Prevention of Vulnerabilities on Location- based Geocasting and Forwarding Routing Protocol in Mobile Ad-hoc Network

D. Kothandaraman[1], A. Amuthan[2], Dr. C. Chellappan[3],
Dr. N. Sreenath[4],
Department of cse (Information security) [1, 2, 4],
Pondicherry Engineering College, Pillaichavady,
Puducherry-605014, India.
Department of cse[3], Anna University, Chennai-600025, India.
Email: ramanm_5@yahoo.co.in[1] , amuthan@pec.edu[2]

Abstract

In this paper the intention is to prevent potential types of vulnerabilities like blackhole and flooding attack on location- based geocasting and forwarding (LGF) routing protocol in Mobile Ad-hoc Network (MANET). The LGF protocol has proposed to the implemented by Global Positioning System (GPS)- free covered location tracking system with Geocast-enhanced Ad-hoc On-Demand Distance Vector (GAODV). In addition backhole and flooding attack will be generating the prevention techniques in LGF protocol and also find the impact of vulnerabilities to overcome the attacks. Simulation of LGF protocol and attacks has been work done by GloMoSim-2.03 network simulator.

Keywords: *Blackhole attack; flooding attack; LGF; Geocast-enhanced (GAODV); Mobile Ad-hoc Network (MANET)*

1. Introduction

Mobile Ad- hoc network in reactive mesh-based multicast routing protocol on location-based geocasting and forwarding (LGF) routing protocol in MANET is a self-organizing system of mobile nodes that communicate with each other via wireless links with no fixed infrastructure or centralized administration such as base stations or access points [1]. Hence, MANET is suitable an applications in exists such as give below.

1. Military battlefield
2. Emergency rescue
3. Vehicular communications

Above these applications, communication and collaboration among a group of nodes are necessary. Instead of using multiple transmissions, it is an advantageous use of multicast in order to save network bandwidth and resources, since a single message can be delivered into multiple receivers simultaneously. In the LGF protocol routing metrics usually used are shortest path, link stability and minimum number of hops towards the destination. But, power conservation and optimized bandwidth are in MANET is stand-alone devices and operates on batteries [2].

The LGF protocol source node will be multicast the Route Request (RREQ) packet to its entire neighbor nodes within its transmission area. The request packet has additional information send the distance from the source to destination. Hence, every node that receives these packets will compare its distance to the destination. If its distance to destination is less than the distance from the source to destination, the source node will be rebroadcast the packet; otherwise, it will discard and cancel its scheduled rebroadcast of the packet. Along the route, participating nodes will send a Route Reply (RREP) packet to the source via intermediate nodes. With Path Accumulation (PA), these routes will be stored and used in the packet is forwarding has via the routes discovered beforehand [2]. Hence, routing overhead and flooding of packets will be reduced extensively. Above the implementation process has finished. After proposed to generate the possible type's prevention techniques like blackhole and flooding attack in LGF protocol and also overcome these attack.

This paper has organized as follows. Section 2 Implement the LGF protocol in MANET. Section 3 Prevention technique for blackhole attack in LGF protocol. Section 4 Prevention technique for flooding attack in LGF protocol. Section 5 Simulation results. Finally, section 6 will be concluding the paper and also future work, section 7 References. Above these sections are all discuses about briefly will be coming as give below.

2. Implement the LGF protocol in mobile ad-hoc network

The LGF protocol has implemented by GPS-free covered location tracking system with geocast-enhanced AODV [2], if we will be using with GPS means this is an infrastructure not eligible for LGF protocol because it is an infrastructure based. My proposed work of the LGF protocol is without any infrastructure and centralized system routing protocol in MANET. So this protocol particular distance only transmit the (RREQ) towards the destination node and also flood the (RREP) towards the source node, because it is GPS-free indoor location tracking system.

For example source 'S' to destination 'D' in between total Distance (DIST), DIST(S,D) =100 meters but DIST (S,4) =120 meters. Comparing these distance between DIST (S, 4) < DIST (S, D) = 120 < 100, this stipulation not satisfy and also automatically discard the RREQ packet because it is out of transmission area and another intermediate nodes in transmission coverage area in between source to destination DIST (S, 1) =40M, DIST (1, 3) =50M, DIST(2, 3)=60M, DIST (3, D) =65M, DIST(S, 2) = 62M, DIST (M, D) =70M, DIST (S, M) =55M, DIST (S, 5)=55M, DIST (5, D)=70M. Above these intermediate nodes distance conditions satisfy and also send the route request packets to all intermediate nodes. This is a way of functioning in LGF protocol.

