Indian Journal of Engineering

RESEARCH

ISSN 2319 – 7757 EISSN 2319 –7765

Impact of Attackers in Location Privacy scheme for Secure Multicasting in MANET

Saravanan TR[1], Sakthivel P[2]

1. Research Scholar, Department of Computer Science and Engineering, Sathyabama University, Chennai, TamilNadu 600119, India
2. Department of Electronics and Communication Engineering, Associate Professor, Anna University, Chennai, TamilNadu 600025, India

Corresponding Author: Research Scholar, Department of Computer Science and Engineering, Sathyabama University, Chennai, 600119, India; Email – saravanantrcse@gmail.com

Publication History
Received: 27 April 2015
Accepted: 19 May 2015
Published: 24 May 2015

Citation
Saravanan TR, Sakthivel P. Impact of attackers in location privacy scheme for secure multicasting in MANET. *Indian Journal of Engineering*, 2015, 12(28), 16-22

ABSTRACT

Mobile adhoc network does not depend on any fixed infrastructure. In MANET all the routing, mobility management functions are performed by nodes in a self-organized behavior. Mobile nodes security in adhoc networks is a difficult assignment. To prevail over this tough task we propose to improve the security by its own location in private key and maintained and those information are maintained by zone leaders. Time stamps are included in the certificate so that the nodes can be rejected if there are any duplicate registrations. To provide more secure self-signed certificates among nodes in the zones private key cryptography is used along with symmetric key encryptions. In the Location privacy scheme to find the impact of attackers in we have taken 5 attackers and the performance is evaluated with performance metrics such as packet drop, resilience and delivery ratio. The blow of attackers in the location privacy scheme provides better results comparing with existing ALERT protocol.

Keywords: Multicast MANET, Symmetric key encryption, Digital certificate

1. INTRODUCTION

Mobile Adhoc Network is an infrastructure less network that has no fixed routers. All the nodes in the network are capable of moving independently and they are connected dynamically in an arbitrary manner. The nodes available in the MANET can function as routers and those nodes are capable of discovering and maintain routes to other nodes in the network. Some of the real time applications of MANET are emergency search and rescue operations, in places where persons want to share the information quickly, data achievement operations in inhospitable terrains.

Saravanan and Sakthivel,
Impact of Attackers in Location Privacy scheme for Secure Multicasting in MANET,
Indian journal of engineering, 2015, 12(28), 16-22,

There are many characteristics of MANET, which are used in data transmission. Some of the characteristics of MANETs are given as follows. They are distributed operation, Multihop routing, dynamic topology, Light weight terminal and shared physical medium. They provide access to information and services regardless of geographic locations. They are robust due to decentralized administration. The nodes are independence from centralized network administration they act as routers and they are less expensive as compared to wired network [1].

1.1. Attackers in MANET

The nodes are vulnerable to various attacks by malicious nodes. There are usually two types of user performing attacks in the nodes. They are malicious users and compromised users. An attacker without any valid shared cryptographic key information who is attacking from outside is called malicious user. A compromised user is inside attacker who posses network authentication with malicious behavior and he is being trusted by other users. There are several attacks that can be performed by either compromised user or malicious user. Some of them are given as follows,

1. A message tampering attack varying packet content
2. Message dropping attack dropping some or all control packet
3. Location tampering attack which alters the information such as physical deletion,alterating the information stored in location table of a node
4. Black mail attack is an attack which identifies a good node as a bad node. This type of attacks happens in network where negative reputation feedback is possible.[7]
5. Attacks with limited communication bandwidth called Denial of service attacks
6. On considering the above attacks security of node is needed. For providing security in security based routing protocols the criteria like location service type, location service robustness, tolerable position inaccuracy, implementation complexity, processing overhead , loop freedom, optimal path , density of nodes should be considered.

2. LITERATURE REVIEW

Srdjan Capkun, Levente Buttyan, Jena Pierre hubaux [2] has proposed a certificate exchange mechanism to share and issue certificates a node issue and hold. This method gives an incomplete view of graph. As the certificate repository is not fully constructed they have developed a repository construction algorithm which has updated certificate repository of nodes. It is a fully self organized public key management algorithm. Main feature of this method is it is not depend on the fixed server or trusted authority still in the initialization phase. The repository construction algorithm which is designed with communication overhead in mind assumes only the partial knowledge of a certificate graph.

