Implementing Cryptographic Technique in Cluster Based Environment for Secure Mobile Adhoc Networks

Kiruba Priyadharshini.P1, L.R.Priya2, Dr.Ruba Soundar.K3

1,2,3 Department of Communication Systems, Francis Xavier Engineering College,Tirunelveli-03.

ABSTRACT

Implementation of security in Mobile Adhoc Networks is a primary concern, since mobile nodes launch attacks to disturb network communication. Though Mobile Adhoc Networks have greater attraction due to their mobility, dynamic topology and ease of deployment, they are vulnerable to more threats. Certificate management is one of the security solutions to provide network security so that secure network communication can be established and thereby removing the certificate of nodes which are launching attacks on neighbourhood. To prevent nodes from such attacks, various types of certificate revocation schemes have been proposed. One among the scheme is Cluster based certificate revocation with vindication capability. In this scheme, warned nodes are recovered to improve the reliability of certificate revocation process. Threshold-based mechanism is also proposed in order to enhance the accuracy and thereby assessing and vindicating the warned nodes as legitimate nodes or not, before recovering the warned nodes. Both numerical and simulation analysis are done and their performances were evaluated. The proposed certificate revocation scheme is effective and efficient in revoking the certificates of malicious attacker nodes, thereby reducing the time taken to revocate the certificate of attacker mode, also improves the accuracy and reliability of certificate revocation process.

Keywords: Certificate Authority (CA), Certificate Revocation (CR), Cluster Head (CH), Cluster Member (CM), Mobile Adhoc Network (MANET).

I. INTRODUCTION

Mobile Adhoc Network is a self configurable, autonomous and self maintaining network which receives much attention. But protected communication cannot be established between moving nodes in a hostile environment since it is an open network [2]. So necessary security solution needs to be provided such as Prevention, Detection and Revocation. Revocation is nothing but Certificate Revocation that means the certificate of a node is removed and that particular node is removed, so that it cannot participate in its network activities.

Various types of Certificate Revocation methods have been proposed to avoid vulnerability of security threats, they are voting based mechanism [3],[4] and non - voting based mechanism[5],[6]. The above mechanisms have some disadvantages such as heavy communication overhead, degraded accuracy and degraded reliability. In order to overcome the disadvantages of existing mechanisms, Cluster Based Certificate Revocation with Vindication Capability is proposed. The proposed system comprises of four modules namely cluster construction, Certification Authority, Node classification and Certificate Revocation.

The proposed system overcomes the disadvantages of both voting based mechanism and non - voting based mechanism and achieves low communication overhead and low revocation time and also improves the reliability and accuracy. The certificate of misbehaving node is removed and its access to the network is immediately stopped and secure network communication is provided in proposed Cluster Based Certificate Revocation with Vindication Capability scheme.
II. CLUSTER HEAD FORMATION

Number of mobile nodes join together to form Cluster. Each Cluster consists of single Cluster Head (CH) and number of Cluster Members (CM). The node which has higher energy acts as Cluster Head and the nodes having lower energy act as Cluster Members. As the energy goes on decreasing, the Cluster Head changes and node which has higher energy acts as Cluster Head. For the transmissions between the Cluster Head, the Remote Manager acts as the intermediate. Remote manager also monitors that if there is any misbehaving node in the cluster and take necessary actions to remove that particular node from the cluster, so that other nodes may not be affected.

The Cluster Head forwards packets periodically to its cluster members which are within its transmission range to detect a new connection.

III. CERTIFICATE AUTHORITY

Certificate Authority is responsible for distributing and maintaining digital certificates of nodes so that they can move freely in network for secure communication. It also maintains two types of lists namely Warning List (WL) and Black List (BL). The Warning List contains accusing node and its information and the Black List contains accused ode and its information.

In order to remove the certificates of accused node, the Certification Authority sends message to the whole network about the accused and accusing nodes in the Warning List and Black List respectively. Basically Certificates are needed to avoid malicious node which are on the path to the target server acts as target. So in order to avoid the Man in the Middle attack, CA Certificate is used to verify the CA signature on the server Certificate so that secure communication can be established.

IV. NODE CLASSIFICATION

Nodes are classified according to their reliability and their behaviour. Based on the behaviour, nodes are of three type’s namely legitimate node, malicious node and Attacker node. Legitimate node removes the certificate of malicious node to establish network communication. Malicious node seriously affects the network performance. Also, If malicious nodes are present in Mobile Adhoc Network, network connectivity is reduced and packet delivery cannot be guaranteed. Attacker node launches attacks on other nodes in the network and disturbs communication between the moving nodes.

