Gray Hole Attack on TORA Routing Protocol with IMEP

Amandeep Gautam1 , Jasdeep Singh*2
1CSE Deptt., RIMT, Mandi Gobindgarh,
aman.gautam02@gmail.com
2CSE Deptt. RIMT , Mandi Gobindgarh,
Jassi42498@yahoo.com

Abstract: **The Temporary Ordered Routing Protocol (TORA) is a distributed routing algorithm that provides loop free routes from the source to destination. Internet MANET Encapsulation Protocol (IMEP) is used in TORA to avoid collision during packet transmission. In this paper, we will study about Impact of IMEP on TORA Routing Protocol and how gray hole attack will be implement on TORA Routing protocol and also will study its parameters.**

Keywords: **TORA, IMEP, Gray Hole.**

Introduction

A MANET is a Mobile Ad-hoc Network that consist multiple nodes capable of transferring data from source to destination without any physical media. MANET can be applied to different applications including battlefield communications, emergency relief scenarios, law enforcement, public meeting, virtual class room. MANET protocols are used to create routes between multiple nodes in mobile ad-hoc networks. The MANET protocols are classified into three huge groups, namely Proactive (Table-Driven), Reactive (On-Demand) routing protocol and hybrid routing protocols. [1]

1. Proactive Routing Protocol

Proactive routing protocols maintain consistent, up-to-date routing information from each node to every other node in the network. The routing information is kept in a number of different tables and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent.[2]

2. Reactive Routing Protocol

In Reactive or On-Demand Routing Protocols, routes are not predefined. For packet transmission, a source node calls for route discovery phase to determine the route. The route discovery mechanism is based on flooding algorithm which employs on technique that a node just broadcasts the packet to all its neighbours and intermediate nodes forwards the packets to their neighbours Some reactive protocols are Dynamic Source Routing (DSR), Ad hoc On-Demand Distance Vector (AODV), Temporally Ordered Routing Algorithm (TORA).[3]

3.Hybrid protocol

A hybrid protocol combines the characteristics of both the proactive and reactive routing protocols. An illustration of such a protocol is the Zone Routing Protocol (ZRP). In ZRP, topology is divided into zones and look for to utilize different routing protocols within and between the zones based on the weaknesses and strengths of these protocols.[4]

TORA

To work in such a network a highly distributed routing algorithm TORA is designed. Temporally-Ordered Routing Algorithm (TORA) is a distributed routing algorithm based on link reversal which provide multiple loop free routes to destination on demand through DAG i.e. Directed Acyclic Graph. TORA perform mainly three functions: 1. Route Creation 2. Route Maintenance 3. Route Erasure. Route creation establishes the DAG and provides all nodes with a route to a particular destination while route maintenance maintains the integrity of the DAG. Route erasure removes all invalid routes when a node detects that it is in a network partition with no route to the destination. In TORA routing protocol each node broadcasts a query packet and receives broadcast packet and update. It supports the loop-free; multiple routes services and provides better scalability. [5][6]

Internet MANET Encapsulation Protocol (IMEP)

IMEP provides services that TORA requires such as link/connection status sensing, broadcast reliability, and message aggregation. IMEP sits below TORA with both protocols residing at the network layer. IMEP is based on

1. Message Aggregation which encapsulates IMEP's own routing control packets and packets passed down by TORA into a single object block message (OBM). This minimizes the number of channel accesses needed since a single OBM packet is sent instead of multiple, smaller IMEP and TORA packets.

