A Survey on Various Cluster Based Certificate Revocation Schemes

Rakhi Bhardwaj[1], Satish Jarang[2], Priya Tupe[3], Priyanka Sulaskar[4], Dnyaneshwar Rathod[5]

[1]Professor, Rakhi Bhardwaj, Dept. of Computer Engineering, TCOER Pune, Maharashtra, India.
[2] Satish Jarang, Dept. of Computer Engineering, TCOER Pune, Maharashtra, India.
[3] Priya Tupe, Dept. of Computer Engineering, TCOER Pune, Maharashtra, India.
[4]Priyanka Sulaskar, Dept. of Computer Engineering, TCOER Pune, Maharashtra, India.
[5] Dnyaneshwar Rathod, Dept. of Computer Engineering, TCOER Pune, Maharashtra, India.

---***---

Abstract - *Mobile Ad hoc Networks (MANETs) are self-configuring wireless networks. MANET is an infrastructure less mobile network formed by a number of self-organized mobile nodes. In today's world the use of such wireless networks has increasing rapidly. As MANET is infrastructure less, hence it is more vulnerable to various security attacks. So in order to guarantee secure network communication and to eradicate the security threats, some efficient security providing mechanism should be there. To address the problem of security here we presented some of the certificate revocation techniques. Certificate revocation of malicious node is challenging in certificate revocation technique. This survey paper focuses on different kinds of such certificate revocation techniques thus isolating the attackers by certificate revocation.*

This survey paper gives details about methods which are used for revoking attacker certificate and recovering falsely accused certificate.

1. INTRODUCTION

Mobile ad hoc networks are simple to arrange, autonomous and scalable. MANET is wireless network therefore they are more prone to various security attacks. Because of dynamic and self-organizing nature of MANET it is difficult to form cluster and select a cluster head. To make communication in MANET more secure and to detect malicious node and to stop it from participating in further communication in network various techniques have been proposed.

Forming a cluster and selecting a cluster head among them is not easy task .Various algorithms have been proposed to form a cluster. When a node is part of any cluster it get attached to the cluster head and keeps sending hello message to the cluster head to check the distance by measuring strength of signal. When the signal strength decreases it searches for other cluster head nearer to it .When no cluster head is nearer to it, it itself becomes a cluster head but this way all nodes could become Cluster head. To overcome this when two cluster heads are one hop distance away from each other all nodes connected to those CH gets attach to other nearer CH's. Remaining nodes and cluster head performs election process among them.

MANET is more vulnerable to various security attacks. To detect attacker or malicious node certificate authority established. Certificate authority distributes certificate to each node when it joins the cluster. Cluster head checks and verify the certificate of the nodes participating in the communication. In paper [1] they have proposed a system with certificate authority which maintains black list and warning list. Black list lists accused node and warning list lists accusing nodes. Section II describes literature survey. Section III describes System Design. Section IV describes conclusion.

2. LITERATURE SURVEY

In [1] Author has described about MANETs security issues. And explained one solution that is certificate revocation of attacker node. For which certificate verification mechanism is used. And this certificate verification is done by certificate authority. First it will distribute certificate to all of the nodes in network and while sending packets nodes will check the certificate of source node if some changes found it sends accusation to Certificate Authority (CA). Certificate Authority will check and take action accordingly. Here Author has introduced mechanism for dealing with false accusation by certificate verification. That is if accusation was false then node will be able to join the network again and information will be updated to all nodes. Otherwise certificate will be revoked and that node will not be part of communicate in MANET. Author has also introduced the previous mechanism those are Voting based and Non-voting based mechanism but some drawback are covered in this new mechanism. Author has used some algorithms like Weight based clustering.

In [2] author has described algorithm for cluster formation that is Weight based hierarchical clustering algorithm. As MANET is dynamic and self-organized and there is no fixed infrastructure. There are different solution for reducing the size of network. From which most intrinsic method is clustering techniques. In this Weight based hierarchical algorithm. This protocol is divided into three subsection. I, cluster head selection. II, Cluster formation. III, Data communication process is explained. In first section cluster head selection is done by using three parameters. i) Highest degree heuristic ii) less mobility factor iii) Transmission range. In this algorithm node with highest degree is chosen as head of culture.

