INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue5)

Available online at: www.Ijariit.com

Comparison of Gray Hole Attack in Manet in OLSR Protocol

ROHIT KATOCH
Department of Computer Science Engineering SRI SAI UNIVERSTY PALAMPUR

ANUJ GUPTA
Department of Computer Science Engineering SRI SAI UNIVERSTY PALAMPUR

Abstract: In this era of wireless devices, Mobile Ad-hoc Network (MANET) has become an indivisible part for communication for mobile devices. Therefore, interest in research of Mobile Ad-hoc Network has been growing since last few years. In this paper we have discussed GRAY Hole attack in OLSR routing protocols in MANET. Security is a big issue in MANETs as they are infrastructure-less and autonomous. Main objective of writing this paper is to apply gray Hole attack in MANET& know How its effect on the MANET Environment. This article would be a great help for the people conducting research on real world problems in MANET security

Keywords: MANET, Gray Hole Attack, OLSR.

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) has become one of the most prevalent areas of research in the recent years because of the challenges it pose to the related protocols. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an ―infrastructure less‖ network. The proliferation of cheaper, small and more powerful devices make MANET a fastest growing network. An ad-hoc network is self-organizing and adaptive. Device in mobile ad hoc network should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. Due to nodal mobility, the network topology may change rapidly and unpredictably over time. The network is decentralized, where network organization and message delivery must be executed by the nodes themselves. Message routing is a problem in a decentralize environment where the topology fluctuates. While the shortest path from a source to a destination based on a given cost function in a static network is usually the optimal route, this concept is difficult to extend in MANET. The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management. Because of these vulnerabilities, MANET is more prone to malicious attacks.

II. ROUTING PROTOCOLS FOR MANET:

Routing protocols in ad hoc networks vary depending on the type of the network [3, 4, 5]. Typically, ad hoc network routing protocols are classified into three major categories based on the routing information updated mechanism. They are proactive (table driven routing

Protocols), reactive (on-demand routing protocols) and hybrid routing protocols. In addition, protocols can also be classified according to the utilization of specific resources, such as power aware routing protocol and load aware routing protocols and so on.

2.1. **Proactive Routing Protocols:** Routes to all destinations are maintained by sending periodical control messages. There is unnecessary bandwidth wastage for sending control packets. Proactive routing protocols are not suitable for larger networks, as it needs to maintain route information every node's routing table. This causes more overhead leads to consumption of more bandwidth. Ex: DSDV [6, 7].

2.2 Reactive Routing Protocols: Routes are found when there is a need (on demand). Hence, it reduces the routing overhead. It does not need to search for and maintain the routes on which there is no route request. Reactive routing protocols are very pleasing in the resource-limited environment. However the source node should wait until a route to the destination is discovered. This approach is best suitable when the network is static and traffic is very light. Ex: DSR, AODV. [8, 9].

2.3 Hybrid Routing: The Ad Hoc network can use the hybrid routing protocols that have the advantage of both proactive and reactive routing protocols to balance the delay and control overhead (in terms of control packages). The difficulty of all hybrid routing protocols is the complexity of organizing the network according to network parameters. The common disadvantage of hybrid routing protocols is that the nodes that have high level topological information maintains more routing information, which leads to more memory and power consumption.

Security Attack

III. GRAY HOLE ATTACK

Gray hole attack **[3]** is a special variation of black hole attack, where nodes switch their states from black hole to honest intermittently and vice versa. It is difficult to detect gray hole attack because nodes can drop packets partially and behaves like a normal honest node.

Gray hole attacks is an active attack type, which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do sound behaves like malicious node. Initially the node behaves correctly and replays true RREP messages to nodes that initiate RREQ message. This way, it takes over the sending packets. Afterwards, the node just drops the some or all packets to launch a (DoS) denial of service attack **[5]**

If neighboring nodes that try to send packets over attacking nodes lose the connection to destination then they may want to discover a route again, broadcasting RREQ messages. Attacking node establishes a route, sending RREP messages. This process goes on until malicious node succeeds its aim (e.g. network resource consumption, battery Consumption). This attack is known as routing misbehavior **[5].**

It is a variation of black hole attack. In this attack node drops the packet selectively. Selective forward attack is of two types: While forwarding TCP packet dropping all UDP packets Dropping 50% of packets. In gray hole attack a node can behave as a normal node or a black hole node. So it is very difficult to find out the attack when it's behaving as a normal node.

