ijecs open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 10 October, 2014 Page No. 8620-8624

An Efficient certificate Revocation Method For Mobile Ad Hoc Network

Yogini R.Joshi[1], Dr.Mrs.Sulabha Apte[2]

[1]Walchand Institute Of Techonology,Solapur.University
Solapur, Maharashtra,India
Joshiyogini89@gmail.com

[2] Professor, CSE Department,Walchand Institute Of Techonology,
Solapur University,Solapur,Maharashtra,India.
Headcsewit@gmail.com

ABSTRACT: Mobile adhoc networks (MANETs) have attracted much attention due to their mobility and ease of deployment. However the wireless and dynamic natures render them more vulnerable to various types of security attacks than the wired networks. Certificate Revocation is an important integral component to secure network communications. The main challenge for certificate revocation is to revoke the certificates of malicious nodes promptly and accurately. When the certificate of malicious node is revoked,it is denied from all activities and isolated from network. In this paper we build upon previously proposed scheme,a clustering based certificate revocation scheme.This scheme is used for quick revocation of attackers certificates and recovery of falsely accused certificates .
To overcome the limitation of the Clustering based certificate revocation scheme we use node release method .To identify the malicious nodes the zkp (zero knowledge protocol) is used.Extensive simulation show that the new method can effectively improve the performance of Certificate Revocation.

Keywords: Warn List, White List, Block List, Certificate Revocation, Certificate Recovery

1. INTRODUCTION

A mobile adhoc network is a self-organized wireless network which consists of mobile devices such as laptops, cellphones ,and Personal Digital Assistants(PDAs),which can freely move in the network. In MANET nodes can join and leave the network freely. Therefore the dynamic nature of MANETs expose them more vulnerable to various types of security attacks than the wired networks.The attacks in MANETs are divided into two major types .These are Internal attacks and External attacks.Internal attacks are directly leads to the attacks on nodes present in the network.and links interface between them.This type of attacks may broadcast wrong type of routing information to other nodes .External attacks try to cause congestion in the network,denial of services(DOS),and
advertising wrong routing information In this paper we discuss the improved cluster based certificate revocation method.When the normal node enter in the network the valid certificate assigns to that node by Certificate Authority(CA). CA is trusted third party that is responsible for issuing and revoking certificates.Then the node sent a CH-discovery packet.
If the node get response it becomes cluster member of that cluster. If the node does not get any response it becomes cluster head of that cluster. Detecting and revoking the certificates of malicious nodes promptly
and accurately is very important for securing network. To find out attacker nodes we use zero knowledge protocol . The cluster based certificate revocation scheme has some limitation. The normal nodes in the network decreases over time.To overcome this limitation we use a node release method.

2. RELATED WORK

Several 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 a Certificate Revocation List (CRL) [7] which is

managed by a single CA or shared among multiple CAs. URSA proposed by H. Luo et al. [8] 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.

The scheme proposed by G.Arboit et al. [9], referred to as the voting-based scheme, allows all nodes in the network to vote. In the voting based scheme [10], 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.

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.J.Clulow et al.[11] proposed the decentralized suicide based 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.

The method proposed in [12] 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. 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.

[13] Explains the procedure of revoking malicious Certificates to revoke a malicious attacker's certificate, there is need to consider three stages accusing, verifying, and notifying. The revocation procedure begins at detecting the presence of attacks from the attacker node, The false accusation of a malicious node against a legitimate node to the CA, will degrade the accuracy and robustness of our scheme. To address this problem, one of the aims of constructing clusters is to enable the CH to detect false accusation and restore the falsely accused node within its cluster.

3. ZERO KNOWLEDGE PROTOCOL

Zero-knowledge protocol [14][15] is an interactive method between two parties so that one (the prover) can prove to another (the verifier) that a statement is true, without revealing anything other than the veracity of the statement. A ZKP must satisfy the following three properties.

1) Completeness: If the statement is true, the honest verifier will be convinced of this fact by an honest prover.

2) Soundness: If the statement is false, no cheating prover can convince the honest verifier that it is true, except with a certain small probability called soundness error.

3) Zero-knowledge: If the statement is true, no cheating verifier learns anything other than the fact in the statement. In zero-knowledge protocol, the entire proof for "the statement is true" is split into two parts, say parts and . The prover and the verifier play several rounds of a game. In each round, the prover arranges so that he can prove either of the two parts and, as he has no prior knowledge of which one will be asked for. The verifier randomly chooses one of the two parts and asks the prover to prove the chosen one in that specific round. Authentication systems motivates all the research of zero knowledge proofs in which prover wants to prove its identity to a verifier through some secrete information but never wants that the second party to get anything about this secret this known as zero knowledge proof. For identification, keys are exchange and other basics cryptographic operations are mainly allowed by zero knowledge protocol. ZKP is an interactive proof system which involve node P node V. P plays prover role where as v as verifier [16].