Karim El Defrawy and Gene Tsudik [17] constructed an on-demand anonymous location-based MANET routing protocol (PRISM) to accomplish loneliness and protection aligned with together outcast and insider adversaries. It depends on group signatures for node authentication and supports in distrustful location based MANET for anonymous reactive routing. Here integrity of routing messages was ensured while preventing node tracking. This method can function with any location forwarding system and with any group signature method.

Nen Chung Wang and Shian Zhang Fang [3] have projected a hierarchical key management mechanism for secure group communication in MANET. According to the hierarchical key management scheme the nodes are splitted into groups. As nodes are splitted into groups it is easier for group communication. In this scheme a cluster head is created that manages information constructs and transmits the group key. Keys can be easily managed as the nodes are splitted into groups. The largest weight value of the nodes is considered as cluster head. The mobility of the node is not considered.

Haiying Shen and Lianyu Zhao [10] has developed an Anonymous Location-based Efficient Routing proTocol (ALERT) which classified the network field into zones and selected zonal nodes randomly as intermediate relay nodes, forming a nontraceable anonymous route. Also the data from node which initiates or receives among many nodes which initiates or receives was hidden to strengthen source and destination anonymity protection. As a result, anonymity protection to sources, destinations, and routes were offered by ALERT.

Joo-Han Song, Vincent W.S Wong, Victor C.M Leung [7] has proposed a secured geographic forwarding mechanism which provides neighbor and source authentication and message integrity by using TIK protocol and shared keys. Here they have used a Secure Grid location service where the correctness of message with location can be verified by any receiver. They have aimed in detecting and isolating both selfish and compromised users. They have evaluated it with a flat grid with 100 nodes. They have assumed 50 of the nodes has constant bit rate and each sending 128 byte messages at the rate of 4 messages in 200s. Simulation results show that there is a high message delivery ratio with the expense of routing overhead and higher average end to end delay.

3. PROPOSED WORK

3.1. Overview

Initially sub group configuration [3] is not based on the location of the node. The largest weight value is selected as cluster head. To overcome this issue in [4] we have projected a hierarchical key management system based on location of node, here the location information of the nodes are considered and the group heads are selected based on the stability index. The nodes are splitted into clusters based on the location information of the nodes. In each cluster formed the stability index of each node is calculated. Cluster head is elected as the node with highest stability index. Here the method of data liberation is to first encrypt packet by private key, then encrypt and decrypt it another time by cluster key and group key. Rekeying of group key and cluster key is done while a node leaves or joins the network.

Saravanan and Sakthivel,
Impact of Attackers in Location Privacy scheme for Secure Multicasting in MANET,
Indian journal of engineering, 2015, 12(28), 16-22,

To apply a secure multicasting for large group size in intra cluster communication [5] a bidirectional tree is constructed based on zones and leader of zone is elected using trust value generated by Markov Trust model. We have used elliptic curve discrete algorithm for secure voting process in the selected zone leader. In [4] and [5] we have considered about zone formation, location based hierarchical key management and sending their location information to the group heads. In [12] as an extension of [4] and [5] the security of location information is considered. A scheme is developed using symmetric key encryption mechanism in addition to private key cryptography, the nodes which are maintained by zone leaders adds its own location in private key.

The main aim of [12] is prevent the identity replication attacks. Here the self signed signatures from malicious nodes would nodes would not be accepted due to lack of message formats. As with signed session establishment messages, any variation in the content or to the original sender's ID can be traced while forwarding in multiple hop networks. In this paper we increase the number of attackers or malicious nodes in the location privacy scheme for secure multicasting and the performance of the location privacy scheme with malicious nodes are evaluated.

3.2. Registration and Initialization

Registration process is done by using private key cryptography in addition to technique of symmetric key encryption. Location server of the grid is indicated as S.A node is selected as zone leader in each grid and each node in grid sends its node ID, signature verification key and certificate to S. The certificate binds nodes identity with its public key and is signed by S.As certificates are time stamped there will an expiration time for each certificate. As public key of S is with each node certificate of other nodes can be easily decrypted. For node joining the following procedure to be followed.

