshhold

1. INTRODUCTION

Mobile Ad-hoc Network is highly flexible network where node can move freely and join the network. Nodes in MANET must contain all the aspects of networking functionalities due to the absence of infrastructure support. MANET is an infrastructure less mobile network formed by a number of mobile nodes [1].The mobile ad-hoc networks are susceptible to various security attacks. Therefore ensuring network security is one of the most critical problem in MANET. Protecting genuine node

from hateful attacks must be considered in MANET which is shown in Fig 1.This is achievable through the use of a key managements scheme which serves as means to provide trust in a public key infrastructure. These certificates are signed by Certificate Authority (CA), which is a third party responsible for issuing and revoking certificates in the networks [3, 4].

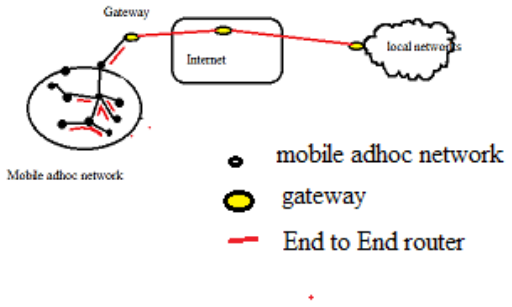

Fig 1: Architecture of mobile ad hoc network

The mechanisms performed by the CA play an important role in enhancing network security. It digitally signs a valid certificate for each node to ensure that node can communicate with each other in the network [5].In such networks, a certificate revocation which invalidates attacker's certificate is important in keeping network secured[6,7]. CA revokes the attacker's node and isolates them from network. However, it is difficult for the CA to determine if an accusation is trustable because malicious nodes can make false accusation [8, 9]. A malicious node will try to remove legitimate node from the network by falsely accusing the as attacker. Therefore false accusation must be taken into account in designing certificate revocation scheme.

2. CERTIFICATE REVOCATION TECHNIQUE

Different types of certificate revocation techniques have been developed for mobile ad-hoc networks.

The most popular method is a simple certificate control approach by using certificate revocation list [CLR] [6] which is managed by a single CA or shared among multiple CAs. A digital certificate which is valid for a certain time period is assigned to each node by the CA. The CA revokes the certificates of accusatory nodes and add them to the CRL.Nodes can be accused by any node with a valid certificate and the updated CRL is broadcasted throughout the entire network.

H. Luo et al. [7] proposed URSA, which uses certified tickets which are locally managed in the network to evict nodes. And it does not use a CA. The tickets of newly joining nodes are issued by their neighbors. In URSA, each node performs one-hop monitoring, and exchanges monitoring information with its neighbors which allows for malicious nodes to be identified. The ticket of the accused node will be successfully revoked when the number of votes exceeds a certain

threshold value. .Since nodes cannot communicate with other nodes without valid tickets, revoking a node's ticket implies the isolation of that node.

The scheme proposed by G. Alboit et al [8], 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 nodes reliability which is derived from its weight will be. The certificate of a suspicious node can be revoked when the sum of the weight of vote against the node reaches or exceeds a predefined threshold.

J. clulow et al [9] proposed the decentralized suicide-based approach. In this approach while the certificate revocation can be quickly completed with just an accusation, the certificates of both accused and accuser's nodes are revoked. In other words at least one node has to scarify itself to remove an attacker from the network. The strategy reduces both the time required to evict a node and the communication overhead of the certificate revocation procedure. 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 node from properly accused malicious nodes.

Park et al. [5] proposed a Cluster-based certificate revocation scheme where nodes are self-organized to form clusters. In this scheme a trusted certification authority is responsible to manage control messages, holding the accuser and accused node in the warning list (WL) and black list (BL) respectively. The certificate of the malicious attacker node can be revoked by a single neighboring node. It also deals with the issue of false accusation that enable falsely accused node to be removed from the black list (BL) by cluster head (CH) .It takes a short time to complete process handling certificate revocation.

