Certificate Revocation for MANET using Clustering

Bhagyashri C. Jadhav
ME, E & TC Department
NMIET, Talegoan, Pune

Gayatri Ambadkar
H.O.D, E & TC Department
NMIET, Talegoan, Pune

Rajendra D. Kanphade, PhD
Principal, NMIET Talegoan
NMIET, Talegoan, Pune

ABSTRACT
A mobile ad hoc network is a self-organized wireless network. Which consists of mobile devices. It is used for gathering the data. It consists of large number of nodes with limited energy or In MANET each node has limited energy resources. MANET is infrastructure less network i.e. it is a open network. Due to open network any node can join and leave a network. Because of this security is more essential for MANET. To secure network communication certificate revocation is an important integral component. The proposed method is depends on k-means clustering algorithm. Certificate revocation is used to examine attackers from participating in networks activities in future. To revoke certificates of malicious nodes present in networks, certificate revocation is one of the best scheme. It plays an important role in detecting falsely accused node within networks. To overcome all these problems, Cluster based certificate revocation for MANET is proposed. The proposed scheme is simulate using NS2.

Keywords
Certificate revocation, K-MEAN algorithm, MANET, Network security

1. INTRODUCTION
In communication network system, Mobile Ad-hoc Network(MANET) comprises of various communication devices such as laptop, mobile, PDA's etc.[1] There is no fixed infrastructure for operation of MANET. Grouping of various nodes for communication with each other in wireless channel is called as MANET and it also uses Standard routing protocols. Transferring and protecting packet is major function of MANET. From numerous clustering algorithm, we have used K-MEAN algorithm.[2] Being, it is very simple, relatively efficient and fast.

Voting based and non-voting based mechanism are two types of certificate revocation mechanism. Malicious node can be effectively and immediately removed while using certificate revocation mechanism.[3] In this paper, we have studied and proposed certificate revocation mechanism for secure network communication. It is very effective method, to isolate outside or external attacker node in network system and also avoid false accusation of node.

This proposed work will ensure the secure network communication and Inherits merits of voting and non-voting based mechanism.

2. LITERATURE REVIEW
For certificate revocation mechanism, lot of literatures are available. Majorly of this mechanisms are based on voting and non-voting based mechanism. Voting based mechanism revokes malicious attacker certificate with the help of votes from neighboring node.

Wei Lie [1] et.al proposed cluster based certificate revocation with vindicate capability for MANET. In this proposed scheme, certificate revocation is very important method for secure communication. For accurate and quick certificate revocation, proposed cluster based certificate revocation with vindication capability for MANET.

Jyoti Patole [2] proposed that Design of MAP-REDUCE and K-MEAN based network clustering protocol for sensor network.

This scheme splits cluster into two phases such as MAP and cutback.

Jissmol Jose [3] proposed Certificate revocation in MANET using clustering. In this scheme, every node must have certificate before entering into the network. There should be one cluster head to give certificate to others node. Nodes should store data in standing table and profile table, giving an threshold work within the network potency method.

Kyung Tae [4] et.al proposed An energy efficient and optimal randomized clustering for WSN. They used new approach for setting threshold work, this proposed theme identifies best variety of cluster network additionally by exploitation tree construction in every cluster. Which will increased the life span of network.

Park [5] et.al proposed Certificate revocation to cope false accusation in MANET. In this scheme, self organized nodes are used to make cluster. Holding defendant node and cristice node in black list and warning node severely. However, single neighboring node will revoke certificate of malicious node. Also incorrectly defendant node is removed by cluster head.

3. SYSTEM ARCHITECTURE
Following figure shows the system architecture. It consists of four blocks such as,

- Cluster construction
- Certificate Authority(CA)
- Certificate Revocation.