1) A simple self signed certificate of N_{PK} is created from the public key pair (N_{PK}, N_{PR}) of node N. It is given as follows

$$CertN = SigN(NID, \mathrm{N}_{\mathrm{PK}}, TN_{PR}) \qquad (1)$$

Here TN_{PR} represents the timestamp of creating TN_{PR}

2) The node N creates and broadcasts the public key registration message which is given below

$$PK(\mathrm{N}) = [\mathrm{Type}, \mathrm{Seq}, \mathrm{Cert}_{\mathrm{N}}, \mathrm{Loc}_{\mathrm{N}}] \qquad (2)$$

Here Type indicates the type of message, Seq indicates the sequence number to prevent loops and duplicate messages, LocN indicates the location of the node and it is calculated as follows

$$\mathrm{LocN} = \mathrm{SignN}(\mathrm{NID}, \mathrm{NGID}, \mathrm{TN}_{\mathrm{PR}}, \mathrm{TCN}) \qquad (3)$$

3.3. Location Update, Request and Response

The locations of the nodes are updated when the nodes are moved from location to another location. The updated location are broadcasted by using the following message [6]

$$\mathrm{LocU(N)} = [\mathrm{Type}, \mathrm{Seq}, \mathrm{LocN}, \tau_{\mathrm{N}}] \qquad (4)$$

The location table holds the location server S which consists of nodes ID, geographic location and grid label. τ_{N} given in equation (4) indicates the reliability of node A. When the reliability falls below a certain level the network excludes the node. The validity of the message not to be verified by all the nodes receiving the location updates messages.

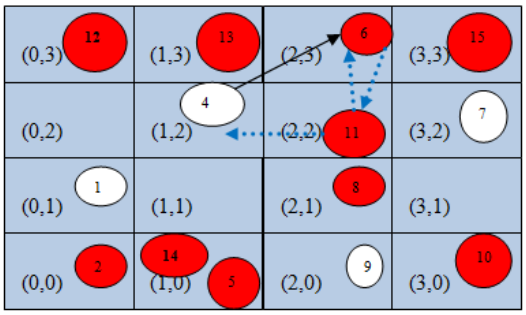

Figure 1
Example for Location Request and Response

Saravanan and Sakthivel,
Impact of Attackers in Location Privacy scheme for Secure Multicasting in MANET,
Indian journal of engineering, 2015, 12(28), 16-22,

The figure1 explains about the location request and response mechanism. Here the location information of node 6 is needed by node 11 and it send a location request node 4.When node11 request node 4 for location information of node 6 , node B broadcast the message to request the location of node A. The message format for the above operation is given as follows.

LocRe = [Type, Seq, AID, LocN] (5)

When node 4 receives the above message the location information of 6 in the location table is seen by node 4.The location response message from 4 for the response of node 11's query about the location of node 6 is given as follows.

LocRs= [Type,Seq,LocB,LocA,LocC] (6)

The location response message is given as unicast transmission.

3.4. Total Work Flow

The MANET is divided into various zones and a bidirectional tree is constructed and trust value is used for electing a zone leader. The total work flow for the location privacy scheme for secure multicasting in MANET is given as follows.