According to reliability, nodes are classified as normal ode, warned node and revoked node. Normal node can act as Cluster Head or Cluster Member so that it can accuse other nodes positively and it does not launch attacks on other nodes. The nodes which are accused are called as warned node. The warned node is composed of both legitimate node and malicious node. These warned nodes can accuse other nodes only once. Accused nodes are called as revoked nodes. Nodes that are present in Black List are the Nodes to be revoked. The Certificates of revoked nodes are removed and the particular node is stopped from its network activities.

V. CERTIFICATE REVOCATION

This module consists of three steps namely accusing, verifying and notifying. Accusing is nothing but, when a node launches attacks on other nodes, the Cluster Head verifies whether the node is present in Black List. Notifying is the information sent to the whole network about the misbehaving node and certificate of particular node is removed or revoked.
VI. SIMULATION

Simulation is done in Network Simulator (NS2). Simulation is done where the mobile devices freely move in the environment. The first step is the formation of node.

Fig. 2. Node Formation

The second step is the distribution of nodes in network. Nodes are distributed to perform communication with its neighboring nodes.

Fig. 3. Distribution of nodes

Group of nodes joined together to form Cluster. Each Cluster consists of one Cluster Head and more Cluster members. The node which has higher energy is the Cluster Head and the remaining are its Cluster members which have low energy. As the energy goes on decreasing, the Cluster Head changes and node which has higher energy acts as Cluster Head. For the transmissions between the Cluster Head, the Remote Manager acts as the intermediate. Remote manager also monitors that if there is any misbehaving node in the cluster and take necessary actions to remove that particular node from the cluster, so that other nodes may not be affected.

Fig. 5. Transmission between Clusters

As said earlier, the Remote Manager helps in transmission between the Clusters.

Fig. 6 Mobile Station moving towards station Base station

After more delivery of packets and transmissions heading towards the base station, the mobile station collects all packets and carries it to the base station.

Fig. 7. Mobile station reaches destination

Mobile station collects all packets and move towards the destination base station. This is the final step and the following routing performances, Throughput, Packet delivery ratio, Energy consumption are analyzed. Also these characteristics are improved when compared to the
existing system and the comparisons are given in the following graphs.

![Fig 8. Routing Performance Analysis](image1)

The process of moving a packet from source to destination is called as routing and is performed by router. Routing Performance is improved when compared with the existing methods. That is, the secrecy of information is highly maintained in the proposed system.

![Fig 9. Packet Delivery Ratio](image2)

Packet Delivery Ratio varies according to the number of sensor nodes respectively. In the proposed system, the number of packets lost is reduced, and packets are correctly forwarded to their destination.

![Fig.10. Throughput](image3)

Throughput increases depending upon the number of sensor nodes. At a particular stage throughput becomes constant.

![Fig.11. Energy Consumption](image4)

Energy Consumed is low when compared to the existing system. Energy consumed decreases when the number of sensor node is increased.

VII. CONCLUSION

While comparing the proposed system with the existing system such as voting based mechanism and non voting based mechanism, the proposed system has higher accuracy and reliability, low revocation time with effective and efficient revocation of certificates from misbehaving node, solution for false accusation, also the number of availability of normal nodes is increased. Since the packet delivery ratio is less due to the loss of packets, the packet delivery ratio is improved and also delay performances and throughput are improved in the future.

REFERENCES


**AUTHOR(S) PROFILE**

**P.Kiruba Priyadharsini**
received the B.E degree in Electronics and Communication Engineering from National Engineering College, Anna University, chennai, Tamilnadu, India. Presently she is pursuing II M.E Communication Systems in Francis Xavier Engineering College. Her area of interest is wireless communication.

**Mrs.L.R.PRIYA**
received B.E degree in Electrical and Electronics Engineering from CSI Institute of technology, Tamilnadu, India in 2005 and the M.Tech in VLSI from Karunya University,Coimbatore,Tamil Nadu in 2007. At present, she is doing her research work in Wireless Network and working as a Associate Professor in Francis Xavier Engineering College, Tamil Nadu, India.

**Dr.K.Ruba Soundar**
received the A.M.I.E degree in Computer Science and Engineering from The Institution of engineers in the year 2000 and M.E and Ph.D degrees from Anna University, Chennai in the year 2004 and 2010 respectively. At present he is working as Professor and Head in P.S.R Engineering College, Sivakasi, Tamilnadu, India. His area of Interest is Digital Image Processing and wireless Communication.