ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Efficient Method for Secure Transmission from Malicious Nodes through Certificate Authentication

M.L.Vijin Stephi[1] and Dr.B.Latha[2]

PG Student, M.E.Computer Science and Engineering, Sri Sairam Engineering College, Chennai-44, Tamilnadu, India[1]

Professor, Department of CSE, Sri Sairam Engineering College, Chennai-44, Tamilnadu, India[2]

ABSTRACT– The main reason for switching from wired network to wireless is the dynamic nature of the nodes. Since the nodes in the MANET have the capability of moving, there is a high possibility of violating the security of the network. The certificate verification involves maintaining secure connections against spoofing and invalid certificates; and the certificate validation examines the certificates to check the recipient's identity. In this paper we proposed a scheme called certificate revocation to prevent the network from malicious attacks. If the certificate of the malicious node is revoked, then it is impossible to communicate with any other nodes in the network by the malicious node. By doing so, it is possible to have Cluster-to-Cluster communication in a secure manner.

KEY WORDS--- Cluster-based routing protocol, Certificate Revocation, Certificate Verification and Validation, MANET, security, Cluster-to-Cluster;

I.INTRODUCTION

Mobile Ad hoc Networks (MANETs) are a kind of wireless ad hoc network. It is a self-configuring network of mobile devices and does not need any infrastructure. This type of mobile network is formed by a number of self-organized mobile nodes such as cell phones, palm handheld computers, iPods, etc. These devices can act as both routers and end users. The reason for using MANET is it does not need any infrastructure support. So it is not assured that all the nodes in the network are trusted. It has all the functionalities of traditional network such as seamless interaction, neighbor discovery, data routing abilities. It provides flexible network architecture so that it can able to provide communication in the case of the limited connectivity range and resource constraints. It enables fast establishment of networks and using the service discovery protocol each node finds its neighbor node to transmit the packet. The MANET architecture is shown in the figure 1

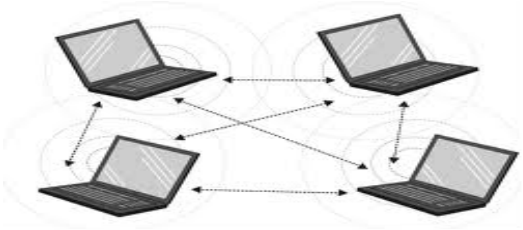

Fig 1 Architecture of MANET

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Each device in MANET is free to join, free to move independently in any direction and then leave the network at any time. Due to the dynamic nature MANET is vulnerable to any kind of attacks. If any intermediate node that does not transmit the receiving packet to its neighbor or it sends many numbers of acknowledgements for a single received packet, then this type of node is considered as a malicious node. This node violates the security of the network. Protecting legitimate nodes in the network from malicious attacks must be considered. To improve security certificate revocation scheme is used and is completely based on public key infrastructure (PKI). This scheme enhances the security and robustness of the network.

Certificate is a certificate provided by the Trusted Authority (TA) which makes the mobile node that joins in the network authenticated. Any node that wants to communicate with other nodes in the network has to get the certificate from the Trusted Authority. Without the certificate it cannot able to communicate with other nodes in the network. Similarly each node can transmit packet to the nodes which are in the transmission range.

II. RELATED WORK

For mobile ad hoc networks many types of certificate revocation techniques have been developed. The simplest technique is Certificate Revocation List (CRL) [1]. In this technique, the list is managed by single CA or it can be shared by multiple CAs. Each node in the network can be assigned with a digital signature which is valid for a particular time period.CA revokes the certificate of the malicious nodes and puts them in the CRL. The information about the list of nodes in the CRL is broadcasted to all the nodes in the network.

URSA technique [2] does not support any third party system such as CA to issue a certificate for authentication. The nodes get their certificate from their neighborhood nodes to join in the network. It gets votes either from the neighborhood node or from all the nodes in the network to decide whether the particular node is accused or not. This type of voting does not address false accusation and makes the network overhead higher. Such a technique is called voting-based certificate revocation.

Another approach that comes under non-Voting-based scheme is Suicide for common good [3]. In this technique CA is responsible for managing the certificates of all the nodes which are joining in the network. Here the accusing node sacrifices itself to remove an attacker node from the network. The main drawback in this approach is it does not differentiate the falsely accused node from the legitimate malicious attackers.

