International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 3, Issue 4, July-August 2014 **ISSN 2278-6856**

Simulation of Clustering Based Certificate Revocation in MANET's

Preeti T[1] and Parikshit Hegde[2]
[1], [2]Department of Computer Science & Engineering
B.V.B.College of Engineering & Technology,
Hubli, India.

Abstract: ***With increased focus on wireless communications, mobile ad hoc networks (MANETs) are attracting much attention in recent years. MANET is an infrastructure less mobile network formed by a number of self organized mobile nodes which is different from traditional networks that has a fixed infrastructure. Certificate revocation is a major security component in mobile ad hoc networks. Because of their wireless and dynamic nature, MANETs are vulnerable to security attacks from malicious nodes. Certificate revocation mechanism plays an important role in securing a network. When the certificate of a malicious node is revoked, it is denied from all activities and isolated from the network. The main challenge for certificate revocation is to revoke the certificates of malicious nodes promptly and accurately. In this project we will simulate the certificate revocation and recovery technique using Clustering method.***

Keywords: MANET, Certificate Revocation, Malicious node.

1. Introduction

Mobile ad hoc networks (MANETs) are autonomous collection of mobile nodes which communicate over relatively bandwidth constrained wireless links. MANETs are self-organizing and adaptive they can therefore form and de-form on-the-fly without the need for any system administration.The main problem in MANET is security. Certificate revocation mechanism plays an important role in securing a network. When the certificate of a malicious node is revoked, it is denied from all activities and isolated from the network. The main challenge for certificate revocation is to revoke the certificates of malicious nodes promptly and accurately.

2. LITERATURE REVIEW

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) [2] 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 suspicious nodes and adds 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.URSA proposed by H. Luo et al. [3] 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 neighbours. Since there is no centralized authority, the ticket of a malicious node is revoked by the vote of its neighbours. In URSA, each node performs one-hop monitoring, and exchanges monitoring information with its neighbours which allow for malicious nodes to be identified. When the number of votes exceeds a certain threshold, the ticket of the accused node will be successfully revoked. Since nodes cannot communicate with other nodes without valid tickets, revoking a node's ticket implies the isolation of that node. Although URSA is robust for false accusation attacks, there is still a remaining issue in coping with collusion attacks by multiple malicious attackers.The scheme proposed by G. Arboit et al. [4], 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 behaviour of its neighbours. 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 behaviour. The higher its reliability is, the greater its weight will be. The certificate of a suspicious node can be revoked when the sum of the weights of the votes against the node reaches or exceeds a predefined threshold. By doing so, the accuracy of certificate revocation can be improved. However, since all nodes are required to participate during every vote, the communication overhead required to exchange voting information is quite high, thus increasing the time needed to revoke the certificate.J. Clulow et al. [5] proposed the decentralizedSuicide 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. This strategy dramatically reduces both the time required to evict a node and the communication overhead of the certificate revocation procedures. 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 nodes from properly accused malicious nodes.

3. CLUSTERING BASED CERTIFICATE REVOCATION

In this section, we briefly describe about clusteringbased certificate revocation scheme. A centralized CA manages certificates for all the nodes in the network. Cluster construction is decentralizedand performed autonomously. Nodes cooperate to form clusters and each cluster consists of a Cluster Head (CH) along with several Cluster Members (CMs) that are located within the communication range of their CH.The advantages of formation of clusters are:

• Cluster members need not communicate directly with the Base Station , but can directly communicate with Cluster Head. Hence this will reduce the network traffic to the base station.

• The bandwidth requirement is reduced because the number of certificates transmitted to Base station is less.

• The speed of transmission is very quick.

First the distance of each node from CA is calculated using Euclidian distance formula. Then a node is selected as Cluster Head for each cluster if it has the shortest distance to Certification Authority. The details of each node like the distance to CA, energy, Cluster to which it belongs are all displayed in the DataGrid table. The malicious node is revoked from the network based on certain conditions.

4. NEW PROPOSED SCHEME

4.1 Simulation Environment

In this section, we discuss about simulation of our proposed scheme using Visual Studio 2008. The purpose of using this IDE is that we can conduct simulation dynamically.

A. Simulation Setup

Table 1: Simulation Parameters

Parameter	Value
Number of nodes	Based on User's input.
Mobility Model	Random-Waypoint
Node placement	Random
Routing Protocol	Modified AODV
Pause Time	5 seconds
Simulation Time	Continuous
Transmission Range	550 m

B.Modules for Simulation

There are three modules for Simulation.

- Module 1- Creation of Network Topology.
- Module 2- Cluster formation and Cluster Head Selection.
- Module 3 - Eliminating Malicious Node from the network and moving a random node in the network.

Module 1: Creation of Network Topology

In this module, the user is allowed to dynamically enter the number of nodes based on is/her requirement. Once the number of nodes is entered and the create topology button is clicked, then a network is created with the number of nodes specified.

Module 2: Cluster formation and Cluster Head Selection.

In this module, we have considered four clusters for cluster formation in the network. Minimum cluster formed is 1 and maximum number of clusters formed is 4. Cluster area is predefined.

In our technique, first cluster is formed and then nodesare placed in the clusters. The formation of the cluster is done using Random function. The number of nodes to be placed in each cluster is based on the range predefined for each cluster. Timer is an object in .NET framework. A timer is set to 5 seconds and is initially enabled to false. After 5 seconds timer is set to true and the Cluster Heads are selected for each cluster. Different colors are used to identify the Cluster Heads in respective Clusters.

