Improved Certificate Revocation Method in Mobile Ad Hoc Network

T.R. Panke
MBES College of Engg.
Ambajogai
Maharashtra, India

B.M.Patil
MBES College of Engg.
Ambajogai
Maharashtra, India

ABSTRACT

The mobile Ad Hoc networks (MANETs) having wireless and dynamic nature. MANETs are more susceptible to security attacks rather than wired networks. So they are vulnerable to security attacks from malicious node due to which it is important to detect malicious nodes to avoid attacks. In this paper certificate Authority (CA) provides it's secret key to all nodes (normal).When node want to send data to other nodes Cluster Head (CH) broadcast R^2mod N to all nodes and it gives challenge to that node whether it sending same data, if it sends RS mod N to CH with its secrete key which is provided by CA, then CH compares its data with itself data. If it is same, then it considers it is as a normal node otherwise as malicious node. Here CA should be legitimate. Finally if node is found as a malicious then revocation of certificate is done for that malicious node and other normal nodes are released due to which the number of normal nodes will increase in mobile network and it get secured from susceptible attacks.

General *Terms*

Mobile Ad hoc Network (MANET),Zero Knowledge Protocol, Certificate Revocation, Certificate Recovery.

Keywords

Warn List, White List, Block List

1. INTRODUCTION

Arbiter topologies are formed by self configuring system of mobile routers which linked by wireless link called as MANET. The mobility of such routers organized as arbitrarily; due to which wireless topology networks alter rapidly [1].Wired networks are more resistive than MANET to various kinds of security attacks. In such wireless network, attacks make intrusion from all possible loopholes to reach at any node. The method of identifying such affected node is very complicated [2].MANETs are vulnerable to various attacks from inside same network and outside different networks.

1.1 Internal Attacks

In MANET, several different types of attacks that cause threat, due to their dynamic nature, each type of attack is different from another. Among them some are active and others are passive. Active attacks may be internal or external. The internal type of attacks launches attack inside of MANET, so it is dangerous when the node is considered as a trusted node at beginning .They directly leads to the attacks on nodes present in the network. It may broadcast wrong type of routing information to other nodes [3].

1.2 External Attacks

External attacks try to cause congestion in the network, Denial of Services (DoS) [4].Some external attacks are modification attacks, dropping attacks, fabrication attacks and timing attacks.

Attacker directly threatens the availability and robustness of nodes. So, there is important issue to protect legitimate nodes from malicious nodes. This is achievable through the use of key management in which public key, secrete key is shared between the Certificate Authority (CA) and other nodes. CA signs certificates of nodes presents in the network. CA [5][6] plays an important role in enhancing the 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 type of network CA invalids the attacker certificate for keeping network secured. If there are much of accusers showing that it is an attacker,then attacker's certificate can be revoked. But ,it is not possible to determine, is it accusations are false or true.So,there is need to take it into account the issue of false accusations.

2. RELATED WORK

There are different developments in techniques of certificate revocation for mobile Ad Hoc networks. The most popular method is simple certificate control approach by using technique of certificate revocation list (CRL) [7],which is managed by single CA or shared among multiple CA's.The certified tickets which are locally managed within the network force affected nodes to move out proposed by URSA of H.Luo.et al. [8].

Instead of using CA,URSA uses certified tickets of newly joining nodes by their neighbours.The vote of neighbors having responsibility for revoking tickets of malicious nodes. This voting based scheme by G.arboit et al. [9] allows all networks to vote and it depends on ticket situation. As rule in voting based scheme [10],the number of nodes, which have accused a particular node,goes beyond predefined threshold value, then revocation of certificate is performed for that accused node and the accused node is removed from the network. This scheme consider as false accusation case, which concludes that each accusation has different weight according to the accusers reliability. In this scheme, each node gives it's opinion about whether the certificate revocation of malicious node is done or not. So it takes much of revocation time and also face the problem of large amount of operational traffic.

There is no existence of CA in the network as like URSA.So each node monitors the behavior of its neighbors and weight is calculated from node's reliability which is derived from its past behavior, the difference is only that nodes vote with variable weight from URSA ,J. clulow et al. [11] proposed the decentralized suicide based approach, In such type of certificate revocation scheme revocation is done with accused as well as accusers nodes means here at least one legitimate node has to be sacrifice itself to remove malicious node from network.

The method [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.

4.1 Working of CA

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 4.2 Working of CH

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

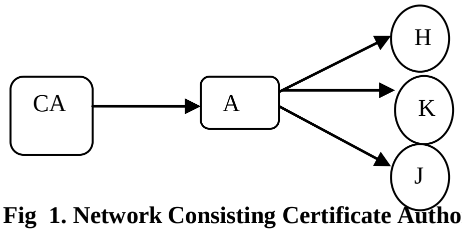

Fig 1. Network Consisting Certificate Authority and other normal nodes.