2. Link/connection status sensing provides TORA with accurate and current link status information of a node to its neighbours and whether the links are bi-directional or unidirectional. It operates using the explicit and implicit method of detecting link failures. In Explicit Method, method determines link status information by having a node i broadcast BEACON packets to its one-hop neighbours. When node i receives a reply in the form of an ECHO packet from a neighbour, it labels the link to that neighbour as bi-directional. In Implicit Method, it utilizes the OBM packets that IMEP sends, where nodes who receive an OBM packet reply with an ACK packet. This procedure mirrors that of the BEACON and ECHO packets used in the explicit method.
3. Broadcast Reliability: TORA requires broadcast reliability in the reliable and broadcast mode, ensuring insequence delivery of messages and broadcasting to all of its neighbouring nodes. The broadcast mode requires all neighbouring nodes to acknowledge any OBM packet sent and this facilitates link/connection status sensing in the implicit method of link failure detection. [6].

Gray Hole Routing Protocol

Gray hole attack is an attack in which some selective data packets are dropped by the malicious node. Gray hole attack is harder to find because of some data packets reached the destination and destination thinks that it is getting the full data. Gray hole attack in routing protocol occur at the time of routing the data packet. One of the major issue about the gray hole attacks is that it misguides the source by advertizing that there is a valid and shortest path to the destination. Thus the malicious node could do harm the network by degrading the network performance, disturbing route discover process. In Gray Hole attack we can't predict the probability of losing data.
In Gray Hole Attack a malicious node refuses to forward certain packets and merely drops them. The packets originating from a single IP address or a range of IP addresses selectively drops by attacker and forwards the remaining packets. [7] [8]

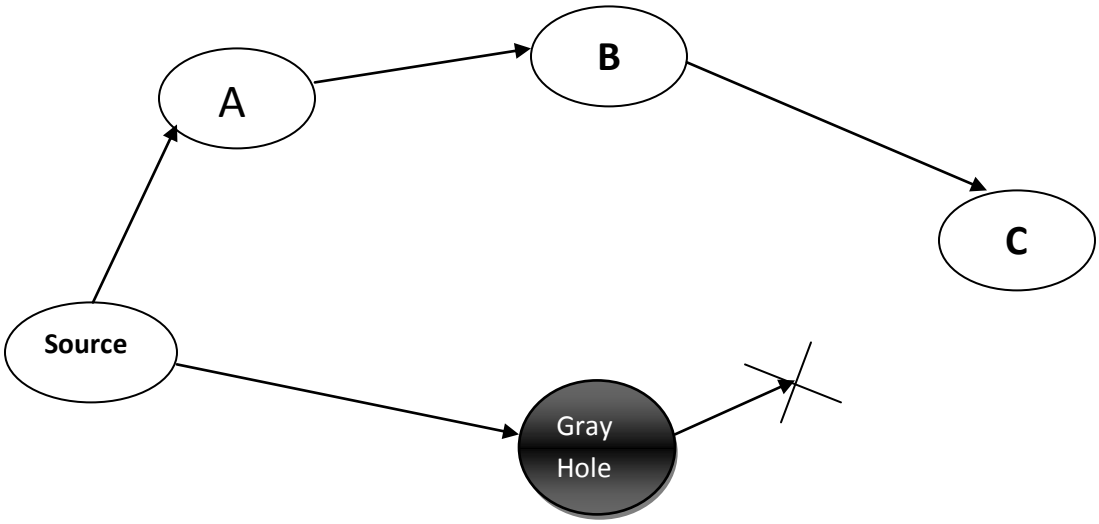

Fig: Gray Hole Attack

In Grayhole attack, node initially behaves normal then turns to malicious node after some time. A Grayhole may exhibit different malicious behaviour. It may drop packets either with certain probability or drop some packets corresponding to specific flow. It is an extension of blackhole attack where node drops the packet selectively. Such a Grayhole is known as selective forwarding. Another type of Grayhole node may behave maliciously for some time duration by dropping packets but may switch to normal behaviour later. A Grayhole may also exhibit a behaviour which is a combination of the above two, thereby making its detection even more difficult.[9]