Table1.Comparisonbetweencertificate revocation techniques

Author	Title	Merits	Demerits
H. Luo, J. kang, P. Zerfos, S. Lu, and L. Zhang	"URSA: Ubiquitous and Robust Accesses Control for mobile ad-hoc network"	1.No need of CA 2.Robust for false accusation	1.Collusion attacks by multiple malicious attackers
G. Arboit, C. R Davis, C. Crepeu and M. Maheswaran	"A localized certificate revocation scheme for MANET"	1.Improved accuracy	1.Communication overhead is high 2.More time needed to revoke certificate
J. Clulow and T. Moore	"Suicide for the common good: A new strategy for credential revocation in self organizing systems "	1.Reduced communication overhead 2.Reduced time to evict a node	1.No mechanism to differentiate falsely accused legitimate node from properly accused malicious node 2.limited application
K. Park, H. Nishiyama ,N. Ansari, N. Kato	"Certificate Revocation to Cope with False Accusation in MANET "	1.Reduced revocation time 2.Restore falsely accused nodes	1.Decrease in number of normal nodes 2.less accuracy and reliability

3. CLUSTER BASEDCERTIFICATE REVOCATION SCHEME

In this section, we briefly describe our Cluster Based Certificate Revocation scheme which was originally proposed in [5].Although a centralized CA manages the certificates of the entire nodes in the Network; cluster construction is decentralized. Nodes co-operate to form clusters within a network. Each cluster consist of a cluster head(CH) along with several cluster members(CMs) that are located within the communication range of their cluster head as nodes co-operate to form clusters. In order to provide robustness against changes in topology due to mobility as each CM belongs to two different clusters. A

node within the communication range not necessary part of its cluster
as it should be note that because cluster overlaps. Clustering information is never used for routing; it is only used for managing certificates. This provides a clear advantage as it enable the scheme to be used along with any type of routing technologies. The aim of using cluster is to enable CHs to detect false accusation. Request for CA to recover the certificates of falsely accused node can only be made from CH.

In order for the clustering based certificate revocation to work, CHs must be legitimate. In the following types of attacks such as Wormhole [12], black hole [10] and flooding [11] attacker's nodes are assumed to be able to detect an attack within the transmission range. Nodes are assumed to be of three categories; normal nodes highly trustable, warned nodes with questionable trust, attacker node with no trust. The warned nodes placed in Warning list (WL) and attacker node placed in Black list (BL).The certificate of the node which is in black list is revoked by CA and ,means node is isolated from the network and denied from all the activities in network.

The WL and BL maintained by CA. Only normal nodes are allowed to become CH.The normal nodes accuse attacker by sending the Attack detection packets (ADP) to CA. Then CA places the accused node in BL and accuser node in WL. The CA place the accused node in BL and accuser node in WL.The certificates of node which in black list is revoked by CA.The node in warning list can communicate with other nodes, but cannot become CH. Sometimes nodes are falsely accused. The CH can identify the false accusation.

CH sends certificate recovery packet (CRP) to CA.The CA removes the recovered node from black list and places it in warning list. The cluster head which send CRP is also placed in warning list.TheFig.2 and Fig.3 shows example of certificate revocation and certificate recovery procedure.

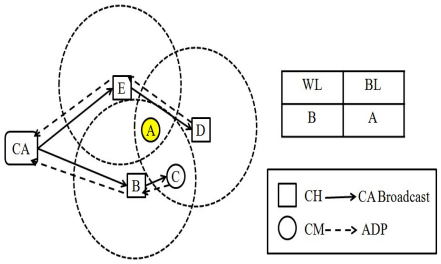

Fig.2.Revoking a node's certificate

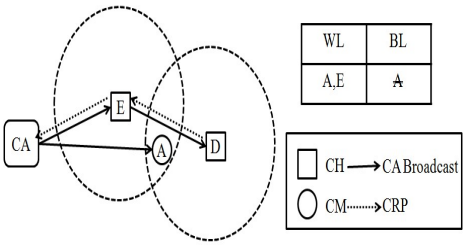

Fig.3 dealing with false accusation

In the fig.2 node A is malicious node and launches attacks on other nodes ie, B, C, D, E. The neighbor sends ADP, s to CA to accuse node A. When CA receives first ADP from node B, CA put it into WL and node A registered in BL. The database maintained by CA is updated and CA broadcast the information to network.