III. PROPOSED WORK

Cluster-based Certificate Revocation scheme [4] is used to revoke the certificate of the accused node to prevent the network from the attack. To find the accused node, the nodes in the network are grouped into several clusters. The process of clustering is done by using the Cluster- based Routing Protocol (CBRP). Each cluster in the network has a head called Cluster Head (CH) and the other nodes within the cluster are called as Cluster Members (CMs). Cluster Members should be in the transmission range of the Cluster Head. Authentication is done by the Trusted Authority and is also called as Certificate Authority (CA). The clustered network is shown in figure 2.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

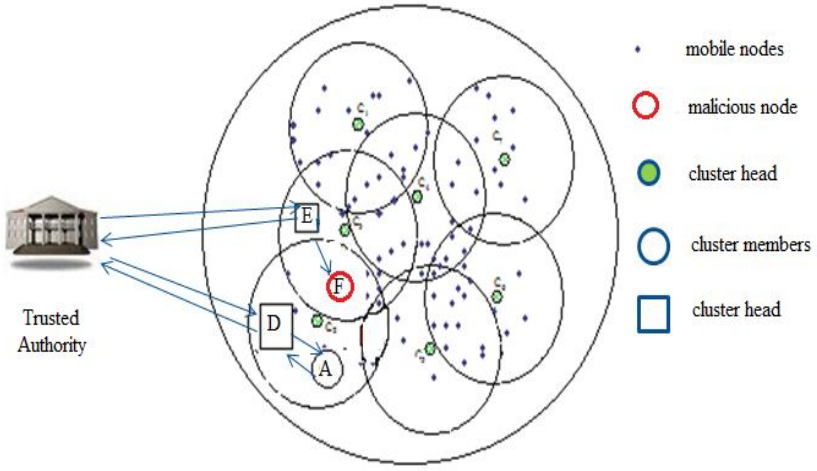

Fig 2 Clustered Networks

It is possible to detect the falsely accused node using the CH. The CH is selected based on either by getting votes from the nodes in its transmission range or by considering the information like packet handling rate, how many packets it has transmitted already and its energy. The former technique increases the overhead in the network and there is a chance of losing packet; so it is not preferred and the latter technique has the advantage over voting based scheme. It does not need any packet transmission to vote and hence reduces the network traffic in the network.

To make revocation process success and quicker, it needs Warned List (WL), Black List (BL). The WL is used to hold the accusing nodes and the BL is used to hold the accused nodes.CA generates certificate and send to all CHs. All CHs generate their own master key. CH sends its master key to its members within the cluster. By using the master key of the corresponding CH, all CMs generate subordinate keys. The master key is split into n subordinate keys; where n is the number of CMs. The subordinate key should be matched with the master key of its CH. If both are not matched, they should not able to communicate with each other. The entire process is shown in the figure 3.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

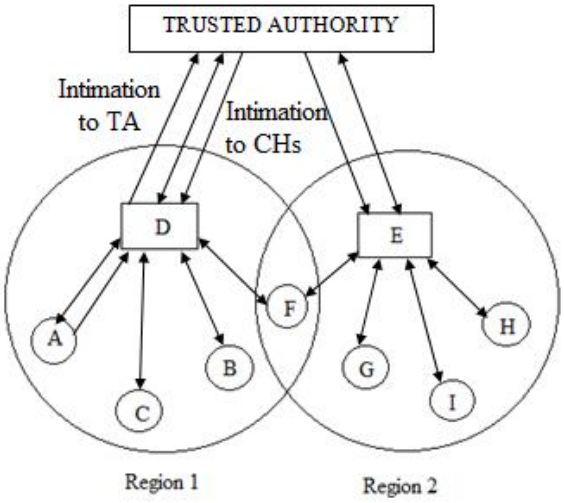

Fig 3 Architecture

Content of table after forwarding to all CHs

Warned List	Black List
A	F

Content of table after concluding the malicious node

Warned List	Black List
	F

It is possible to implement cluster-to-cluster communication or group-to-group transmission. In general, different cluster heads have different keys. To communicate these two cluster heads, they should be matched. Generally they do not match. To make these two keys matched, advanced hashing function method is used.

Certificate verification is an important tool which is used to protect the secure connections from spoofing and invalid certificates. Spoofing is an attack in which the attacker node transmits packets with the source address field containing an address of a legitimate node which has valid certificate to transfer; similarly any attacker node without valid certificate can send unwanted packets to the various nodes in the network to violate security. Such kinds of attacks can be avoided by certificate verification process.

Certificate Validation examines the certificate of the recipient's identity. This prevents the network from unwanted packet transfer from legitimate node to the malicious node and thereby can improve the security of MANET.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

IV. IMPLEMENTATION

The CA provides certificate to each node in the network. If there is any accused node in the network, then it will not transmit the original packet from the source to the destination. To make the transmission secure, the certificate of the attacker node should be revoked.