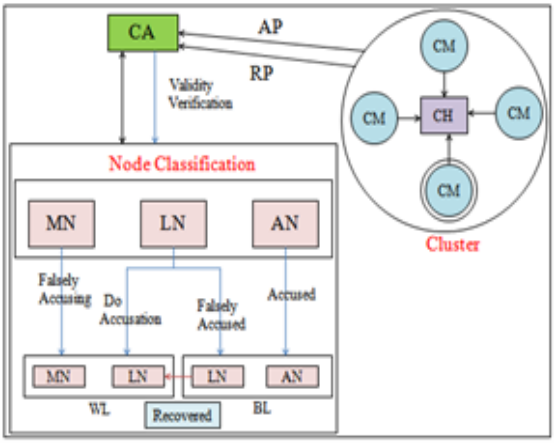


Fig. 1: System Architecture

3.1 Cluster Construction

In the network, number of nodes are present. These nodes are classified into group or cluster with help of K-MEAN algorithm. Each cluster consist of one cluster head (CH) and other nodes are cluster members(CMs). In each cluster ,the cluster head plays an important aspect. All cluster members do not directly communicate with base station or other cluster[3]. All cluster member send packet to cluster head. The cluster will received packet from cluster member and send to other cluster or base station. Due to this communication, the energy of cluster head gets reduced.

3.2 Certificate Authority Function

The newly join node will received valid certificate from certificate authority (CA). The CA consists of two list such as warning list (WL) and black list (BL). This two lists will be managed and renewed regularly by CA. The information of accused and accusing nodes are store in BL and WL respectively. Where, fully revoked nodes are hold by BL. The nodes in WL are analyzed to find the attacker node in cluster and revoke completely from network and store in BL.

3.3 Certificate Revocation

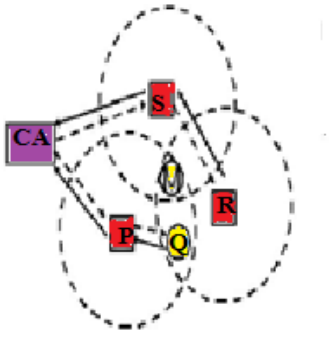
The main focus of the certificate revocation procedure is removing the certificate of malicious node and restoring falsely node as normal node in the network, which is described below,

1. Procedure of Certificate Revocation

Finding the presence of attacker node is first stage or step of certificate revocation procedure. After identification of malicious node, neighboring node transfer accusation packet to CA.

Below mentioned example describes the certificate revocation procedure , when malicious attacker M launches attack within one-lop range as shown in following fig.2

1. P,Q, R,S nodes (called as neighboring nodes) identifies the attacks made by node M (malicious node).
2. Every neighboring nodes send accusation packet to CA against malicious node M.
3. As per first accusation packet from Node P, CA puts P in WL as an accuser node and puts M node in BL as an accused node, after verification of validity of node P
4. Revocation message will be spread in the network by CA.
5. Updation of local list (WL & BL) will be done by CH to cancel M node's certificate.



WL	BL
P	M

Fig.2 A Nodes Certificate Revocation

Results of Revoking malicious certificate

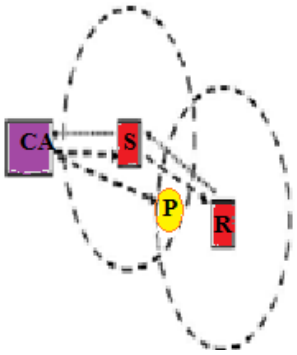
1. Node P is in Warning List (WL).
2. Node M is in Black List (BL).

2. False Accusation

When external node send accusation packet to CA then CA will put nodes in BL and WL. CA this list will spread in the network. Every nodes gets information by continuous Updation of list. Even nodes will get intimation of false accusation with the help of this list.

Below mentioned example describes the false accusation procedure as shown in following fig.3

1. Information regarding BL & WL will be spread by CA to all the nodes in the network.
2. CH R & S update their WL & BL, determine that node P was framed
3. CH R & S will send recovery packet to CA for the repairing of falsely accused node P.
4. CA will eliminate P from the BL and puts P & R in WL, after receipt of the first recovery packet.
5. All nodes will renew their local list (WL and BL) to restore node P.