In fig.3 certificate revocation procedure is shown. The cluster heads E and D get information that node A is accused. After a long period of time E and D never detect attack from A. They conclude that accusation is false. Then C and D send CRP to CA to recover node A's certificate. When CA receives CRP from node E then CA removes A from BL and place in WL along with E.

The advantages of certificate revocation are quick revocation, reduced overhead and it resolves the problem of false accusation. But the limitation of the scheme is, when the number of malicious nodes increase it decreases the number of normal nodes in the network. This degrades the system performance.

4. PROPOSED SCHEME

The cluster-based certificate revocation has following limitation that the normal node in network decreases overtime. We propose a method to release nodes from WL based on a threshold in order to increase the number of normal nodes.

Nodes in WL are of two types' legitimate nodes and misbehaving nodes. We need to distinguish between legitimate and misbehaving nodes. In clustering based approach the CA receives first ADP and ignores other accusation by other nodes against the same node. In the proposed scheme we use threshold based approach to release legitimate nodes from warning list [WL].Thus the number of normal nodes can be increased in the network.

5. CONCLUSION

Mobile ad hoc network has gained much attention in the recent year due to mobility and ease of deployment. In this paper, we have enhanced our proposed cluster based certificate revocation scheme which allow fast certificate revocation and reduced false accusation. In order to develop the efficiency of certificate revocation scheme, we have developed a threshold based mechanism to ensure sufficient normal nodes to accuse malicious nodes in the MANET.

REFERENCE:

[1].Yang, H. Luo, F. Ye, S .Lu, and L.Zhang"Security in mobile ad hoc networks: challenges and solutions", IEEE Wireless communication, 11(1), pp.38-47, feb.2004

[2].Sakarindr. P, Ansari. N, Security service is group communications over wireless infrastructure, mobile ad hoc and wireless sensor network. IEEE wireless communications 2007;

[3].Hegland .Am, Winjium .E, Rong .C, Spilling .P A Survey of key management in Ad hoc networks. IEEEcommunication survey and tutorials 2006;

[4].Zhou L, Hass ZJ Securing ad hoc networks.IEEE Networks Magazine 1999;

[5].Park K, Nishiyama H, Ansari N, Kato N. Certificate revocation to cope with false accusation in mobile ad hoc networks.proc.2010 IEEE 71st Vehicular Technology Conference;

[6].Micali .S .Efficient Certificate Revocation, Massachusetts institute of technology, Cambridge, MA, 1996

[7].Luo H, Kong J, Zerfos P,Lu S, Zhang L. URSA: Ubiquitous and Robust Access Control for Mobile Ad hoc Network 2008;

[8].Arboit G, Crepeau C, Davis C R, Maheshwaran M.A Localized Certificate Revocation Scheme for Mobile Ad hoc Networks.2008;

[9].Clulow .J, Moore .T. Suicide for Common Good: A new strategy for Credential Revocation in Self organized System. ACMSIGOPS Operating Systems Reviews 2006;

[10].Raja Mahmood RA, Khan AL.A survey on detecting black hole attack in AODV-based mobile ad hoc network.Int'1 symp. High Capacity Optical Networks and Enabling Technologies Nov 2007;

[11].Yi P, Dai z, zhong Y, Zhang S.Resisting Flooding Attacks in mobile ad hoc network.Int'1 conf. Information Technology , coding and computing 2005;

[12].Nait-Abdesselam F, Bensaon B. Taleb T. Detecting and Avoiding worm hole attacks in wireless ad hoc networks .IEEE commun. May 2008;

[13].Newsome J.shi E. Song D. Pemig A. The Sybil Attack in Sensor Network .Analysis and Defence information processing in sensor networks 2004;

[14].Scalable Network Technologies: Qualnet http://www.scalablenetwork.com

[15].Camp T, Boleng J, Davies V. The survey of mobility models of mobile ad hoc networks, search –wireless Communication and mobile computing 2002;

[16].H.Yang, J .Shu, X .Meng and S.Lu," SCAN: Self Organized Networks", IEEE J.Selected Area in commu.vol 24 .no.2, pp.261-273, Feb 2006.