2.1. Implementation of the LGF protocol

1. Source node wants to communicate with destination node.
2. The source node will multicasts the RREQ to all intermediate nodes with contain the IP address of the destination node and also distance from the source to destination.
3. The RREQ packet has received from the intermediate nodes; it will compare the distance in between source to destination.
4. Total distance between source to destination where, DIST(S, D) =100, these are all intermediate nodes distance from source to destination, DIST (S, 1) =40M, DIST (1, 3) =50M, DIST (3, D) =65M, DIST(S, 2) = 62M, DIST (2, 3) =60M, DIST (S, 5) =55M, DIST (5, D) =70M.
5. Now compare the distance for all nodes in between 'S' to 'D'.

```
If (intermediate nodes distance< source to destination node distance)
{
These are all the intermediate nodes in between 'S' to 'D', this conditions satisfy and also successfully sends the RREQ towards the destination node.
}
Else
```

{
Any intermediate nodes out of the transmission area in between 'S' to 'D' in the nodes sends Route Error (RRER) packet to the source node.
}
6. The RREQ has received from destination node, after send the RREP packet towards the intermediate nodes along with the source node.
7. The source node has received from RREP to intermediate nodes, after compare its distance from source to destination.
8. Whether the RREP to an intermediate nodes path has received exactly from source to destination node, the node will choose correct route and also send the original data packet to the destination node this is the algorithm for LGF protocol. The LGF protocol process diagram is given below.

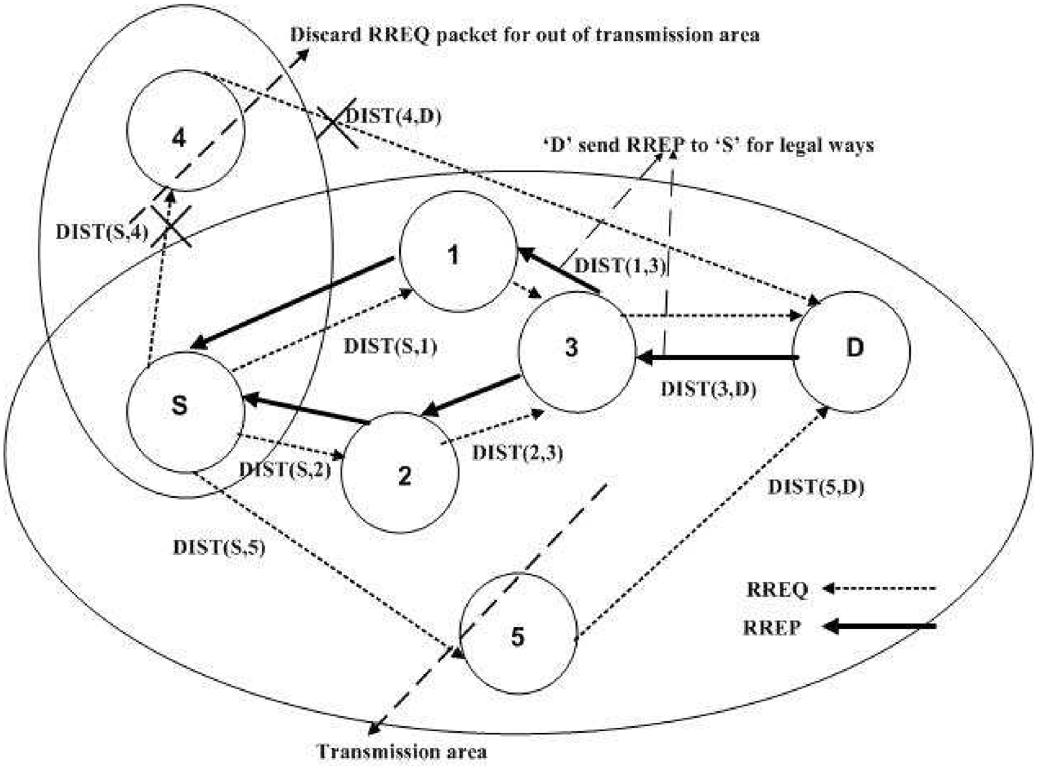


Figure 1. The LGF protocol implemented by GPS- free covered location tracking system

In this paper was existing protocol and attacks that is not a problem, if we will be establishing LGF protocol for the purpose of an applications will be developing like Military battlefield, Emergency rescue in the instant occurs means how can will safely communication between source to destination in between without any packet losses and also unwanted person do not attack in the protocol, if attack means. What can we do in this situation? So we have been implemented by two prevention techniques for each and every potential type of attacks in the LGF protocol. These are attacks as given below.

1. Blackhole attack
2. Flooding attack

Above this problem we shall facing means. You will generate the prevention techniques in LGF protocol and you will find the hateful node as the same time prevents the impact of vulnerabilities, after send the packets securely in between source to destination. This is the proposed work intent.

3. Prevention technique for blackhole attack in LGF protocol

In the blackhole attack source node receives more numbers of route reply RREP packets to the malicious node and also malicious node ahead of the RREP from intermediate nodes. It is the blackhole attack objective.

1. First source node sends the route request RREQ packet to all intermediate nodes along with the destination node.
2. After route request RREQ packet is received from the neighbour nodes and it will set the timer expired table for entire request nodes and will be stored in sequence order.
3. And also Collect Route Reply Table (CRRT) is monitoring which node repeatedly sends the Route Reply (RREP) packets to the source node.
4. In CRRT whether there is any repeated hop count node value is present in the reply paths it assumes the paths are correct reply path otherwise the chance of malicious paths is limited [3].
5. The malicious node no hop count node because it is drop the original RREQ packets towards the destination node in the process right chance to identify blackhole attack node.
6. The RREP such a way repeated hop count node value has received to source node after sends the original packets to right RREP path along with destination node. This is the way of prevent the blackhole attack in LGF protocol, and also the process diagram is given below.