The Gray Hole attack has two phases: Phase 1: A malicious node exploits the AODV protocol to

advertise itself as having a valid route to destination node, with the intention of interrupting packets of spurious route. Phase 2: In this phase, the nodes has been dropped the interrupted packets with a certain probability and the detection of Gray Hole attack is a difficult process. Normally in the Gray Hole attacks the attacker behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [8]. Both normal node and attacker are same. Due to this behavior it is very hard to find out in the network to figure out such kind of attack. The other name for Gray Hole attack is node misbehaving attack.[10]

Experimental Approach

In TORA Routing protocol, data is transfer on demand from source to destination. TORA Protocol works efficient when packets transfer on small network with small number of traffic connections. But the performance of the network drastically decreases with large number of traffic connections. With large connections, collision occurs during the transfer of data in the network. As TORA has to perform unnecessary route maintenance due to incorrect detection of link failure, this may cause congestion and delay in the delivery of packets. Internet MANET Encapsulation Protocol (IMEP) helps to resolve this problem by encapsulating IMEP's own routing packets and packets transfer by TORA in a simple object block message(OBM) and then sensing the link connection status. IMEP can detect this when it do not receive ECHO packets in response to a Beacon packet sent. This is an explicit method to sense link failure.

MANET network is created with 4 nodes and a mobile server was created in which all the nodes are connected to them. Two other nodes such as Application Configuration & Profile Configuration have been used to define the application definition & profile definition & defining the topology & configuration required for the network. After the implementation of the network, control traffic rate parameter of the network is checked and the performance of the network is compared.

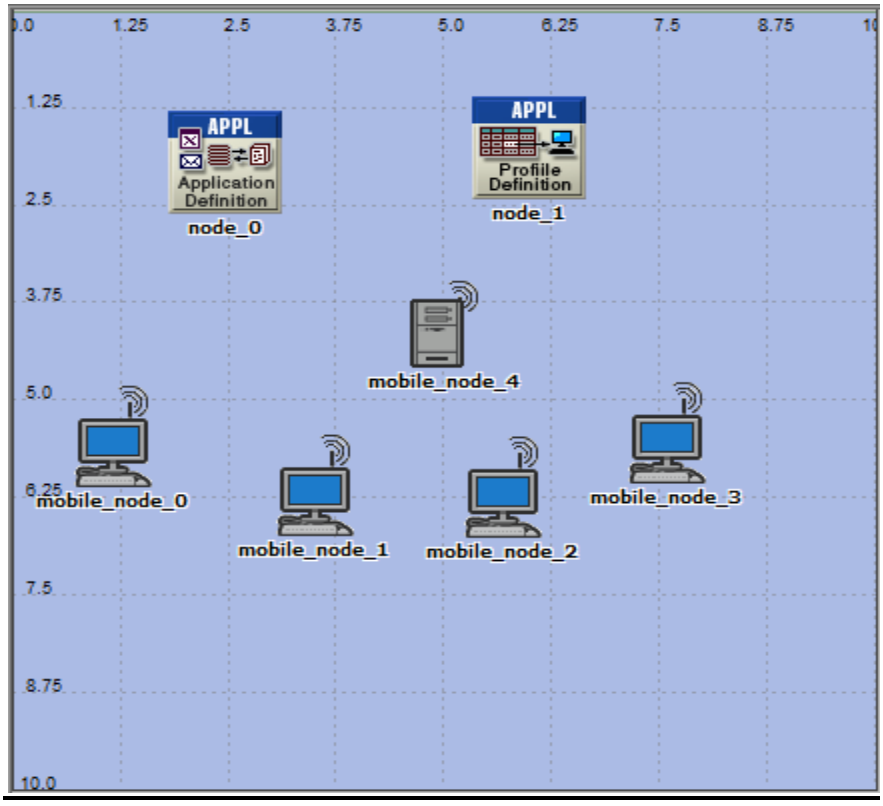

Fig 1. Network Setup of MANET

TORA Parameters With Gray Hole Attack

S.No.	Parameters	Network Without Grayhole Attack	Network Grayhole Attack
1	Beacon Period	20 sec.	20 sec
2	Maximum IMEP Packet Length	1500 Bytes	5000 bytes
3	Maximum Retries (No. of attempts)	3	10
4	Maximum Beacon Time	60 sec	60 sec