Module 3: Removing malicious node from the network and movement of a random node in the network

In this module, we have used three timers for the automatic working of the simulation. There are two Data Grids for the display of the details about cluster node, distance of each node from Base Station, Malicious node etc.Following are the formats of the Data Grids.

Node	Energy	Base Station	Cluster	Malicious

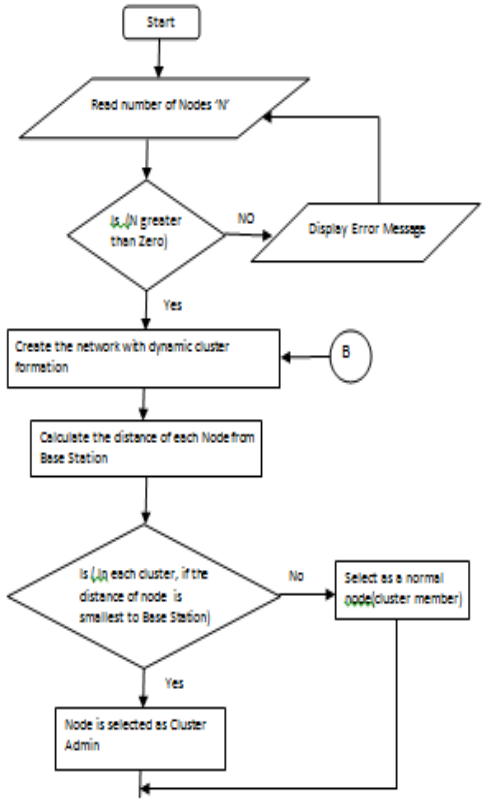
Fig 1: Clusters and respective Node Details

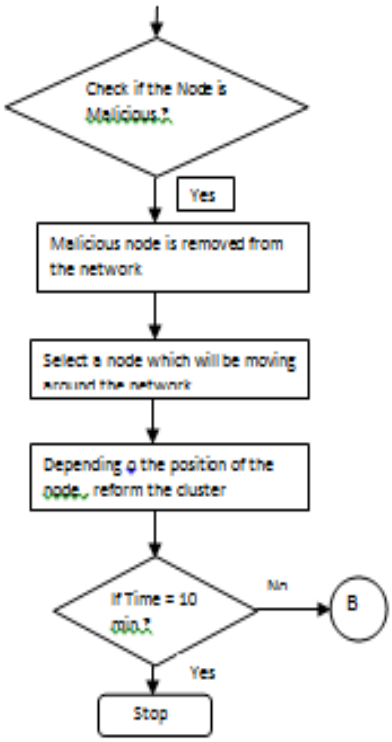
Cluster	Number of Nodes

Fig 2: Clusters Information

First the network topology is created. Then after certain time the cluster heads for each cluster are selected based on the distance of the node from the Base Station. The smallest the distance of node to Base Station in the cluster, then that node is selected as Cluster Head. Then after that we remove the malicious node from the network and using certain conditions a random node is selected and moved in the network.

C.Flowchart





D.Screen Shots of Simulation

Fig 3: Creation of Network

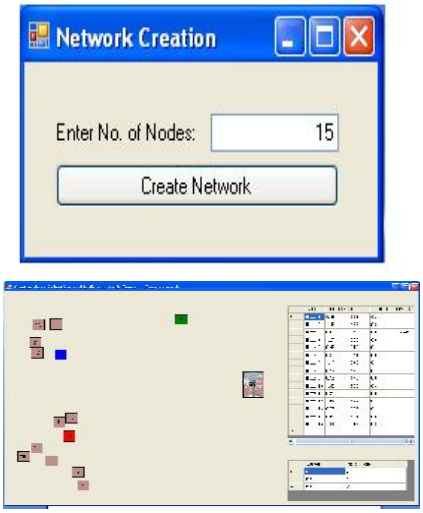


Fig 4: Cluster Head formation and Removal of Malicious Node from Network

5. CONCLUSION AND FUTURE WORK

In this paper, we have used an Integrated Development Environment (IDE) and have successfully simulated Clustering based certificate revocation in MANET's using Microsoft Visual Studio 2008 rather than the routine network simulator tools like NS2, Qualnet etc. We have used this IDE as the conceptualization becomes simple because of its dynamic nature.

In our future work, we will work on developing an application for Clustering based certificate revocation in MANET's.

References

[1] V. Anil Kumar, K.Praveen Kumar Rao, E.Prasad, N.Gowtham Kumar, "Clustering Based Certificate Revocation in Mobile Adhoc Networks" , International Journal of Computer Science and Management Research Vol 2 Issue 1, pp. 1228-1233, January 2013.

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

[3] 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.

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

[5] 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.

[6] Cluster based certification revocation and vindication capability for mobile ad hoc networks, Wei Liu, Student Member , IEEE , Hiroki Nishiyama, Member , IEEE,Nirwan Ansari, Fellow, IEEE, Jie Yang, and Nei Kato, Senior Member , IEEE.

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

AUTHORS

Preeti T has received B.E. degree in Information Science and Engineering from B.V.B.College of Engineering and Technology in 2004. She has served as Lecturer in the Department of Computer Science & Engineering since 2004.She is currently pursuing her 4th semester M.Tech Program in Computer Science.

Parikshit Hegde has received B.E. degree in Computer Science and Engineering from R.V..College of Engineering and Technology, Bengaluru in 2005. Completed his M.Tech Program from Siddaganga Institute of Technology, Tumkur in 2009. Presently working as Asst Professor in the Department of Computer Science & Engineering and has teaching experience of nine years.