WL	BL
P,S	P

Fig.3 False accusation

Results of certificate recovery

1. Node P which is present in Black List (BL) will get removed from BL and is entered into a WL.
2. Nodes P and R are in Warning List (WL)

4. IMPLEMENTATION

For cluster formation, K-MEAN algorithm is used as below.

1. Determine the seed node co-ordinate.
2. Determine the distance of each node from the seed node.
3. Make the group of nodes based on minimum distance (find the closest seed node). The distance between node is calculated by using distance formula. The distance formula is given by,

$$d = \sqrt{(x2 - x1)^2 + (y2 - y1)^2}$$

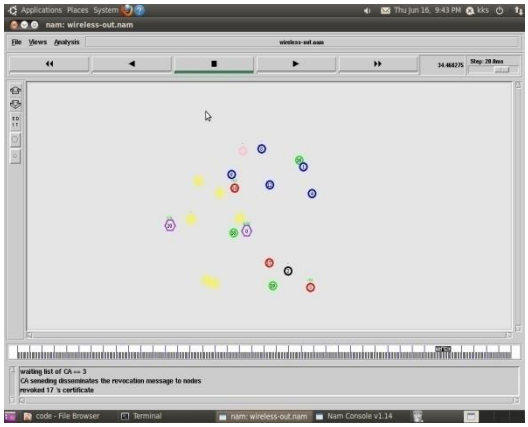


Fig. 4: Cluster Formation

- After cluster formation communication between node will start.
- All the nodes are present in source cluster send packet to cluster head and cluster head send packet to destination cluster head.
- These received packets are send to all nodes present in destination cluster.
- After few second source cluster head will change as well as destination cluster head and so on.

  (Notation used Old cluster head become light pink and new cluster head become red.)

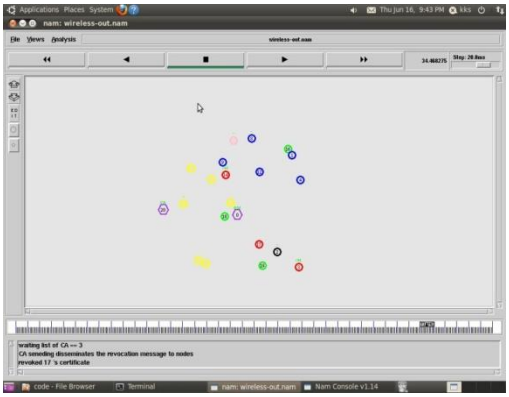


Fig.5: Certificate revocation NAM –NS2 interface

- After receiving key from CA, external node will enter into source cluster as well as destination cluster.
- If the external node misbehave in source cluster then all node present in source cluster will send accusation packet to CA.
- After receiving first accusation packet from node then CA will hold node in warn list and black list.
- Broadcast this list in source cluster.
- CH will update list and send to CA.
- Malicious node become de-active.
- A recovery packet will be sent to CA for the repairing of falsely accused node.

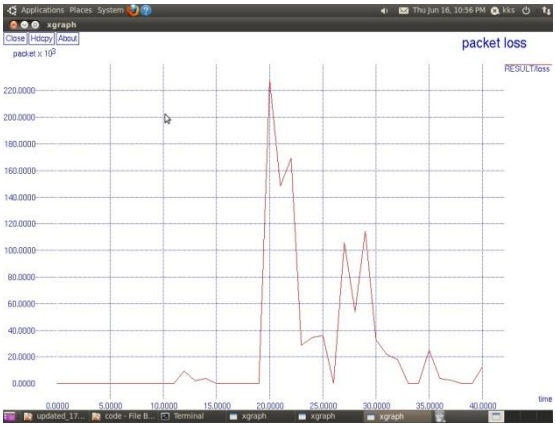


Fig. 6: Packet Loss

5. RESULT

Table.1: Simulation Parameter

Parameter	Value
Simulator	Network Simulator 2
Total Cluster	3
Total Node	21
Cluster node	Random
Simulation time	40sec
Area	4000mm2
Packet size	1000kb

6. CONCLUSION

This scheme combine advantages of voting & non -voting based mechanism, also resolve the problem of false accusation. A revocation time is reduces as compared to voting based mechanism.