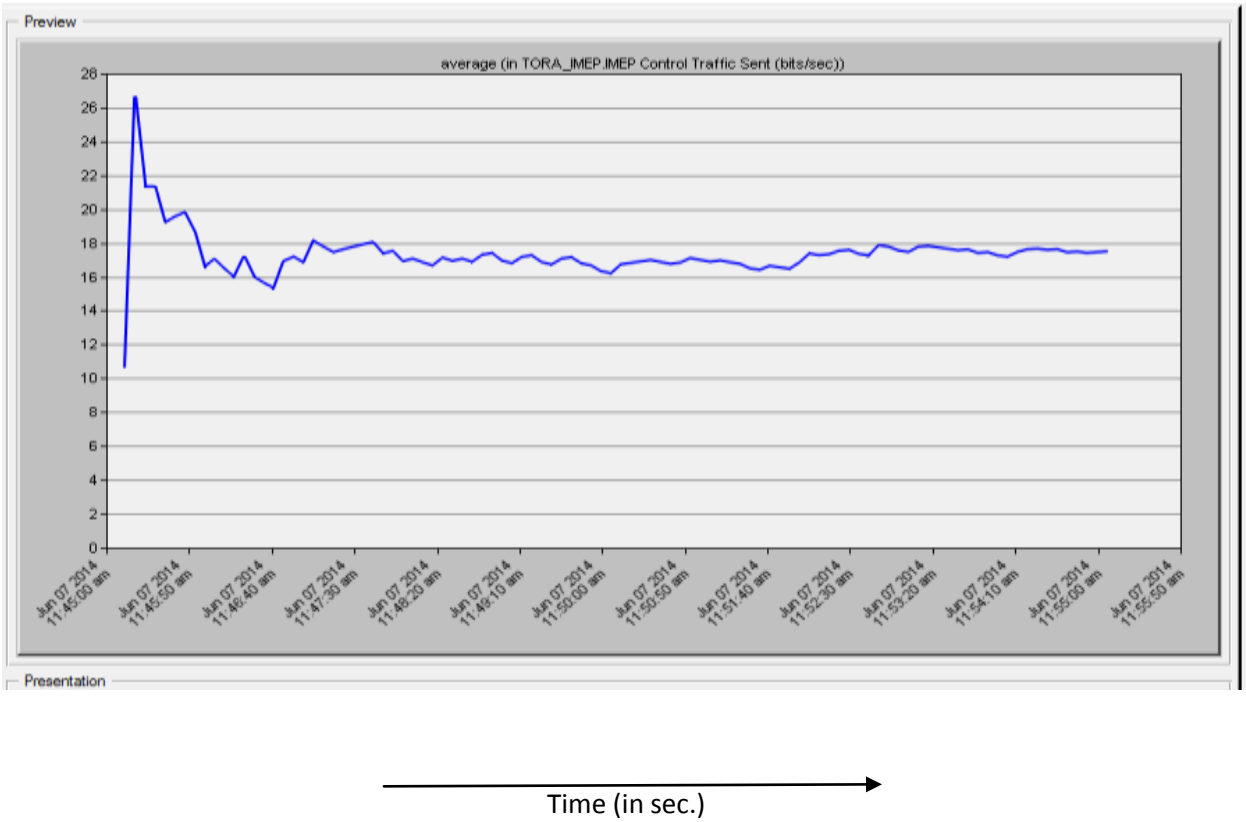

Fig 2. TORA Protocol with IMEP (traffic rate)

In TORA network, the control traffic sent rate of the network is 18 bits/sec. When we implement the Gray Hole attack on TORA routing protocol, the traffic rate of the network change. Attacker will read the data sending on the destination by implementing the Gray Hole attack, so it need more time to copy the data from network and the performance of the network would effected. In the setup of the gray hole attack network, Node 3 of the network is implement as gray hole node.