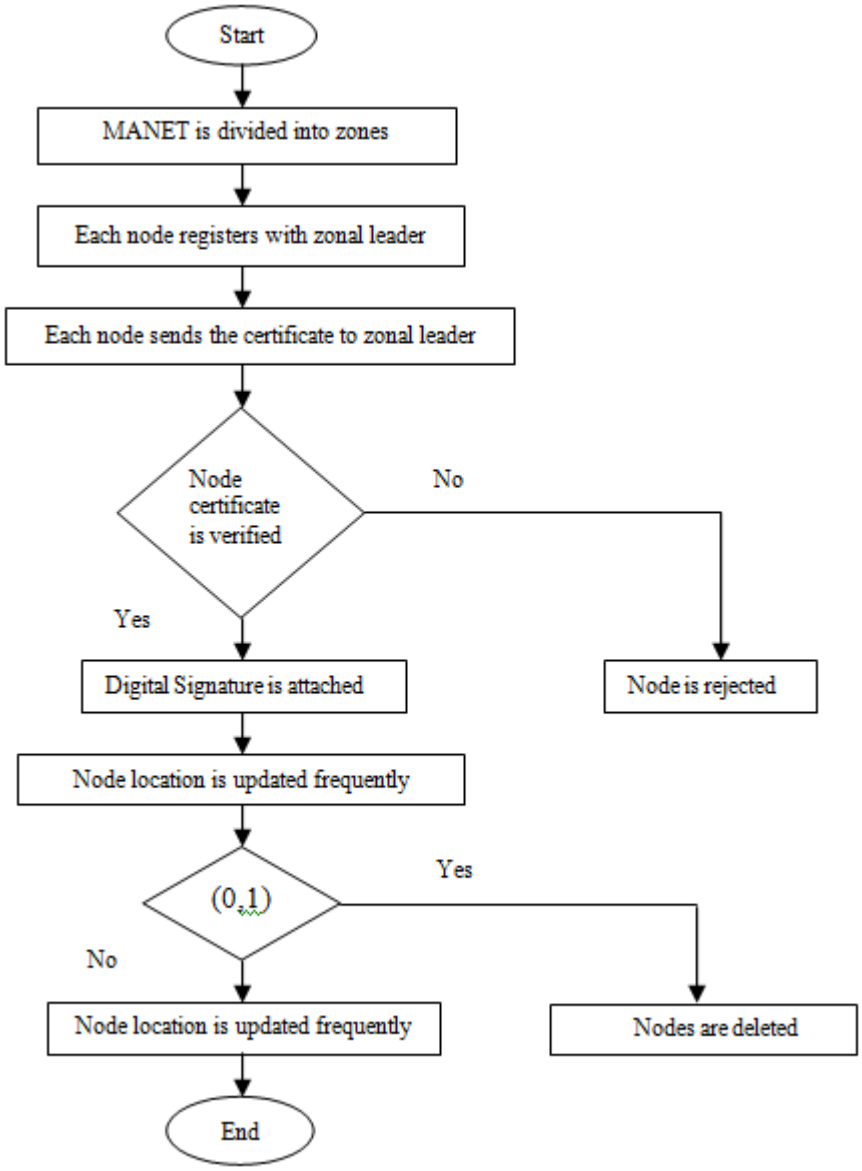

Figure 2
Total Work Flow

Saravanan and Sakthivel,
Impact of Attackers in Location Privacy scheme for Secure Multicasting in MANET,
Indian journal of engineering, 2015, 12(28), 16-22,

The above Figure 2 gives the work flow of the Location privacy scheme of secure multicasting in Adhoc network. The MANET is divided into zones. There will be location server for each zone. The public key of all the nodes in the zones are available in the location server. Each node sends the certificate to the zone leader. If the node certificate verification is successful then digital certificate is attached else node is rejected. If digital certificate is attached then node location is updated frequently. Current time stamp is also attached with node location details. When node position changes the location it is updated immediately to zonal leader.

3.5. Signature based Verification Technique

Identity replication attacks can be detected by using signature based verification technique. As time stamp is included in the certificate the duplicate registrations are rejected. By forwarding in multiple hop networks an establishment message with signed sessions any variation in content or original id can be traced easily. If the verification message is invalid the following broadcast message is given as follows.

Err Alarm = [Type, Seq, err type, SigN(Type, Seq, err type)] (7)

While the node receives the above broad cast message the it should verify the message validity, removing the previous location and update the location and changing the reliability of node. Malicious node is found as the node having false digital signatures or a node without digital signatures. Each node entry is saved in location server.

4. SIMULATION RESULTS

4.1. Simulation Model and Parameters

The proposed location privacy scheme for secure multicasting in MANET is simulated using NS2[18].In our proposed scheme as an extension of [12] we have added 1 to 5 attackers and the performance is evaluated.2 Mbps is set as the channel capacity of the mobile nodes. The network layer link breakage notification is done by using the distributed co ordination function of IEEE 802.11 for Wireless LAN.We have used 50 nodes for simulation and the nodes are allowed to move in a area of 1000 X 1000 meter region with a simulation time of 100 seconds. Transmission range of all nodes is 250 meters. The number of receivers is fixed at 10 with the node speed of 25 m/s. We have used Constant Bit Rate (CBR) as the simulated traffic using Random way point model. The following table 1 summarizes the simulation parameters.