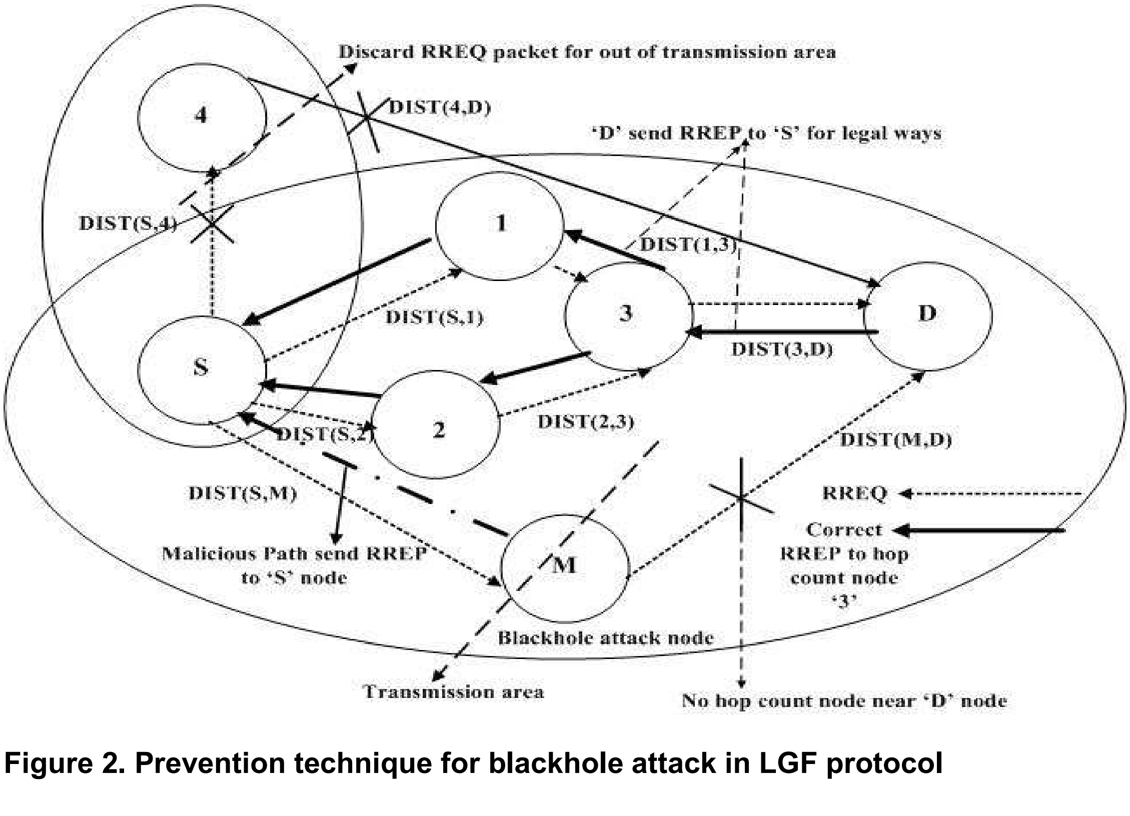
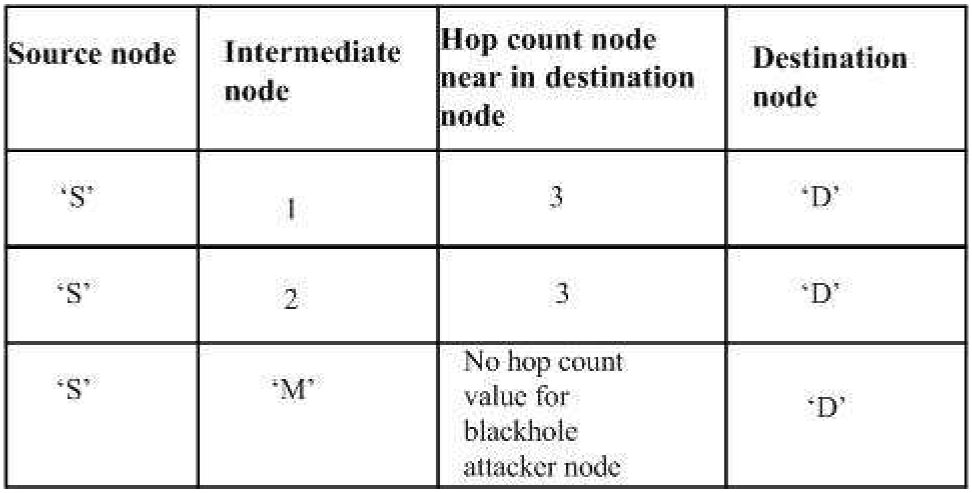

Discard RREQ packet for out of transmission area
4
DIST(4,D)
'D' send RREP to 'S' for legal ways
DIST(S,4)
1
DIST(1,3)
3
D
DIST(S,1)
DIST(3,D)
S
2
DIST(S,2)
DIST(2,3)
DIST(M,D)
DIST(S,M)
RREQ
Correct RREP to hop count node '3'
Malicious Path send RREP to 'S' node
M
Blackhole attack node
Transmission area
No hop count node near 'D' node

Figure 2. Prevention technique for blackhole attack in LGF protocol

Table 1. Collect route reply table (CRRT) for source to destination in is given below



Source node	Intermediate node	Hop count node near in destination node	Destination node
'S'	1	3	'D'
'S'	2	3	'D'
'S'	'M'	No hop count value for blackhole attacker node	'D'

3.1. Following steps of prevention technique for blackhole attack in LGF protocol

1. The blackhole attack intention is RREP suddenly sends the source node but legal hop count node takes some time after sends the RREP to intermediate nodes.

