Prevention of Wormhole and Rushing Attack 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],

[1, 2, 4]Department of Computer Science & Engineering (Information security)
Pondicherry engineering college, Pillaichavady,
Puducherry- 605014, India.

[3]Department of Computer Science & Engineering
Anna University, Chennai- 600025, Tamil Nadu, India.

ABSTRACT

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

Keywords: Wormhole attack; Rushing attack; LGF; Geocast-enhanced (GAODV); Mobile Ad-hoc Network (MANET); IN-Intermediate Node; Source S; Destination D.

1. INTRODUCTION

Application independence 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 from a temporary and dynamic wireless network on a shared wireless channel without the aid of a fixed networking infrastructure or centralized administration [1]. Hence, MANET is suitable an applications in exists such as give below.

1. Military battlefield
2. Emergency rescue
3. Vehicular communications
4. Urgent Business meetings

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 reduce rushing and overhead, 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 highlighted because Mobile Node (MN) in MANET is stand-alone devices and operates on batteries [2]. Performance evaluations of the protocol are packet delivery ratio and end to end delay.

This paper describe the real MANET test bed integration of GPS-free indoor location tracking system with on demand geocasting enhanced AODV. The LGF protocol source node will be multicast the Route Request (RREQ) packet to its entire Intermediate Nodes (IN) 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 intermediate nodes will be multicast the packets, otherwise it will discard and cancel its scheduled multicast 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 rushing of packets will be reduced extensively. Above the implementation process has finished. After proposed to generate the possible type's prevention techniques like wormhole and rushing attack in LGF protocol and also overcome these attack.

Rest of this paper has organized as follows. Section 2 Implement the LGF protocol in MANET. Section 3 Prevention technique for wormhole attack in LGF protocol. Section 4 Prevention technique for rushing attack in LGF protocol. Section 5 Simulation results. Finally, section 6 will be concluding the paper and also future work. 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 implementation because it is an infrastructure based. In the 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 packets towards the destination node and also flood the RREP packets 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 condition 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 (S,2)=52M,DIST (S,5)=70M, DIST (1, 3) =60M, DIST(2, 3)=65M, DIST (3, D) =80M, DIST (S, 4) =120M, DIST (4,D)=130M, DIST(5,6)=75M, DIST (6,D)=78M 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 in real MANET test bed