In [3] new system is proposed in which both accused and accusing nodes are listed in warning list and analyzed. After analyzing the malicious node's certificate, malicious node's certificate is revoked and it is stored in black list. Once node is stored in black list, it cannot be recovered again. In this system also both voting and non-voting based mechanism is used. But in previous mechanisms certificate was revoked using both voting and non -voting based mechanism. Accused node was listed in black list and accusing node was listed in warning list. In previous system nodes in black list could be recovered and listed in warning list, it had some drawbacks.

In [4] Author has introduced various types of attacks in MANET. These attacks are classified in to two types. Data traffic and Control traffic attacks. This two categories are based on common characteristics and attack goals. Some attacks have implicate in both categories, so they cannot be categories.

Data Traffic Attack: In this type of attack either packet is dropped completely or delaying of forwarding. This type of attack leads to extreme speed fall. It could reduce speed 100 times less than original speed. This type of attack can be prevented by two strategies. (a) Collecting multiple RREP messages from few nodes. And hoping multiple paths unless safe route is found. (b) Each node maintains table by increasing order of previous sequence number.

Control Traffic Attack: MANET is having some characteristics like its openness that any node can join or leave network at any time so it makes it more vulnerable to various types of attack. So use of routing protocols like AODV and D use of routing protocols like AODV and DYMO could make network fast.

In [5] they have proposed new mechanism which uses trust value of the node which is used for certificate revocation. Trust value and Final trust is evaluated in [5] When any node accuses the node in the cluster, CH checks the FT value of the accusing node, if the FT value is greater, then CH checks the accused node in the warning list and if it is already present then the certificate of the accused node is revoked and it is listed in black list. If the FT value of the accusing node is less then both nodes are listed in warning list and CH evaluates it later. In previous papers the nodes were listed in warning list and black list using voting mechanism.

In [6] they have done research to reduce the repetition of election process. In previous papers election process was performed when node no longer could attach to the cluster head of its cluster. When node could not found any cluster head, it itself becomes cluster head. This way all nodes could be cluster head, to overcome this when two cluster heads are one hop distance from each other all nodes attached to them find other cluster head nearer to them and get attach to those cluster head then remaining nodes which could not found any other cluster head and the cluster heads themselves forms a cluster and perform election process and select their cluster head. This way no need of performing election process throughout the network and it does not affect whole network.
`

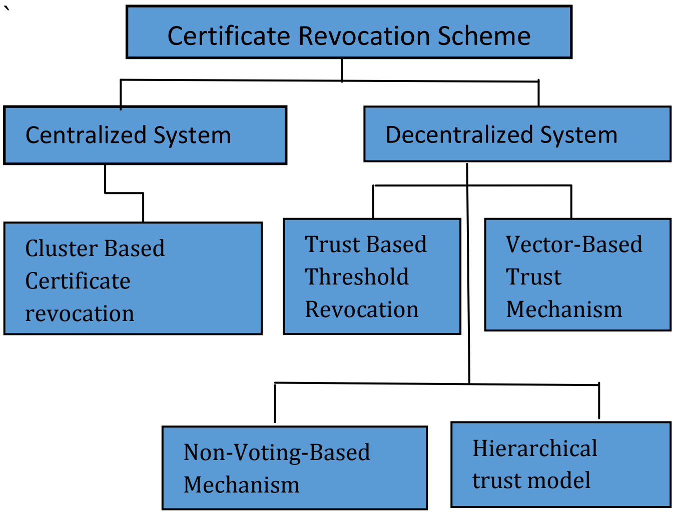
Certificate Revocation Scheme
Centralized System
Decentralized System
Cluster Based Certificate revocation
Trust Based Threshold Revocation
Vector-Based Trust Mechanism
Non-Voting-Based Mechanism
Hierarchical trust model

Fig -1: Taxonomy of Certificate Revocation Schemes

In [7], shows the two drawbacks are described which are. 1) From which way they will locate CA servers? And. 2) How to perform proactive share update? Provide the secured communication to all nodes in network that is biggest challenging problem. Cluster is formed using mobile ad hoc network with N nodes. Shamir proposed threshold scheme. The secret is distributed multiple entities having different properties. Reconstruction of secret can be done by the secret shares gathered from t or more users. With fewer shares which are secret construction of secret cannot be done is called as threshold.