2. Find the safe RREP to an intermediate node towards the source node and also how can discover a legal RREP packet. There are some descriptions as given below to recover a safe RREP to intermediate nodes. Assume source node value = 1 and 2.

```
Intermediate nodes value = 1, 2.
Hop count node value = 3.
If (source node value == intermediate nodes value 1and 2)
{
Accept the RREP packet to source node.
}
Else
{
The Source node discards the RREP packet, because it is malicious node paths.
}
```

3. Above the condition has finished after source node waits and checks for safe route reply RREP packet to intermediate nodes.

4. After some time takes the destination node send the RREP packet to hop count node value 3.

5. The hop node has received from RREP packet, after send the RREP packet to intermediate nodes 1, 2.

6. Below the process to find the safe route reply an intermediate node.

```
If (intermediate nodes value 1, 2 < hop count nodes value 3)
{
Accept the RREP packet to intermediate nodes.
}
Intermediate nodes RREP packet has received, after send the RREP packet to
source node. Else if (source node value == intermediate nodes value 1 and 2)
{
Accept the RREP packet to source node.
}

Else
{
Discard the RREP packet to intermediate nodes.
}
```

7. These are all above the condition has been finished the source node has got the safe RREP packets to intermediate nodes.

4. Prevention technique for flooding attack in LGF protocol

The main intention of flooding attack is that the malicious node sends huge number of RREQ packets towards the destination node and also intermediate nodes cannot find out these types occurrences of the attacker node, but source node send one RREQ along with the destination node at the time of communication[4], so has been developed by Prevention Technique Transmission Table (PTTT), this table has used to found the legal RREQ in the LGF protocol and also record the legal RREQ packet has received and enroll existed communication routes. The flooding attack prevention process diagram is given below.

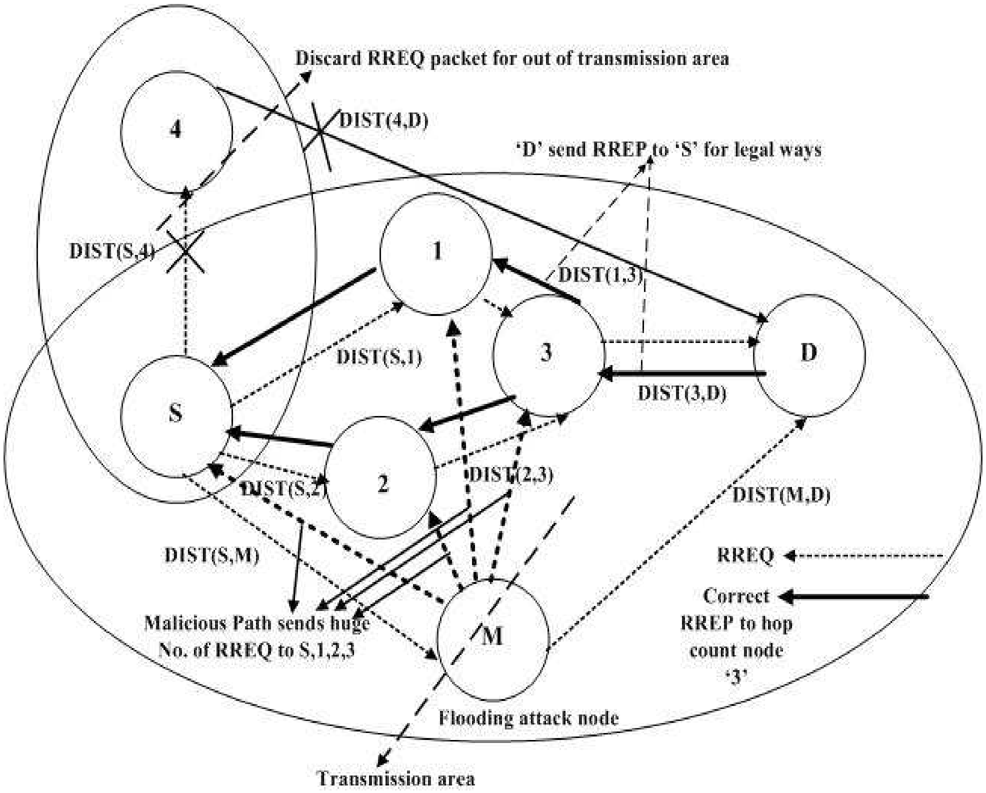
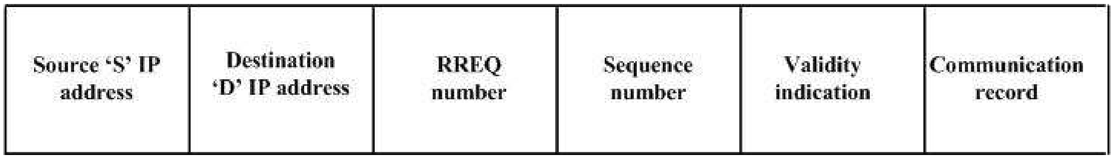