1. Source node S wants to communicate with Destination node D.
2. The source node S will multicasts the RREQ packets to all Intermediate Nodes (IN) with contain the IP address of the destination node D and also distance from the source S to destination D.
3. The RREQ packet has received from the intermediate nodes; it will compare the distance in between source to destination. Otherwise ignore it and also drop the RREQ packet.
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 (S,2)=52M, DIST (S,5)=70M, DIST (1, 3) =60M, DIST(2, 3)=65M, DIST (3, D) =80M, DIST (S, 4) =120M, DIST(5,6)=75M, DIST (6,D)=78M
5. Now compare the distance of intermediate nodes in between S to D.

```
If (IN are 1, 2, 5, 3, 6< Source S to Destination D node distance)
{
These are all the IN between S to D, these conditions satisfy and also successfully sends the RREQ packet towards the destination node.
}
Else
{
Any IN 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 packet has received from destination node, after send the RREP packet towards the intermediate nodes are 3, 1 and 3, 2 and 6, 5 along with the source S node.

7. The source S node has received from RREP packet to above these IN, after compare its distance from S to D.

8. Whether the RREP to an intermediate nodes 3 to1 and 3 to 2 and 6 to 5 path has received exactly, which nodes first received via shortest path link from source to destination node, will be come under first in first out policy basis that path only choose of Source S 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.

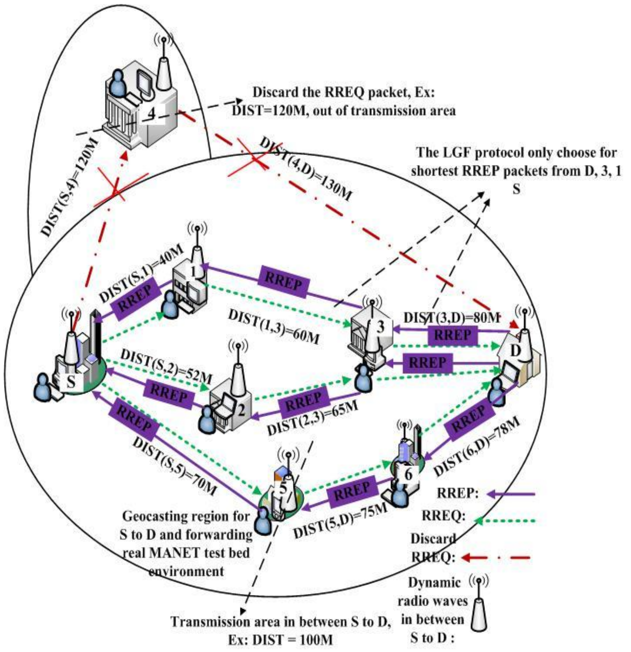

Discard the RREQ packet, Ex:
DIST=120M, out of transmission area
4
DIST(S,4)=120M
DIST(4,D)=130M
The LGF protocol only choose for shortest RREP packets from D, 3, 1 S
DIST(S,1)=40M
1
RREP
RREP
DIST(1,3)=60M
3
DIST(3,D)=80M
RREP
RREP
D
S
DIST(S,2)=52M
RREP
2
RREP
DIST(2,3)=65M
RREP
DIST(S,5)=70M
RREP
6
DIST(6,D)=78M
5
RREP
DIST(5,D)=75M
RREP:
RREQ:
Discard RREQ:
Geocasting region for S to D and forwarding real MANET test bed environment
Dynamic radio waves in between S to D :
Transmission area in between S to D, Ex: DIST = 100M

Figure: 1. The LGF Protocol Implemented by Real MANET Test Bed without Using GPS- free Covered Location Tracking System

In this paper existing for protocol and attacks that is not a problem, if we will be implementing real time in 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 attacker attack means. What can we do in this situation? So we have been implemented by two prevention techniques for each and every possible type of attacks in the LGF protocol. These are attacks as given below.