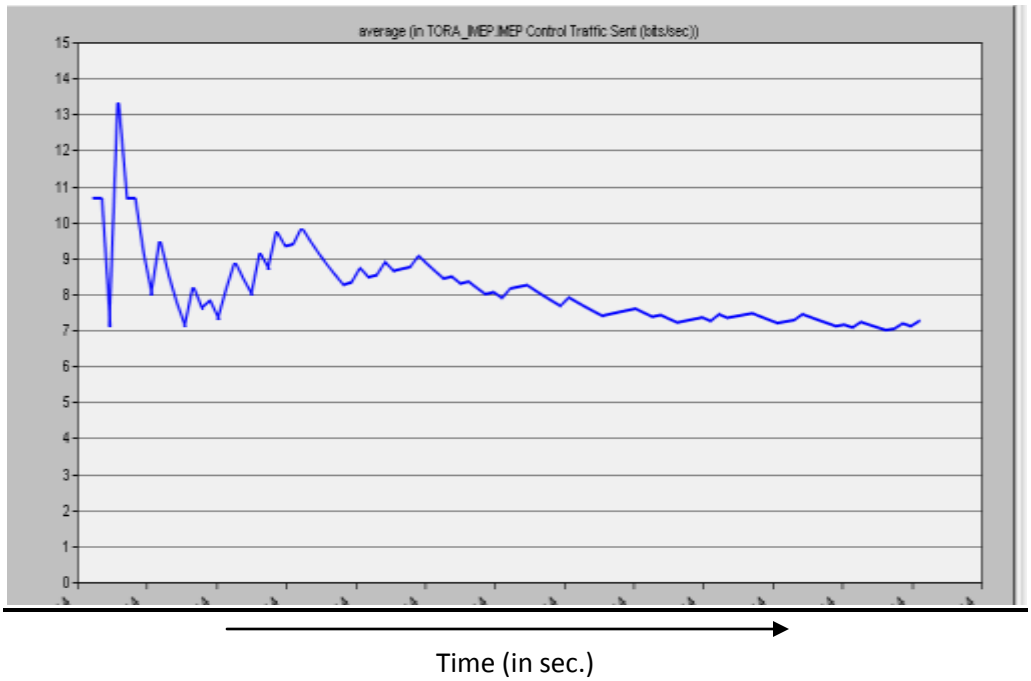

Fig 3. TORA with Gray Hole (control traffic rate)

With the implementation of the gray hole attack on the network, the control traffic rate of the network change . Now the control traffic sent rate is 8 bits/sec.