In [8], author describes the analyzing existing clustering approaches for mobile ad-hoc networks and have implemented this clustering approaches using some algorithms. Those are topology based, Energy based, Weight based and Identifier Neighbor based clustering algorithms etc. Basically Routing means moving a packet of data from one network to another i.e. from source to destination .There are two types of Routing and it can be classified into flat structure or in hierarchical structure types of routing. All nodes in flat structure routing have same role in network. In flat structure network could get saturated because of the excessive information flow. Hierarchical structure is used for solving this problem which occurs in flat routing structure. In this method network is divided into groups called as clusters. Then author used some different routing schemes i.e., inter-cluster and intra-cluster. In MANETs the structuring of network is very important step for simplifying some routing information which are related to the network.

In this paper different clustering schemes are mentioned and these schemes have different characteristics. Also this is designed for implementing certain goals, which depends on some context.

The network is divided into interconnected sub-structures called as cluster. One is selected as cluster head. For cluster head selection several algorithms are- lowest-id, distributed clustering, weighted clustering, highest degree, distributed weighted clustering algorithm (DWCA) etc. Neighbor Based Clustering algorithm assigns some unique ID or value to each node in the network and each node knows the ID of its neighboring node. Then cluster head is selected using this unique ID and this ID may be lowest ID or Highest degree ID. Then in Linked clustering algorithm they show node either as cluster head, gateway node or member node. In Least Cluster Change (LCC) algorithm i.e., updated version of Linked clustering algorithm shows when two nodes are neighbor node, then one with the highest ID considered as cluster head. When there is no CH, the node itself becomes CH and forms its own cluster. Then Topology Based Clustering Algorithm was introduced, in that cluster head is selected by using metric computed from network topology that is node connectivity. High-Connectivity clustering protocol is used to select cluster head. When two or more nodes have same degree of connectivity then node which has lowest ID is considered as cluster head. All this procedure of algorithms shows basic fundamental concepts of clustering, routing etc. All algorithms show some clustering schemes in mobile ad-hoc network which helps to organize MANET at hierarchical level.

3. SYSTEM DESIGN

The proposed system can be designed in three modules

a) Cluster Construction
b) Certification Authority function
c) Certificate Revocation
 - Revoking malicious nodes certificate
 - Detection of false accusation

System for dealing with false accusation can be designed. Using cluster based certificate revocation system we can secure communication in MANET by revoking certificate of attacker node and stopping it from participating in future communication.

4. CONCLUSION

This paper address to major issues to ensure secure communications for mobile ad hoc networks by certificate revocation. Study has found that this scheme is more effective and efficient in revoking certificates of malicious attacker nodes, reducing revocation time, and improving the accuracy and reliability of certificate revocation. And false accusation can be handle using Cluster based certification. In future some kinds of MANET attacks can be prevent which are discussed [4]. And using Weight based hierarchical algorithm network size can be reduced.

REFERENCES

[1] Megha R Jarang, "Implementation of Cluster Based Certificate Revocation in Mobile Ad Hoc Networks", Published in IEEE. 978-1-4673-7910-6/15/$31.00_c 2015

[2] Soumyabharat Saha, SuparnaDas Gupta, "Weight Based Hierarchical Clustering Algorithm for Mobile Ad Hoc Networks", doi:10.1016/j.proeng.2012.06.137 Published by Elsevier, 2012.

[3] Kiruthiga, Lakshmipathi, Prem & Preetha Kurup "cluster Based Certificate Authentication for Mobile Ad-Hoc Network" , International conference on Simulations in Computing Nexus, ISBN : 20-21 March, 2014

[4] Aniruddha, Arnab, Dipayan, Himadri, Debika "Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques".

[5] S.J. Indhu Lekha, R. Kathiroli "Trust Based Certificate Revocation of Malicious Nodes in MANET", Published By ISBN No. 978-1-4799-3914-5/14/$31.00 ©2014 IEEE

[6] Vincent, Nidal , Noufissa Mikou, "A Weighted Clustering Algorithm Using Local Cluster-heads Election for QoS in MANETs" Published in IEEE 1-4244-0357-X/06/$20.00 © 2006.

[7] Y. Dong , Ai-Fen Sui , S.M. Yiu , Victor O.K. Li , Lucas C.K. Hui "Providing distributed certificate authority service in cluster-based mobile ad hoc networks", Y. Dong et al. / Computer Communications 30 (2007) 2442–2452.

[8] Abdelhak Bentaleb, Abdelhak Boubetra, Saad Harous, "Survey of Clustering Schemes in Mobile Ad hoc Networks", Scientific Research,doi:10.4236/cn.2013.