1. Wormhole attack
2. Rushing attack

Above this problem we shall facing means. We will generate the prevention techniques in LGF protocol and we will find the hateful node as the same time prevents the impact of attacks, after send the original packets securely in between Source S to Destination D. This is the proposed work intent.

3. PREVENTION TECHNIQUE FOR WORMHOLE ATTACK IN LGF PROTOCOL

A wormhole attack [3] is one of the most sophisticated and severe attacks in LGF protocol. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality [4]. Below the wormhole attack prevention technique process diagram is given below.

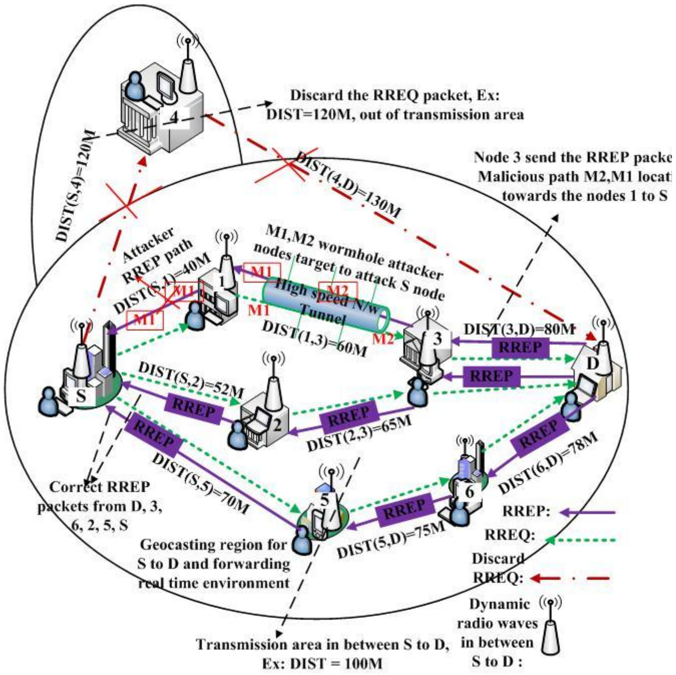
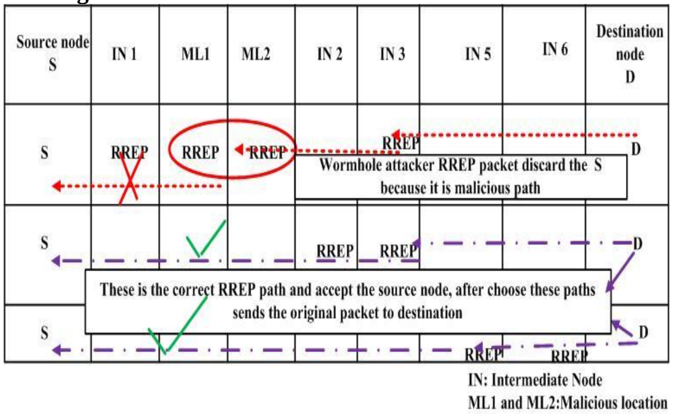


Figure: 2. Prevention Technique for Wormhole Attack in LGF Protocol.

Table 1. Collect Safe Route Reply table (CSRRT) for source node is given below



Source node S	IN 1	ML1	ML2	IN 2	IN 3	IN 5	IN 6	Destination node D
S	RREP	RREP	RREP		RREP			D
S		✓		RREP	RREP			D
S						RREP	RREP	D

Wormhole attacker RREP packet discard the S because it is malicious path

These is the correct RREP path and accept the source node, after choose these paths sends the original packet to destination

IN: Intermediate Node
ML1 and ML2:Malicious location

3.1 Following Steps for Wormhole Attack Prevention Technique in LGF

The wormhole attack objective is against a reactive routing protocol are two colluding attacker node target to attack Source S node.

1. Source S node multicast the RREQ packets towards the destination D node through IN values 1, 2, 5.

2. IN values 1, 2, 5 received RREQ packets from S node, after send the RREQ packets through IN value 1 to Malicious Location ML1 to ML 2 these paths are colluding attacker node suddenly send the RREQ packet to IN value 3 via Destination D node received first because it is malicious path link, but IN value 3-D and IN value 6-D are legitimate node it will take some time after reached RREQ packet to D.

3. The Destination D node multicast RREP packets towards the IN value 3 and 6.

4. IN value 3 will send the RREP packet through ML2 location to ML1 are colluding attacker location it will suddenly send the RREP packet to IN value 1 via S, if we will accept the RREP packet though this path destroyed the legal communication.

5. Now will find the safe RREP packet through IN value 1, 2, 5 there are some description to recover the safe RREP packet.