Comparison of the TORA with Gray Hole Attack

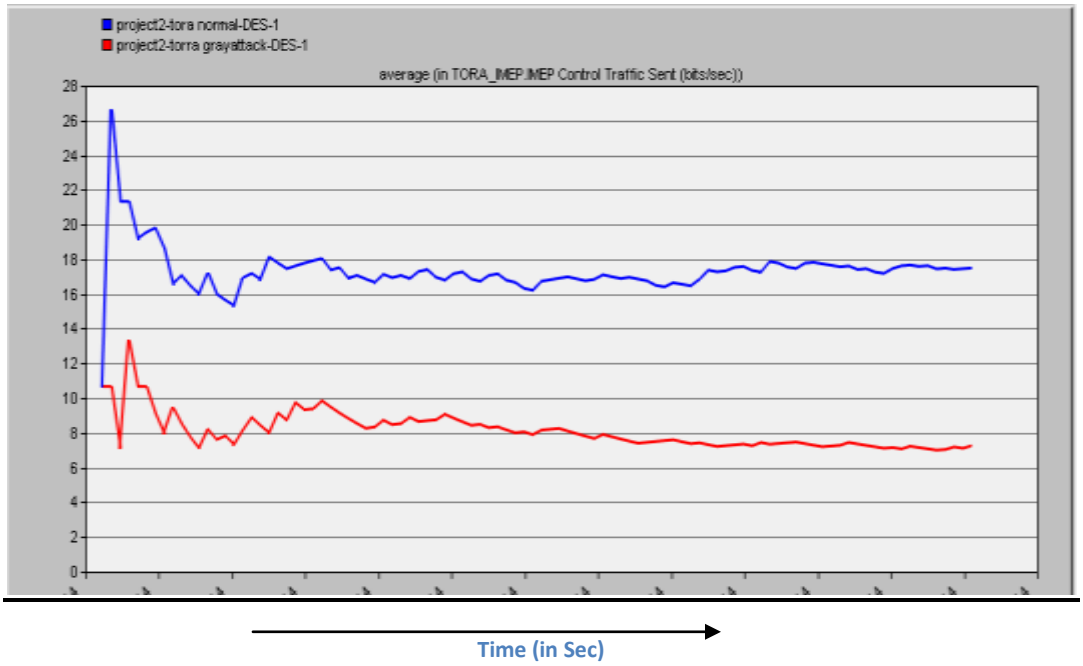

Fig 4. Comparison of TORA and Gray Hole

Conclusion

In TORA routing protocol, control traffic rate of the network is about 18 bits/sec without gray hole attack. But when we implement gray hole attack on the TORA routing protocol, the control traffic rate is 8 bits/sec. As the gray hole attacker reads or copy the data it needs time. So when we compare these control traffic rates, we got to know that the performance of the network decrease. As the traffic on the network will increase, the performance of the network will further degrade.

References

[1] Tamilarasan-Santhamurthy **"A Quantitative Study and Comparison of AODV, OLSR and TORA Routing Protocols in MANET"** Department of Information Technology, LITAM, Guntur, Andhra Pradesh, 522412, India.

[2] Er.Punardeep Singh Er**.**Harpal Kaur Er. Satinder Pal Ahuja, **"Brief Description of Routing Protocols in MANETS And Performance And Analysis"** Department of C.S.E, Kapurthala 144601 (Punjab)

[3] Sandeep Kaur, Supreet Kaur **" ANALYSIS OF ZONE ROUTING PROTOCOL IN MANET"** Punjabi University Regional Centre for IT & Management Mohali, Punjab, India.

[4] Kriti Gupta, Maansi Gujral and Nidhi **"Secure Detection Technique Against Blackhole Attack For Zone Routing Protocol in MANETS",** Department of computer science,Amity University,Noida, UP -201303, India

[5] A.VANI **" Study of MANET Routing Protocols TORA, LDR, ZRP",** ECE Department, CBIT, Telagana, INDIA

[6] Kwan Hui Lim and Amitava Datta **" An In-depth Analysis of the Effects of IMEP on TORA Protocol"** The University of Western Australia, Crawley, WA 6009, Australia.

[7] Avenash Kumar , Meenu Chawla **"Destination based group Gray hole attack detection in MANET through AODV"** Computer Science and Engineering Department MANIT Bhopal INDIA

[8] Mahesh Kumar Kumawat, Jitendra Singh Yadav **"A Survey on Detection and Prevention Techniques for Gray-Hole Attack in MANET"** Department of Computer Science Engineering JECRC University, Jaipur, Rajasthan, India

[9] Divya Khajuria Sudesh kumar " **Detecting multiple Blackhole and Grayhole attacks in MANETS by modifying AODV",** Department of computer science and engineering Shri Mata Vaishno Devi University,Katra, India

[10] Sandeep Kumar, Mrs. Sangeeta,Pramod Kumar Soni **" A Review on Gray Hole Attack in MANETs"** Dept of comp. CDLU Sirsa, INDIA.