The revocation process involves three stages - accusing, verifying and notifying. If the accused node is found, its certificate is verified for its certificate. If the certificate is invalid, it is revoked. At last the notification is sent to all the nodes through the cluster heads in the network except to the one which is the malicious. After that the WL, BL are updated for denoting the revocation process. If the node is falsely accused, then it is removed from the black list and is kept in the warned list.

The virtual implementation of this paper is shown using Network Simulator (NS2.34) and Fedora Operating System. The implementation of this technique is shown in the following figures. Each node in the Mobile Ad Hoc Network transmits Hello packets to the neighborhood nodes to determine the active links.

The existing system of voting based mechanisms has many disadvantages. This can be illustrated in the figure 4. There may be a loss of packets while electing for cluster head and there may be a chance of selecting malicious node as a cluster head. It also increased the communication overhead and increased revocation time.

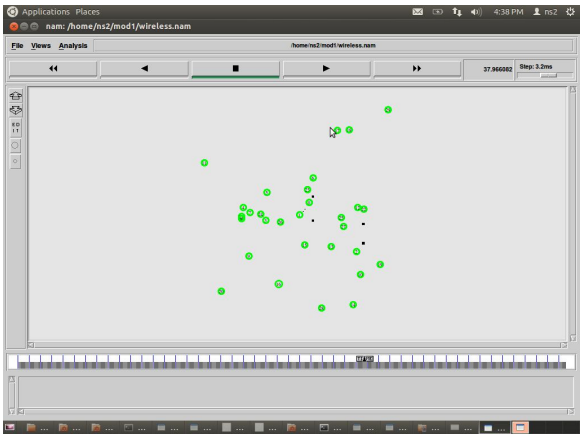

Fig 4 Packet loss in voting-based scheme

After both certificate verification and validations, the Cluster Heads are selected for secure communication among the nodes in MANET. This is shown in figure 5

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

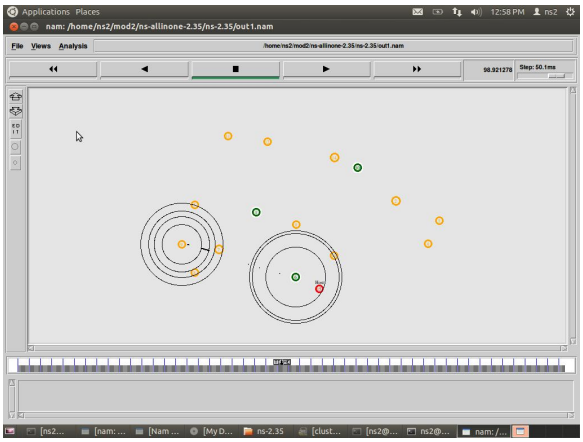

Fig 5 Secure communication through CH

V. CONCLUSION

In this paper we have overcome the demerits of the existing voting-based certificate revocation by revoking the certificate of the malicious node by forming clusters in the network, which reduces the network traffic. Similarly, the time taken to perform certificate revocation is reduced in this proposed technique when compared with the time taken in the existing voting- based technique. It increases the reliability and the accuracy of the network. Group-to-group transmission is achieved. The effectiveness of the cluster based technique has been experimented using network simulator.

REFERENCES

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

[2]H.Luo,J.Kong,P.Zerfos,S.Lu, and 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.

[3]J.Clulow and T.Moore,"Suicide for the Common Good:A new strategy for Credential Revocation in Self-organizing Systems,"ACMSIGOPS Operating Systems Reviews, vol.40,no.3,pp.18-21,Jul.2006.

[4]Wei Liu,Hiroki Nishiyama,Nirwan Ansari,Jie Yang,Nei Kato,"Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks",IEEE Transactions On Parallel And Distributed Systems,Vol.24,No.2, February 2013.

[5]H.Yang, H.Luo, F.Ye, S.Lu,and L.Zhang, "Security in Mobile Ad Hoc Networks: Challenging and Solutions," IEEE Wireless Comm.,vol.11, no.1,pp.38-47, Feb.2004.

[6]P.Sakarindr and N.Ansari,"Security Services in Group Communications Over Wireless Infrastructure, Mobile Ad Hoc,and Wireless Sensor Networks," IEEE Wireless Comm., vol. 14, no.5, pp.8-20,Oct.2007.

[7]B.Kannhavong, H.Nakayama, A.Jamalipour, Y.Nemoto, and N.Kato," A Survey of Routing Attacks in MANET," IEEE Wireless Comm. Magazine, vol. 58, no. 5, pp.2471-2481, June 2009.

[8]G.Arboit, C.Crepeau, C.R. Davis, and M.Maheswaran, "A Localized Certificate Revocation Scheme for Mobile Ad hoc Networks," Ad Hoc Network, vol.6, no.1,pp.17-31, Jan.2008.