The scheme can remove an accused node based on a single node's accusation, and reduce the revocation time as compared to the voting-based mechanism. In addition, the cluster-based model to recover falsely accused nodes by the CH, thus improving the accuracy as compared to the non-voting based mechanism.

In this scheme, for secure communication of MANET, certificate revocation of malicious attacker is address.

7. FUTURE SCOPE

Energy Efficient Cluster Based Certificate Revocation For MANET will proposed. The clustering process takes energy level of node & location information in terms of coordinates as an input. To save the node energy, the cluster head will rotate after few second. So the node energy is balanced & life time of network is increased.

8. ACKNOWLEDGMENTS

The authors would like to gratefully and sincerely thank the anonymous reviewers and advisors for their constructive

9. REFERENCES

[1] Wei Liu,Nei Kato,"Cluster Based Certificate Revocation With Vindication Capability For MANET",IEEE Transactions on Parallel & distributed system,vol 42,no.2,doi:10.1109/TPDS.2012.85.February 2013.

[2] Jyoti Patole, "Design Of MAP –REDUCE & K-MEAN Based Network Clustering protocol for Sensor Networks",IEEE-20180,ICCCNT'12,26th-28th july 2012,coimbatore.India.

[3] Jissmol Jose ,"Certificate Revocation In MANET using Clustering", ISCO,2015,IEEE 9th conference.

[4] Megha R.Jarang ,"Implementation of cluster based certificate revocation in MANET",IEEE conference publication ,Green computing & internet of things,2015 international conference.

[5] J. Kong, "A Secure Ad-Hoc Routing Approach Using Localized Self-Healing Communities, Proc. Sixth ACM Int'1 Symp. Mobile Ad hoc Networking and Computing", pp. 254-265. 2005

[6] Kyung Tae,Man Youn,"An energy Efficient & optimal Randomized clustering for WSN", IEEE2015,SNPD2015, june1-3 2015,Takamatsu.

[7] 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.

[8] K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks", Proc. IEEE 71st Vehicular Technology Conf., May 16-19, 2010.

[9] Neda Enami, Rem Askari Moghadam, "Energy Based Clustering Self Organizing Map Protocol For extending Wireless Sensor Networks Lifetime and Coverage", Canadian Journal on Multimedia and Wireless Networks Vol. I, No. 4, August 20 10.

[10] http://people.revoledu.com/kardi/tutorial/kMean/index.html

[11] Hishman Dahshan,Fatma,"A Trust Based Threshold Revocation Scheme For MANETs",IEEE 2013.

[12] Raghavendra Kulkarni,"Technical correspondence",IEEE Transaction On System & Cyberetics-Part C.vol.41.No2,March2011.

[13] Wendi heinzelman,"An Application –Specific Protocol Architecture For Wireless Microsensor networks ",IEEE Transaction On Wireless Communications,vol.1,No.4,Oct-2002.

[14] Seema Bandyopadhyay,"An Energy Efficient Hierarchical Clustering Algorithm For WSN",IEEE INFOCOM 2003.

[15] Raghavendra V. Kulkarni and Ganesh Kumar Venayagamoorthy, "Technical Correspondence Particle Swarm Optimization in Wireless-Sensor Networks: A Brief Survey", IEEE Transactions on Systems, Man, and Cybernetics—Part C: Applications and Reviews, Vol. 41, No. 2, March 2011