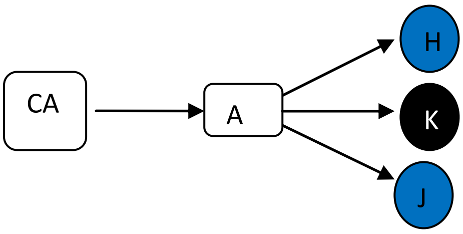

Fig 2. Certificate Revocation

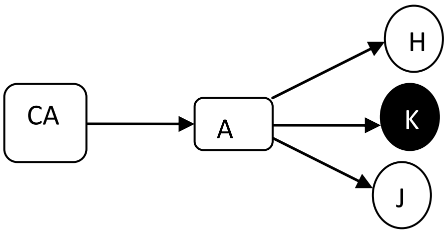

Fig 3. Certificate Recovery

○ → Normal Nodes

🔵 → Nodes in Warn List

● → Nodes in Block List

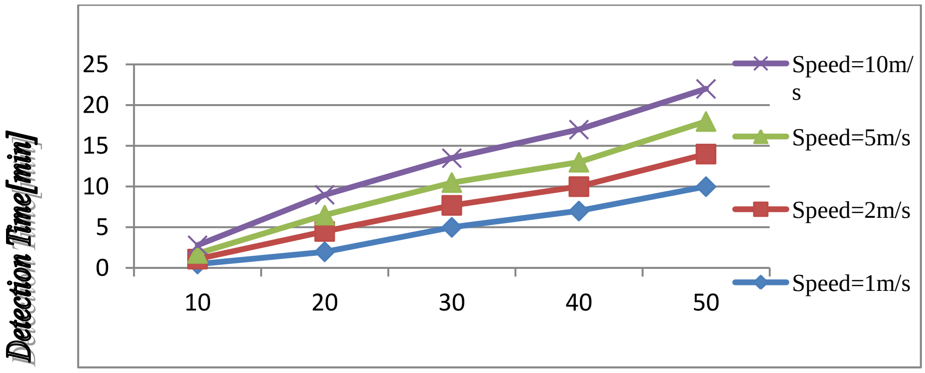

Fig 4. Impact of mobility

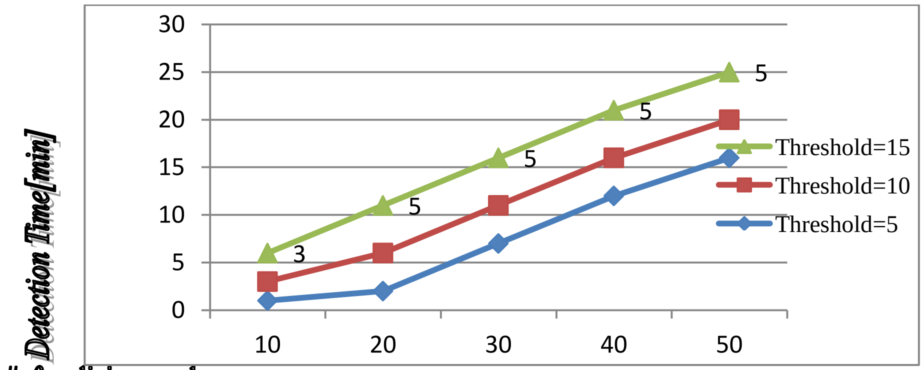

Fig 5. Impact of Threshold

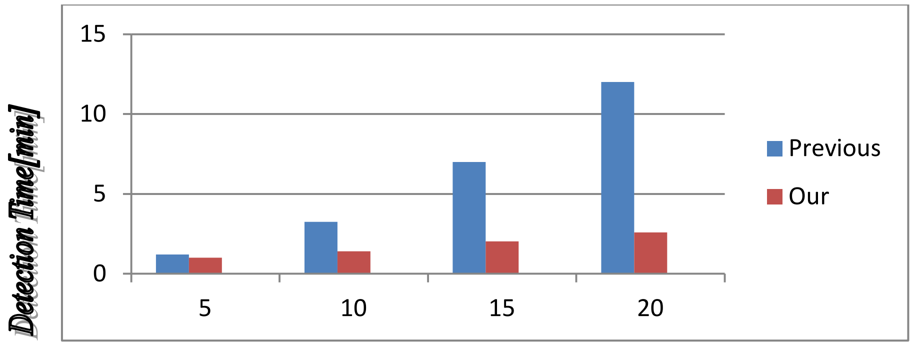

Fig 6. Previous method versus Our method

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.

5. EVALUATION

In this section, simulation results for our method proposed. For this results, Java language is used,50 normal nodes are used,10-50 malicious nodes are used.

5.1 Impact of mobility

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.

5.2 Impact of Threshold

The simulation measures the impact of the threshold value on the detection performance as shown in Fig 5.Here threshold values are considered as 5,10,15 having constant movement at 10m/s in the mobile network.As shown in Fig 5,when threshold becomes large,the detection time increases.

5.3 The detection performance

Fig 9. Shows comparative results of previous method in which nodes in Warn List are not released versus our method.For this result we have taken 20 normal nodes and malicious nodes are changes as 5,10,15,10.As number of malicious nodes are increases detection time varies fastly in previous method but there is just slight change in detection time of our method , also whatever the nodes present in Warn List are released after certificate revocation of malicious node.

6. CONCLUSION AND FUTURE SCOPE

In this paper, we have improved certificate revocation method which maximizes the normal nodes. In this method, the nodes which are present in Warn List are released and the nodes which are present in Block List are removed from the network. Due to which normal nodes becomes large and malicious nodes reduced and from this method false accusers minimized. By using ZKP algorithm we can find out critical malicious attacks in organizations. Also in less time by detecting malicious nodes major harm can be reduced.

7. 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”, Department de Ciencias e Ingeniaria de la Computacion

[18] K.Park,H.Nishiyama et al.,”certificatess 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.