ZKP: Proof of identity of node

1) CA that is trusted third party generates a random number N to be used as modulus. This modulus is a product of two large primes.

2) CA provides secrete key to all nodes present in the network and at verification CA sends secret key S^2 mod N to CH.

3) When node want to communicate then it discovers CH after discovering CH, CH sends R^2 mod N to that node and gives challenge for proving itself (node).

4) After accepting challenge of CH, node send RS mod N to CH, then it verifies whether $(RS \bmod N)^2 \bmod N = (R^2 \bmod N * S^2 \bmod N) \bmod N$ Where R,N are random numbers and S is the secret key. Then it is considered as normal node otherwise it is malicious [18].

4. IMPROVED CERTIFICATE REVOCATION METHOD

In this section, we enhances certificate revocation scheme which is proposed in [19].Network consisting of Certificate Authority, Cluster Heads and nodes.

To solve the problem mentioned in clustering based certificate revocation scheme, the node release method is proposed to release nodes from the WL based on a threshold in order to increase the number of normal nodes in the network. Nodes in the WL are not only legitimate nodes but also misbehaving nodes. If misbehaving nodes are released, they may continue to falsely accuse other nodes. Therefore, we need to be able to distinguish between legitimate and

misbehaving nodes to only release the legitimate nodes from the WL.

4.1 Working of Certificate Authority

When CH want to join the network it request for the secret key to the CA ,then CA response secret key that is S^2 mod N to the CH and after that CH joins the network by getting certificate. At the time of packet sending if any node is found as a malicious node then CA revokes the certificate of malicious node and also certificate recovery is done by CA.

4.2 Working of Cluster Head

CA issues certificates to Cluster Members (CM) then CM discover CH after getting discover message from CM, CH responses hello discover message to CM. when there is need to send packets CH broadcasts R^2 mod N to all CM and gives challenge to prove its identity. After accepting challenge it sends RS mod N to CH. If it is malicious node after referring ZKP algorithm then CH sends attack detection message to CA.

4.3 Certificate Revocation and Recovery

The CA maintains both a Black List 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. This is in contrast to more serious behavior such as conducting active attacks. When the CA receives a CRP sent by a CH to request a node to be recovered from the BL, the recovered node is removed from the BL and registered in the WL. At the same time, the CH which sent this packet is also placed in the WL. Since this will cause the CH to lose its credentials, the cluster topology will need to be reconstructed. This conservative strategy is designed to cope with collusion attacks where a CH works to falsely recover other malicious nodes listed in the BL. Since all nodes are initially classified as normal nodes upon joining the network, nodes with malevolent intentions also have a chance to become CHs and run false recovery. However, by adopting this conservative strategy, we can minimize the damage caused by collusion attacks. It should be noted that when the CA receives multiple ADPs or CRPs against the same target.

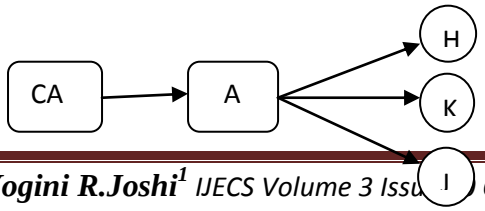


Fig 1.Network Consisting Certificate Authority and other normal nodes.

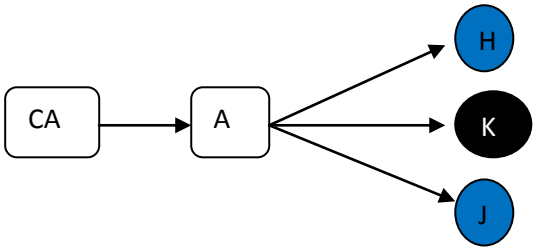
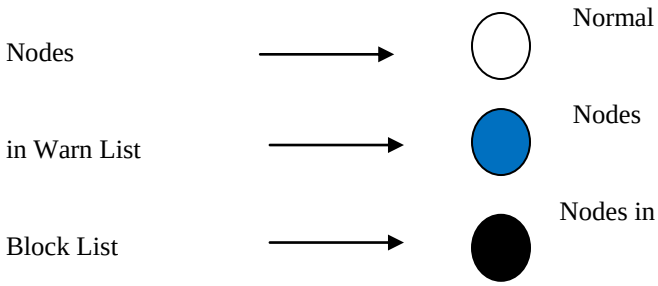