OLSR Routing Protocol in MANET: "OLSR is a proactive routing protocol for mobile ad hoc networks. The protocol inherits the stability of a link state algorithm and has the advantage of having routes immediately available when needed due to its proactive nature. OLSR is an optimization over the classical link state protocol, tailored for mobile ad hoc networks."

Simulation: We create Manets network with 4 nodes and a mobile server is created in which all the nodes are connected to them. In this, two other nodes such as Application Configuration & Profile Configuration have been used. These are used to define the application definition & profile definition. GRP protocol manages a network & Shows how hello packet travels in the network. In this simulation we create a manet network with GRP Routing protocol & gray hole attack is applied on the network. In this network we apply a gray hole attack on node 3. By increasing speed of the hello message of the node3.Gray hole attack is different from Black hole attack because in which the data forwarding packet will not stop.

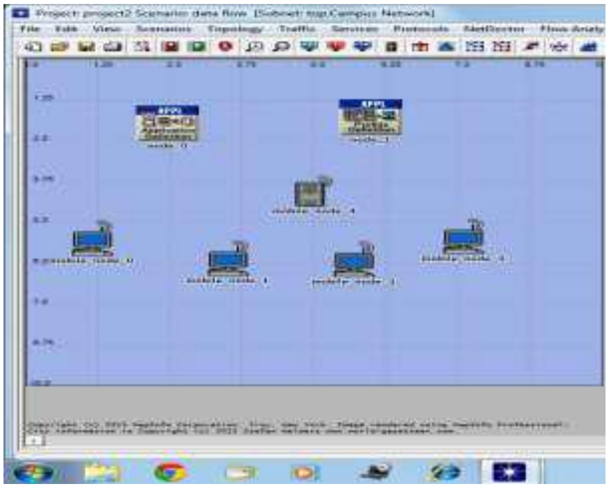

Fig 1.1 Manet Network

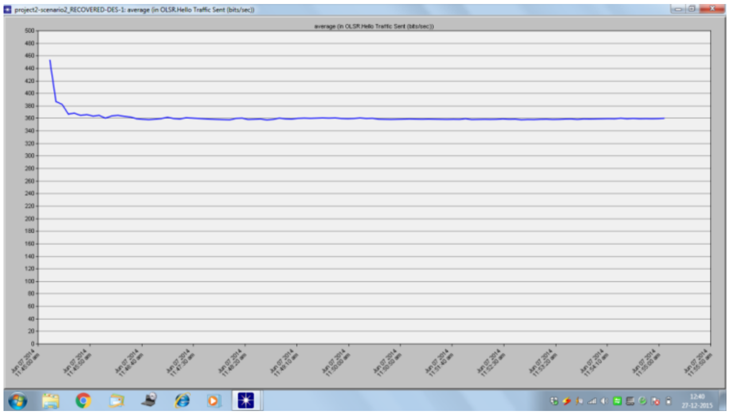

Fig 1.2 Comparison between MANET Network & MANET with Gray Hole

S.No	Factor	Scenario 2(Gray Hole)	Scenario 1
1	Hello Interval(sec)	10	5
2	Neighbor Expiry Time	20	10
3	Distance Moved	1000	1000
4	Position Request Timer	10	5