```
Assume- Source S node value 2, 5.
Intermediate Node IN values 1, 2, and 5.
If (Assume Source S node value 2, 5 == IN value 1, 2, 3)
{
Accept the RREP packet to Source S node.
}
Else
{
Discard the RREP packed to Source S node.
}
```

6. Above the condition has finished as well as Source S node discards the colluding attacker location ML1-ML2 RREP packets because it is malicious location path.

7. After some time the IN value 2, 5, are legitimate node and also legal paths of RREP packet to the Source S node.

Now some mechanism of find the safe RREP packets to legal paths.

```
If (Assume Source S node value 2, 5 == IN value 2, 5)
{
Accept the shortest legal path RREP packet to Source S node.
}
Else
{
Discard the malicious RREP packet to source node.
}
```

8. Above the condition are satisfies, after Source S node will choose accepted RREP packet path to send the original data packet towards the Destination D node. This is legal communication between S to D.

4. PREVENTION TECHNIQUE FOR RUSHING ATTACK IN LGF PROTOCOL

The rushing attack [5], acts as an effective denial-of-service attack against all currently proposed on-demand ad hoc network routing protocols. The main intention of rushing attack is that the malicious node suddenly sends the RREQ packets to IN value 3 towards the Destination D node has received first, but legal intermediate nodes are S-2-3-D and S-5-6-D it will takes some time after has received the legal RREQ packet to D, and also it will be taking some times after sends the RREP packets to Destination D node. This is rushing attack intention. The rushing attack prevention technique process diagram is given below.

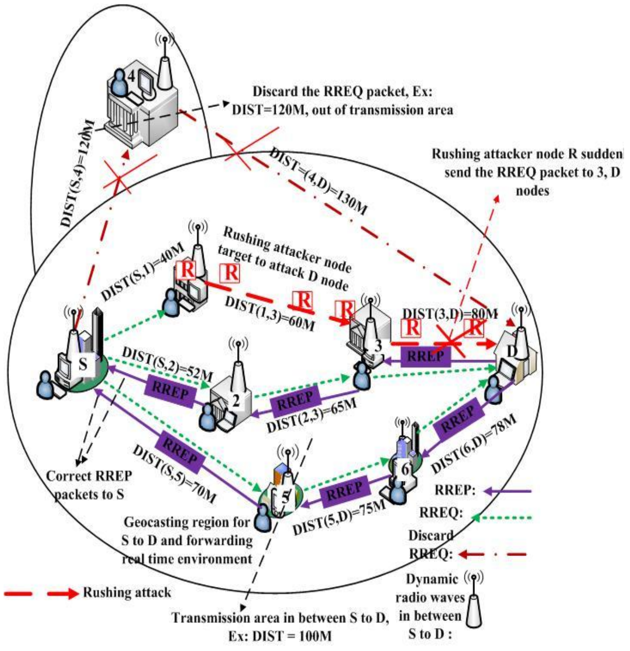
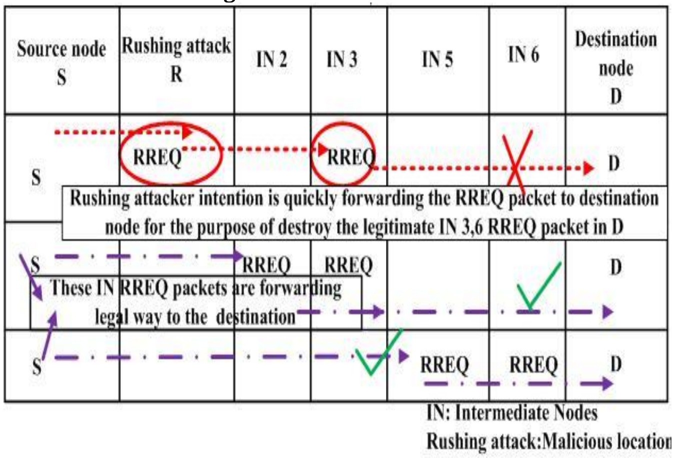


Figure: 3. Prevention Technique for Rushing Attack in LGF Protocol

Table 2. Collect Safe Route Request Table (CSRRT) for Destination D node is given below



Source node S	Rushing attack R	IN 2	IN 3	IN 5	IN 6	Destination node D
S	RREQ		RREQ			D
S		RREQ	RREQ		✓	D
S			✓	RREQ	RREQ	D

Rushing attacker intention is quickly forwarding the RREQ packet to destination node for the purpose of destroy the legitimate IN 3,6 RREQ packet in D

These IN RREQ packets are forwarding legal way to the destination

IN: Intermediate Nodes
Rushing attack:Malicious location

4.1 Following Steps of Prevention Technique for Rushing Attack in LGF Protocol

1. Source S node multicast the RREQ packets towards the Destination D node this is goal of the communication of the protocol.
2. First Source S node send the RREQ packets to S-R and S-2 and S-5 has received the RREQ packet from IN.
3. After received above these IN values to R, 2, 5, the Rushing R attacker node values are R-3 is malicious path quickly forwarding the RREQ packet to Destination D node. But intermediate nodes it will take some time after received the Destination D node.
4. Now will recover the safe RREQ packets from rushing attacker node.

There are preventive mechanisms as follows.