Discard RREQ packet for out of transmission area
DIST(4,D)
'D' send RREP to 'S' for legal ways
4
DIST(S,4)
1
DIST(1,3)
3
D
DIST(S,1)
DIST(3,D)
S
2
DIST(S,2)
DIST(2,3)
DIST(M,D)
DIST(S,M)
RREQ
Correct RREP to hop count node '3'
Malicious Path sends huge No. of RREQ to S,1,2,3
M
Flooding attack node
Transmission area

Figure 3. Prevention technique for flooding attack in LGF protocol

4.1. Following steps of prevention technique for flooding attack in LGF protocol

Format of Prevention Technique Transmission Table (PTTT) is given below.

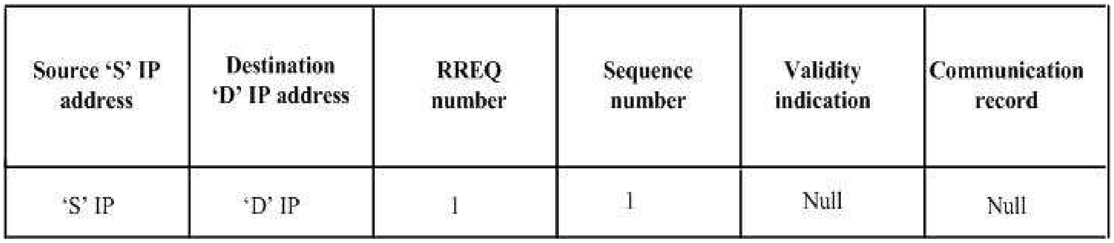
Table 2. Format of PTTT



Source 'S' IP address	Destination 'D' IP address	RREQ number	Sequence number	Validity indication	Communication record

4.1.1. RREQ value: The node 'S' wants to send packet to node 'D', it floods RREQ packet. Every node receiving this RREQ adds and item in its PTTT, fills the source IP address, destination IP address, sequence number according to the packet, and sets the RREQ Num as 1. After that, whenever receives a RREQ with the same source IP address, destination IP address and sequence number, this RREQ value will increase by 1. The RREQ value PTTT as given below.

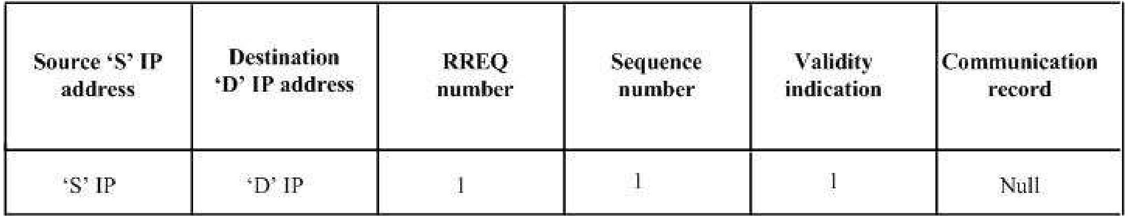
Table 3. RREQ value



Source 'S' IP address	Destination 'D' IP address	RREQ number	Sequence number	Validity indication	Communication record
'S' IP	'D' IP	1	1	Null	Null

4.1.2. Validity indication: After node 'D' receives RREQ from 'S', it adds corresponding item in its PTTT. Then 'D' sends RREP packet whose source IP address is 'S' IP address, destination IP address is 'D' IP address and sequence number is 1 through 'D' intermediate nodes, 3, 1 'S'. When this RREP reaches intermediate nodes, 3, 1, they check its validity. If node 'D' is found legal, they search their PTTT, and set corresponding items, validity indication as 1. Otherwise, it will discard this RREP packet and do not set the validity indication items PTTT as given below.

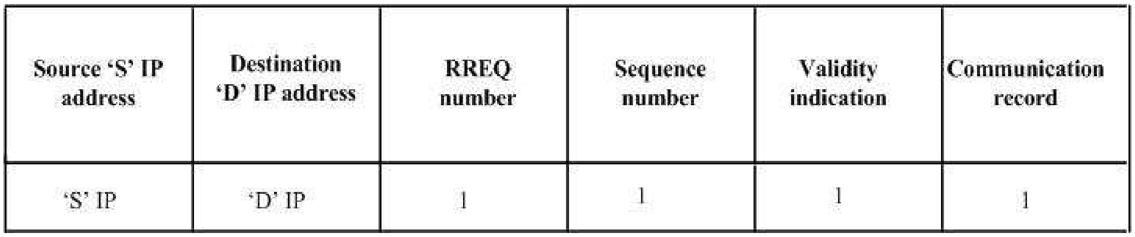
Table 4. Validity indication



Source 'S' IP address	Destination 'D' IP address	RREQ number	Sequence number	Validity indication	Communication record
'S' IP	'D' IP	1	1	1	Null

4.1.3. Communication record: When a node forwards a data packet, such as from 'S' to 'D', it sets the communication record of the item whose source IP address is 'S' and destination IP address is 'D' in its PTTT as 1. In this way, whenever sends a data packet, midway nodes set the corresponding Communication recording their PTTT by 1. For example, when a data packet sent by ‘S’ to ‘D’ passing through intermediate nodes like 3 and 1, they change their PTTT as show in table given below.