Table No .1 Comparison between MANET & MANET with Gray Hole Attack

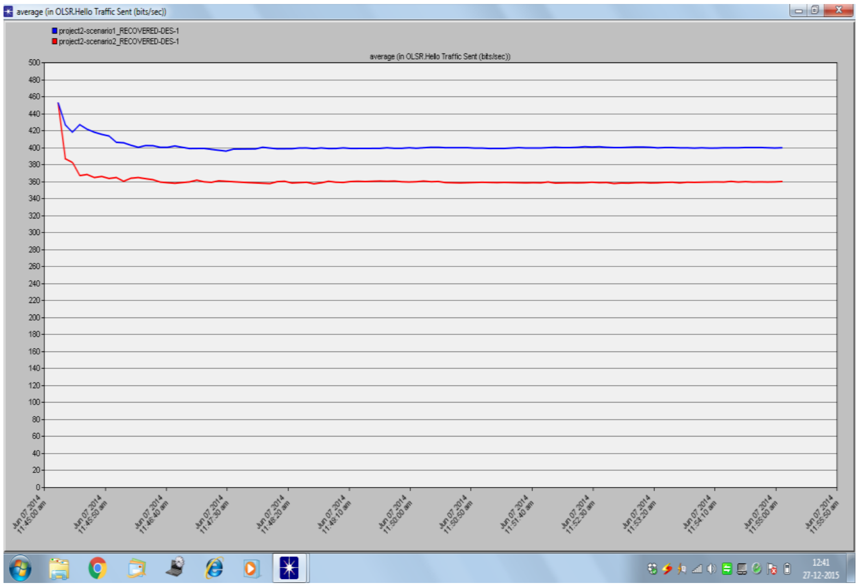

Fig 1.3 Comparison between MANET & MANET with Gray Hole Attack

From the comparison of the results of both the scenarios it has been find out that the packet bit rate decreased on applying the gray hole attack on the nodes. The data rate of data packet decreased from 400b/s to 350b/s.

CONCLUSION AND FUTURE WORK

A Gray Hole attack is one of the serious security problems in MANETs. It is an attack where a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. In this paper a gray hole attack is applied on MANETs The simulation Results show that the Network Performance is degrade when we applied gray Hole attack on that. In Future work various Protection Scheme will applied on the Manet Environment to reduce the effect of gray Hole attack.

REFRENCES:

[1] Wu, J., and Gao, M. ”On Calculating PowerAware Connected Dominating Sets for Efficient Routing in Ad Hoc Wireless Networks”, in Proc. of the 30th Annual International Conference On Parallel Processing,Valencia, Spain. Sept. 2001

[2] B. Chen, K. Jamieson, H. Balakrishnan, R. Morris, ”Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks”, in Proc. ACM International Conference on Mobile Computing and Networking, Italy, July 2001

[3] L. Hanzo (II.) and R. Tafazolli, “Quality of Service Routing and Admission Control for Mobile Ad-hoc Networks with a Contention-based MAC Layer”, Centre for Communication Systems Research (CCSR), University of Surrey, UK.-2005.

[4] Ronan de Renesse, Mona Ghassemian, Vasilis Friderikos, A. Hamid Aghvami, "Adaptive Admission Control for Ad Hoc and Sensor Networks Providing Quality of Service" Technical Report, Center for Telecommunications Research, King.s College London, UK, May 2005.

[5] H. Badis and K. Al Agha, “Quality of Service for Ad hoc Optimized Link State Routing Protocol (QOLSR)”, IETF-63 Meeting, Internet Engineering Task Force, , Vancouver, Canada, November 2005.Draft IETF.

[6] Venugopalan Ramasubramanian and Daniel Mossee “BRA: A Bidirectional Routing Abstraction for Asymmetric Mobile Ad Hoc Networks”, IEEE/ACM Transactions on Networking, Vol 16, No.1,February 2008.

[7] Hua Qu, Peng Zhang, Ji-Hong Zhao, “A New Local Repair Scheme Based on Link Breaks for Mobile Ad Hoc Networks”, 2009 Seventh Annual Communications Networks and Services Research Conference.

[8] Perkins C, E. Belding-Royer, and S. Das, “Ad hoc on-demand distance vector (AODV) routing,”IETFRFC3561,July2003.

[9] Doyle S L. Doyle, A. Kokaram, T. Forde. “Ad-hoc n etworking, randommarkov fields and decision making”. IEEE Signal Processing Magazine, 2006