```
Assume- Destination D node value=6.
IN-Intermediate Node value near in D node=6
If (IN RREQ packet value 6 received to D == Destination D node value 6)
{
Accept the legal RREQ packet from IN value 6 to destination.
}
Else
{
Discard the malicious RREQ packet from Rushing R attacker node from IN value 3 via to Destination D node.
}
```

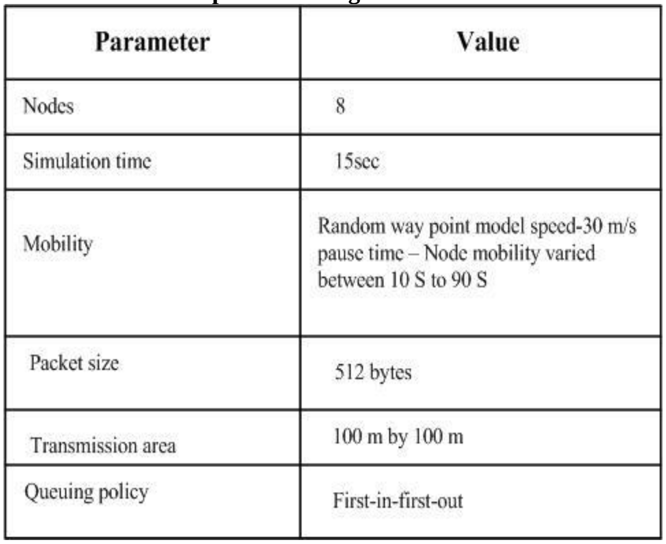
5. Above the condition are satisfies the Destination D node received legal RREQ packet from IN values are S-5-6-D.
6. After received destination D node RREQ packet it will send the RREP packet from IN values D-6-5-S.
7.The source S node received the RREP packet from IN value 5 in the path will be choose to send the real time data communication between S to D.

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

Table 3. Simulation parameter is given below



Parameter	Value
Nodes	8
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.

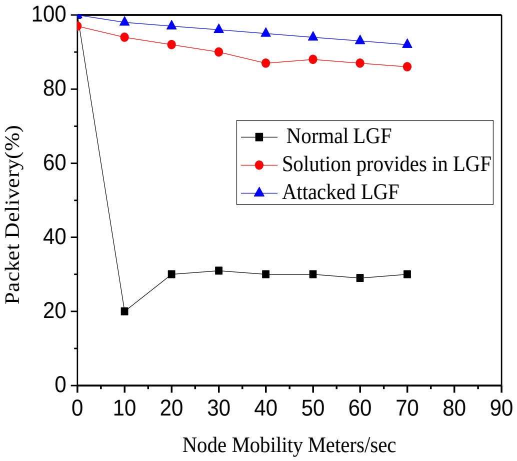


Figure: 4. PDR (%) of Prevention Technique for Wormhole Attack in LGF Protocol

Figure 4 Graph has mentioned line symbol "Normal LGF" protocol has been implemented in real MANET test bed, line symbol "Solution provides in LGF" Prevention technique for wormhole attack, line symbol "Attacked in LGF protocol" no solution provides.

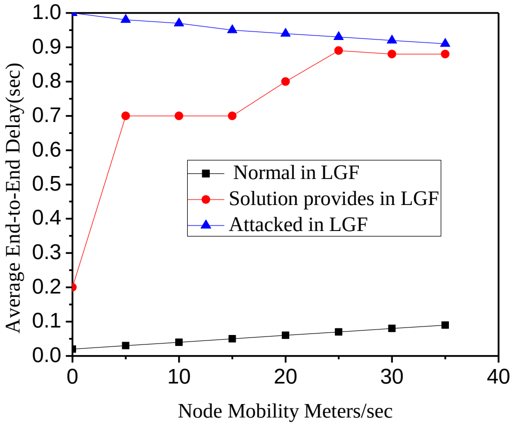


Figure: 5. End to End Delay of Prevention Technique for Wormhole Attack in LGF Protocol

Figure 5 Graph has mentioned line symbol "Normal LGF" protocol has been implemented in real MANET test bed, line symbol "Solution provides in LGF Prevention technique for wormhole attack, line symbol "Attacked in LGF protocol" no solution provides.

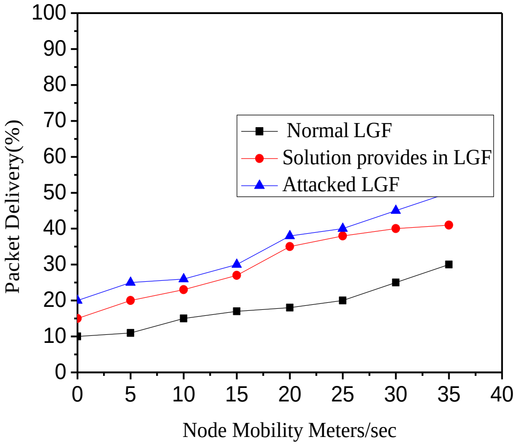


Figure: 6. PDR (%) of Prevention Technique for Rushing Attack in LGF Protocol

Figure 6 Graph has mentioned line symbol "Normal LGF" protocol has been implemented in real MANET test bed, line symbol "Solution provides in LGF" Prevention technique for rushing attack, line symbol "Attacked in LGF protocol" no solution provides.