TABLE 1

SIMULATION PARAMETERS

No. of Nodes	50
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	100 sec
Traffic Source	CBR
Packet Size	500 bytes
Mobility Model	Random Way Point
Speed	25 m/s
No. of Receivers	10
Pause time	5 s
Attackers	1 to 5

4.2. Performance Metrics

The performance of the location privacy scheme based on the simulation settings in table 1 is estimated using the following metrics

4.2.1 Average Packet Delivery Ratio

It is the ratio of the integral amount of packets received successfully and the total integral amount of packets transmitted.

4.2.2 Packet Drop

The numeral of packets dropped during the data transmission period.

4.2.3 Resilience against Node Capture

It is calculated by estimation of the fraction of communications compromise between non compromise nodes by a detain of x-nodes. We have implemented Location privacy protection scheme for secure communication in multicast MANET. We are going add 5 malicious nodes as

Saravanan and Sakthivel,
Impact of Attackers in Location Privacy scheme for Secure Multicasting in MANET,
Indian journal of engineering, 2015, 12(28), 16-22,

attackers and the performance is analyzed by taking attackers as x axis and the performance metrics in the y axis. The results are given in the next section.

4.3. Simulation Results

The number of receivers and speed of the node are not varied. The number of receivers is fixed as 10 and the speed of the node is also kept fixed as 25 m/s. The simulation results are given as follows. From the simulation results of Figure 2 we finalize LPSMA (Location Privacy for Secure Multicasting Architecture) outperforms ALERT (Anonymous Location based Efficient Routing protocol) by 70% in terms of delivery ratio with the impact of attackers.

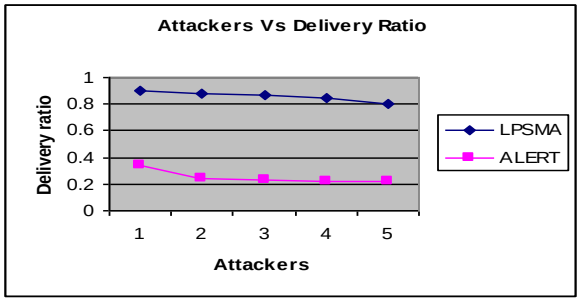

Figure 3

Attackers Vs Delivery Ratio

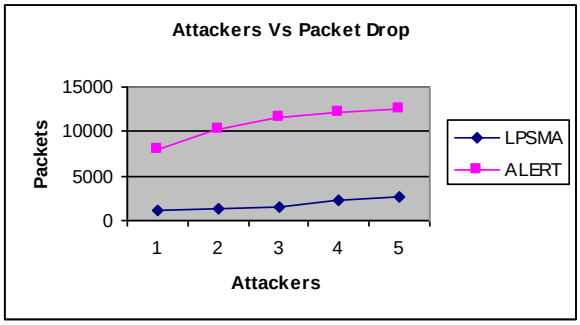

Figure 4

Attackers Vs Packet Drop

From the figure 4 we finalize that with the impact of attackers the packet drop our proposed LPSMA is 83% less than the existing ALERT protocol

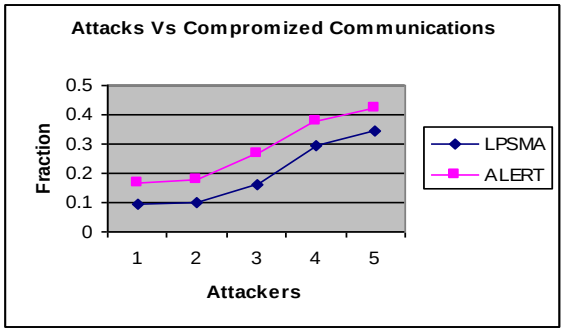

Figure 5

Attackers Vs Compromised communications

Saravanan and Sakthivel,
Impact of Attackers in Location Privacy scheme for Secure Multicasting in MANET,
Indian journal of engineering, 2015, 12(28), 16-22,

From the figure 5 we conclude that our proposed LPSMA outperforms ALERT protocol by 34% in terms of compromised communications or resilience of nodes with the impact of 1 to 5 attackers. Thus we have finalized that the proposed LPSMA outperforms existing ALERT in the impact of attackers in the multicast communication.

5. CONCLUSION

In this paper we proposed a scheme using symmetric key encryption and private key cryptography. In this node adds the own location in the private key and it is maintained by zone leaders. Initially the network is divided into clusters and each cluster is splitted into various zones and each zone is headed by zone leader. The node certificate is verified and the digital certificate is attached and the node location is updated frequently. We have added 1 to 5 attackers in the location privacy scheme proposed for secure multicasting in MANET and it is compared with existing ALERT protocol. Performance of LPSMA is better with the impact of attackers compared with existing ALERT protocol. The Impact of attackers with LPSMA is evaluated with performance metrics delivery ratio, packet drop and resilience of nodes.