Table 5. Communication record



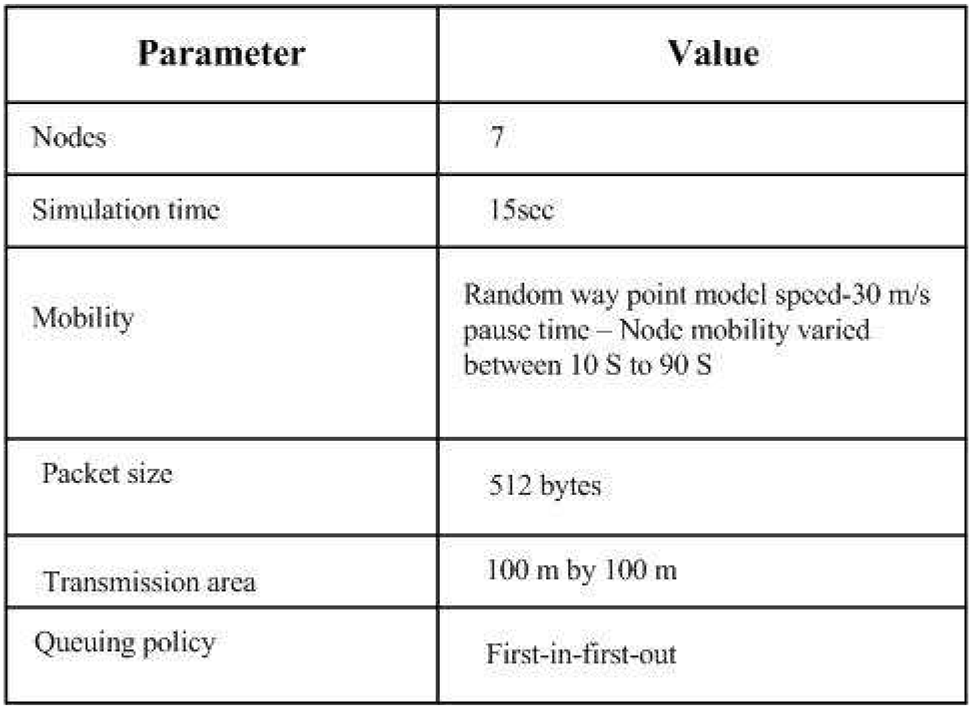
Source ‘S’ IP address	Destination ‘D’ IP address	RREQ number	Sequence number	Validity indication	Communication record
‘S’ IP	‘D’ IP	1	1	1	1

4.1.4. Deletion of items in PTTT: After two nodes finish the communication, source node will send RANC (Rout Announcement) to intermediate nodes. All the nodes receives RANC will delete corresponding items in their PTTT [5].

5. Simulation results

The simulation of work has done by GloMoSim version 2.03[6], a scalable environment for Mobile Ad-hoc Network.

5.1. Simulation parameters



Parameter	Value
Nodes	7
Simulation time	15sec
Mobility	Random way point model speed-30 m/s pause time – Node mobility varied between 10 S to 90 S
Packet size	512 bytes
Transmission area	100 m by 100 m
Queuing policy	First-in-first-out

5.2. Performance metrics

5.2.1. Average Packet Delivery Ratio: The packet delivery ratio (PDR) of a receiver is defined as the ratio of the number of data packet transmitted by the senders. The average packet delivery ratio is the average of the packet delivery ratios taken over all the receivers.

5.2.2. Average end- to- end delay: The end to end delay of a packet is defined as the time a packet takes to travel from the source to the destination. The average end to- end delay takes over all the received packets.

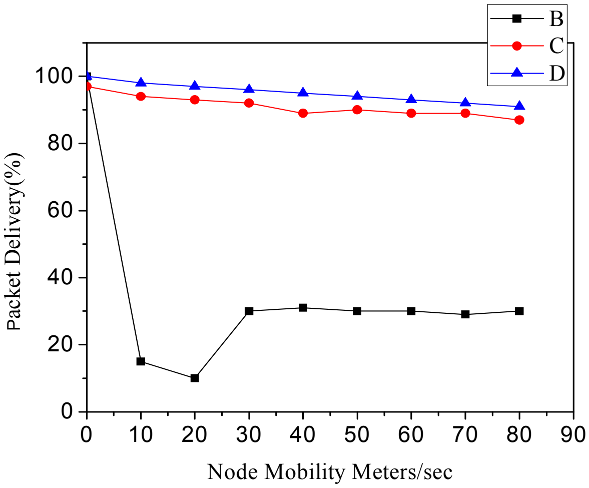


Figure 4. Packet delivery (%) in Prevention technique for blackhole attack in LGF protocol

Figure 4 Graph has mentioned line symbol 'B' is Normal LGF protocol has been implemented in MANET, line symbol 'C' is Prevention technique for blackhole attack solution provides in LGF protocol, line symbol 'D' is blackhole attack after in LGF protocol no solution provides.