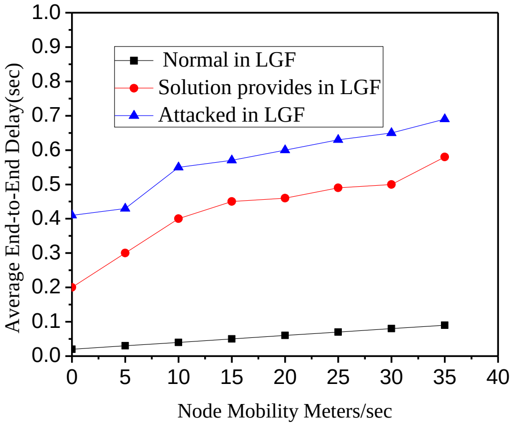


Figure: 7. End to End Delay of Prevention Technique for Rushing Attack in LGF Protocol

Figure 7 Graph has mentioned line symbol "Normal LGF" protocol has been implemented in real MANET test bed, line symbol "Solution provides in LGF" Prevention technique for rushing attack, line symbol "Attacked in LGF protocol" no solution provides.

6. CONCLUSION AND FUTURE WORK

In this paper intend to prevent possible types of attacks are wormhole and rushing attack on location-based geocasting and forwarding (LGF) routing protocol in MANET. In the proposed work to generate the prevention techniques for each and every attack in LGF protocol as well as overcome the impact of attacks in the protocol. Future will be making protected and efficient product to implement 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 future 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] Shalini Jain, Dr.Satbir Jain, "Detection and prevention of wormhole attack in mobile ad-hoc networks", International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010.

[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] V. Palanisamy, P.Annadurai, " Impact of Rushing attack on Multicast in Mobile Ad Hoc Network", (IJCSIS) International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009.

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

[7] 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).*

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

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

[10] G.S. Mamatha and Dr. S. C. Sharma, "A Highly Secured Approach against Attacks in MANETS", International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October, 2010.

[11] Li Shi-Chang, Yang Hao-Lan, Zhu Qing-Sheng, "Research on MANET Security Architecture Design", Signal Acquisition and Processing, 2010. ICSAP '10. International Conference on, 10.1109/ICSAP, 2010.19, Page(s): 90 – 93.