Fig 2.Certificate Revocation



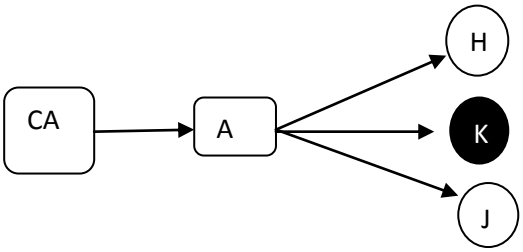


Fig. 3 Certificate Recovery

Fig 1.shows the network consisting Certificate Authority and other normal nodes.Fig 2 and Fig 3 shows examples of certificate revocation and recovery.Here CA Broadcasts messages to all nodes.In Fig 1 A,H.K,J are found as normal nodes.But in Fig 2 node K launches attacks on H,J that is detected by both of nodes H,J.So,H,J are placed into Warn List and malicious node K is placed into Block List, by

which certificate revocation of malicious node K is done.At last nodes H and J are released from Warn List and placed into White List,due to which normal nodes are increased.Here certificate revocation scheme is enhanced that is described in [19].The false accusers are detected and placed into Block List and normal nodes are released from Warn List

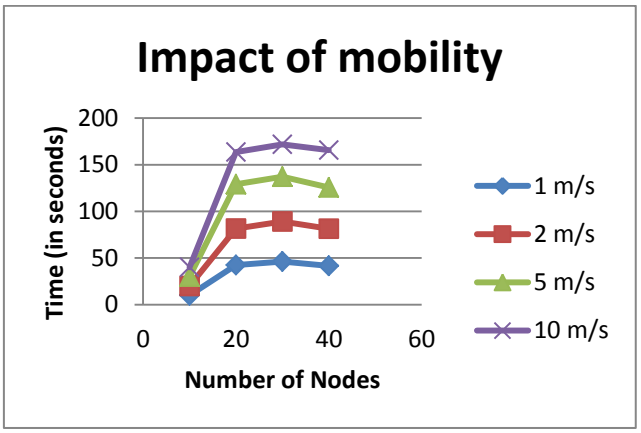


Fig.4 Impact of Mobility

X-axis=detection time of malicious nodes

Y-axis=number of nodes

Speed=1 m/s,2m/s,5m/s,10 m/s

To evaluate the detection performance of the scheme, we studied the mobility on the detection time. Fig 4 shows the detection time as the mobility changes. In this simulation threshold is equal to 2 is used and mobility is set to be 1m/s,2m/s,5m/s and 10m/s .From this results, the detection time reduces as the node mobility increases.

5. CONCLUSION

In this paper, we have improved the 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 develop a node release method to restore the accusation function of nodes in the WL.

6. REFERENCES

[1] A. Mohammed and A.Zuriati,"Performance Comparisons of AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment," European Journal of Scientific research, vol .32, no.3, p.p.430-443, 2009.

[2] S.Mutlu and G.Yilmaz,"A Distributed Cooperative Trust Based Intrusion Detection Framework MANETs",the seventh International Conference on Networking and Services (ICNS) pp 292 to 298,2011.

[3] M.Ilyas "The Handbook of Ad Hoc Wireless Networks".

[4] A.Mishra,"Security and Quality of Service in Ad Hoc Wireless Networks",ISBN-13978-0-521-87824-1 Handbook.

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

[6] L.Zhou and I.J.Haas,"Securing ad hoc networks",IEEE Network Magazine,13(6),pp.24-30,1999.

[7] S.Micali, "Efficient certificate revocation," Massachusetts institute of technology, Cambridge, MA, 1996.

[8] 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.

[9] G. Arboit, C.Crepeau et al., "A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks,"Ad Hoc Network, vol. 6, no. 1, pp. 17-31, Jan. 2008.

[10] C. Crepeau and C.R. Davis, "A Certificate Revocation Scheme for Wireless Ad Hoc Networks," Proc. of ACM Workshop Security of Ad Hoc and Sensor Networks, 2003.

[11] J. Clulow and T. Moore, "Suicide for the Common Good: A Strategy for Credential Revocation in Self-organizing Systems,"ACMSIGOPS Operating Systems Reviews, vol. 40, no. 3, pp.18-21, Jul.2.

[12] H.Chan, V. D. Gligor et al., "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.

[13] W.Liu and N.Ansari"Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks "IEEE Transactions on parallel And Distributed systems,vol.24,no.2,Feb.2013.

[14] Zero-Knowledge Proof. [Online]. Available: http://en.wikipedia.org/wiki/Zero-knowledge_proof

[15] S. Goldwasser, J.Lagarias et al.,"Cryptology and computaional number theory," in Proc.Symp. Appl. Math., 1989, pp. 89–114.

[16] J.Binder,H.Peter,"zero knowledge proofs of Identify for Ad Hoc Wireless Networks An In-Depth Study,TechnicalReport",2003.http://www.cs.rit.edu/jsb7384/zkp-survey.pdf

[17] G.Simari,"A Primer on Zero Knowledge Protocols", Departamento de Ciencias e Ingeniaria de la Computacion

[18] K.Park,H.Nishiyama et al.,"certificate revocation to cope with false accusations in mobile ad hoc networks," proc.2010 IEEE 71st Vehicular Taipei,Taiwan,may 16-19,2010.

[19] W.Liu,H.Nishiyam et al.,"A Study on Certificate Revocation in Mobile Ad Hoc Networks,"IEEE ICC 2011.