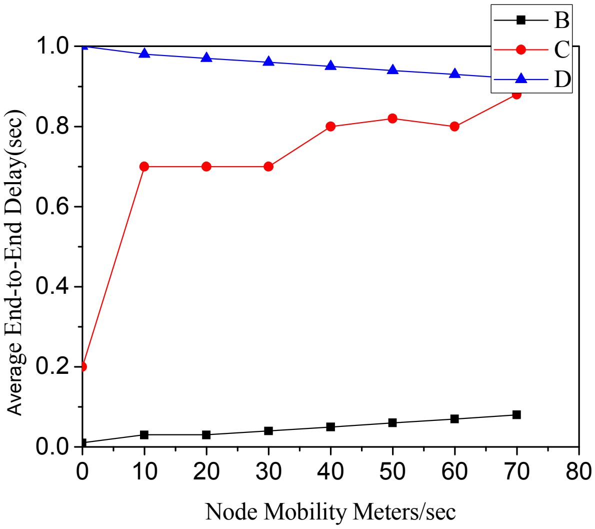


Figure 5. End to End delay in Prevention technique for blackhole attack in LGF protocol

Figure 5 Graph has mentioned line symbol 'B' is Normal LGF protocol has been implemented in MANET, line symbol 'C' is Prevention technique for blackhole attack solution provides in LGF protocol, line symbol 'D' is blackhole attack after in LGF protocol no solution provides.

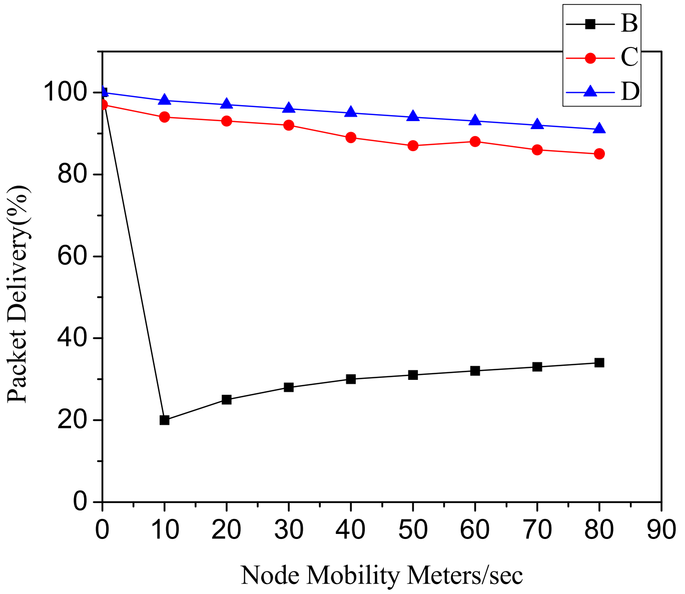


Figure 6. Packet delivery (%) in Prevention technique for flooding attack in LGF protocol

Figure 6 Graph has mentioned line symbol 'B' is Normal LGF protocol has been implemented in MANET, line symbol 'C' is Prevention technique for flooding attack solution provides in LGF protocol, line symbol 'D' is flooding attack after in LGF protocol no solution provides.

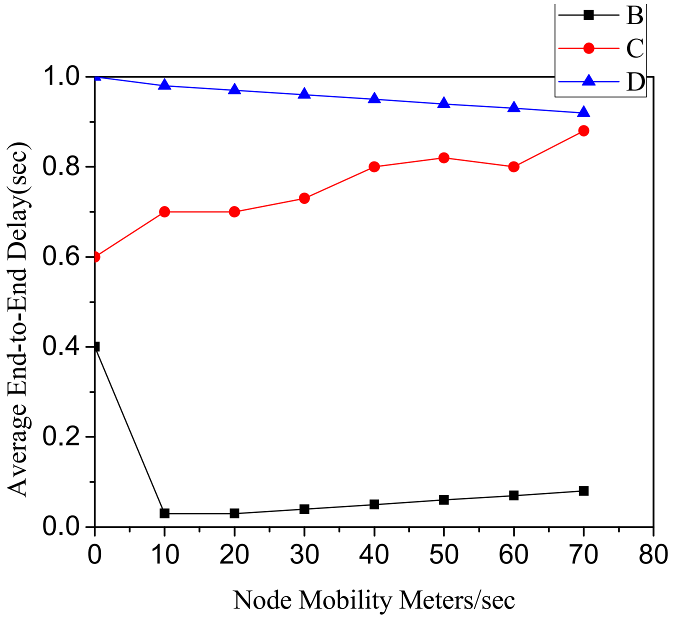


Figure 7. End to End delay in Prevention technique for flooding attack in LGF

protocol

Figure 7 Graph has mentioned line symbol 'B' is Normal LGF protocol has been implemented in MANET, line symbol 'C' is Prevention technique for flooding attack solution provides in LGF protocol, line symbol 'D' is flooding attack after in LGF protocol no solution provides.