REFERENCES

1. M. Shobana, R.Saranyadevi and Dr.S.Karthik, "Secure Data Delivery Using Geographic Multicast Routing", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol. 1, No. 7, September 2012.
2. Srdjan Capkun, Levente Buttyan, Jean Pierre Hubaux, "Self Organized Public key Management for Mobile Adhoc Networks", IEEE Transactions on Mobile Computing, Vol.2, No.1, pp.1-13, Jan- March 2003.
3. Nen Chung Wang and Shian Zhang Fang, "A hierarchical key management scheme for secure group communication in mobile adhoc networks, "Journal of Systems and Software Vol.80,no.10,pp.1667-1677,2007
4. Saravanan TR, Sakthivel P, "Location Based Hierarchical Key Management For Secure Group Communication In MANETS Based On Number Of Receivers," International Journal of Research In Engineering And Advanced Technology, Vol.1, Issue 4 , pp 1-7, 2013
5. TRSaravanan and P Sakthivel, "Zone based Secure Multicast Architecture for Intra-cluster communication inMANET", International Review on Computers and Software, Vol No.11, pp.1834-1842, 2014.
6. Namrata Marium Chacko, Shini sam and P.Getzi Jeba Leelipushpam, "A survey on various privacy and security features adopted in MANETs routing Protocol", International Multi-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013.
7. Joo-Han Song, Vincent W.S. Wong and Victor C.M. Leung, "Secure position-based routing protocol for mobile ad hoc networks", Ad Hoc Networks, Vol.5, pp. 76–86, 2007.
8. T. R Saravanan and P. Sakthivel ,"Nodes Mobility Based Secure Group Communications in Mobile Adhoc Networks using Location based Hierarchical Key Management System", International Conference on Mathematical Computer Engineering (ICMCE), 2013.
9. T. R Saravanan and P. Sakthivel, "Secure Multicast Architecture for Intra-cluster communication in MANET", 4th National Conference on Current Academic Revolution in Communication & Networking (CARCN), 2014
10. Haiying Shen and Lianyu Zhao, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs",IEEE Transactions On Mobile Computing, Vol. 12, No. 6, June 2013.
11. Ehsan Bagherian and Siavash Khorsandi, "ARMAN: A new Anonymous Routing Protocol for Mobile Ad-Hoc Networks", 10th IEEE International Symposium on A World of Wireless, Mobile, and Multimedia Networks, 2009.
12. T. R Saravanan and P. Sakthivel ,"Location Privacy Protection for Secure Multicasting in MANET", National Conference on Recent Advances in Electronics & Computer Engineering, Feb 2015.
13. T. R Saravanan and P. Sakthivel, "Effectual Locality Privacy Protection for Secure Multicasting in MANET for Speediest Nodes", National Conference on Recent Advances in Electronics & Computer Engineering, April 2015.
14. Vivek Pathak, Danfeng Yao and Liviu Iftode, "Securing Geographical Routing in Mobile Ad-hoc Networks", Department of Computer Science, Rutgers University, Tech. Rep. 638, 2008.
15. Mohamed Slim BenMahmoud and Nicola Larrieu, "An ADSB based Secure Geographical Routing Protocol for Aeronautical Ad Hoc Networks", 37th Annual International Computer Software & Applications Conference, IEEE COMPSAC, Kyoto, Japan, 2013.
16. Sanjay Keer and Anil Suryavanshi, "To Prevent Wormhole Attacks Using Wireless protocol in MANET", IEEE International Conference on Computer and Communication Technology (ICCCT), 2010.
17. Karim El Defrawy and Gene Tsudik, "Privacy-Preserving Location-Based On-Demand Routing in MANETs", IEEE Journal On Selected Areas In Communications, Vol. 29, No.10, December 2011.
18. Network Simulator: http:///www.isi.edu/nsnam/ns.

Saravanan and Sakthivel,
Impact of Attackers in Location Privacy scheme for Secure Multicasting in MANET,
Indian journal of engineering, 2015, 12(28), 16-22,