6. Conclusion and future work

In this paper intend to prevent potential types of vulnerabilities like blackhole, flooding attack on location- based geocasting and forwarding (LGF) routing protocol in MANET. In this paper proposed to generate the prevention techniques for each and every attack on LGF protocol and also overcome the impact of vulnerabilities future will be making protected and efficient product to establish the real time applications. This is the conclusion about the paper.

In this paper two attacks only prevention techniques solution provides in LGF protocol, so remaining possible type's attacks is there, we will be choosing the attacks and generate the prevention techniques in LGF protocol. This is the further work of the paper.

7. References

[1] Luo Junhai, Ye Danxia, Xue Liu and Mingyu, "A Survey of Multicast Routing Protocols for Mobile Ad-Hoc Networks", IEEE Communications Surveys & Tutorials, vol. 11 No. 1,First Quarter 2009.

[2] L.A.Latiff, AAli[1], chia-ching,Ooi[2], N.Fisal[3], "Location- based Geocasting and Forwarding (LGF) Routing Protocol Mobile Ad hoc Network", Telecommunications, 2005. Advanced industrial conference on telecommunications/service assurance with partial and intermittent resources conference/e-learning on telecommunications workshop. Aict/sapir/elete2005. Proceedings on 17-20 July 2005.

[3] Latha Tamilselvan and Dr. V Sankaranarayana, "Prevention of Blackhole Attack in MANET", wireless Broadband and Ultra Wideband Communications, 2007. Auswireless 2007. The 2nd international conference on 27-30 Aug 2007.

[4] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, And Nei Kato, "A Survey Of Routing Attacks In Mobile Ad Hoc Networks", Wireless Communications IEEE, volume :14, issues:5, 2007.

[5] Shaomei Li, Qiang Liu, Hongchang Chen, Mantang Tan, "A New Method to Resist Flooding Attack in Ad Hoc Networks", Wireless Communications, Networking and Mobile Computing 2006(WiCOM 2006). International Conference on 22-24 Sept 2006.

[6] Jorge Nuevo, "A Comprehensible Glomosim Tutorial", INRS.

[7] J. Garcia- Luna- Aceves and E. Madruga, "The Core Assisted Mesh Protocol", IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, 1999.

[8] Hoang Lan Nguyen and Uyen Trang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", *Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06).*

[9] Nital Mistry, Devesh C Jinwala, Member, IAENG, Mukesh Zaveri, " Improving AODV Protocol against Blackhole Attacks", *Proceedings of the International MultiConference of Engineers And Computer Scientists 2010 Vol II, IMECS 2010,March 17-19,2010,HongKong.*

[10] Saman Desilva, Rajendra V. Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks", IEEE Communications Society/WCNC 2005.

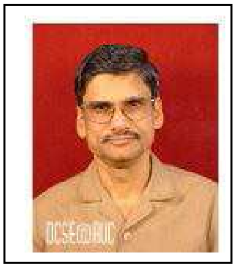
[11] J. Zhen and S. Srinivas, "Preventing replay attacks for secure routing in ad hoc networks", In ADHOC-NOW, LNCS 2865, pages 140–150, 2003.

Authors

D.kothandaraman received B.E. degree in Computer Science and Engineering during (2003-2007) from Dr. Pauls Engineering College, Villupuram District, Under Anna University, Chennai, Tamil Nadu, India. He received M.Tech. degree in Computer Science and Engineering(Information Security) during (2008-2010) from Pondicherry Engineering College, Pillaichavady, Under Pondicherry University(A

Central University), Puducherry-605014, India. His current research interest are mobile ad-hoc network security and computer networks.

A. Amuthan is a Assistant Professor in the Department of Computer Science and Engineering at Pondicherry Engineering College, Pillaichavady, Puducherry-605014, India. He recevide his B.Tech in Computer science and Engineering during (1992-1996) from Pondicherry Engineering College, Pillaichavady, Puducherry-605014, Under Pondicherry University(A Central University), India. He received M.E in Computer Science and Engineering during (2000-2002) from Anna University, Chennai, Tamil Nadu, India. His research areas are computer network and mobile ad-hoc network security.



Dr. C. Chellappan is a Professor in the Department of Computer Science and Engineering at Anna University, Chennai, India. He received his B.Sc. in Applied Sciences and M.Sc in Applied Science–Applied Mathematics from PSG College Technology, Coimbatore under University of Madras in 1972 and 1977. He received his M.E and Ph.D in Computer Science and Engineering from Anna University in 1982 and 1987. He was the Director of Ramanujan Computing Centre (RCC) for 3 years at Anna University (2002–2005). He has published more than 60 papers in reputed International Journals and Conferences. His research areas are computer networks, distributed/mobile computing and soft computing, software agent, object oriented design and network security.

Dr. N. Sreenath is a Professor and Head in the Department of Computer Science and Engineering at Pondicherry Engineering College, Pillaichavady, Puducherry-605014, India. He received his B.Tech in Electronics and Communication Engineering (1987) from JNTU College of Engineering, Ananthapur-515002, Andhara Pradesh, India. He received his M.Tech in Computer Science and Engineering (1990) from University of Hyderabad, India. He received his Ph.D in Computer Science and Engineering (2003) from IIT Madras. His research areas are high speed networks, optical networks.