International Journal of Engineering Sciences Paradigms and Researches (IJESPR)
Volume 48, Issue 02, Quarter 02 (April-May-June 2019)
An Indexed, Referred Journal with Impact Factor: 2.80
ISSN (Online): 2319-6564
www.ijesonline.com

Black Hole Attacks Prevention in VANET

Varun Sharma[1], Dr. Sandeep Tayal[2], Ankit Bansal[3], Bijender Bansal[4], Monika Goyal[5]

[1]M. Tech. Student, Department of ECE, Vaish College of Engineering,
Rohtak, Haryana, India
varunsharma0325@gmail.com

[2]Associate Professor, Department of ECE, Vaish College of Engineering,
Rohtak, Haryana, India
tayalsan@gmail.com

[3]Associate Professor, Department of Electrical Engineering, Vaish College of Engineering,
Rohtak, Haryana, India

[4]Assitant Professor, Department of Computer Science and Engineering, Vaish College of Engineering,
Rohtak, Haryana, India

[5]Assitant Professor, Vaish Mahilamaha Vidyalaya,
Rohtak, Haryana, India

Publishing Date: June 04, 2019

Abstract

Mobile ad-hoc network (MANET) is a wireless network that can transfer the data from source to destination wirelessly. Now days this network is widely used all around the world because it does not require any fixed wired network to establish communication between the source and the destination. In today's scenario the mobile ad hoc network used in many real time applications like military surveillance, disaster management, air pollution monitoring etc. The mobile ad-hoc network due to the open communication medium has some security limitations there are the possibility of information leakage in the network. Many researchers are working on it to achieve the privacy concern. In MANET some routing protocols are also defined like reactive, proactive routing, and hybrid protocols. On these routing protocols there are attacks with harm the MANET for example black hole, warm hole, jellyfish, Sybil attacks etc. for these attacks some prevention techniques are their likewise AODV, PSO, Cluster-based intrusion technique, packet leases.

Keywords: *MANET, AODV, PSO, Protocols, DSDV.*

Introduction

The meaning of protocols is that it a set of rules which are commonly implemented and established for the proper transmission of information at both the ends. A network protocol is a set of well-known rules which imposes that how to design, transmit and receive data as a result the computer network devices from servers and routers end to end points can broadcast despite of the difference in their fundamental design or standard.

The routers communicates with each other is define by the routing protocol and the sharing of the information which allows them to choose routes among any of two on a computer network. On the internet routers achieve the "traffic directing" functions; the data packets are redirected by the networks of the internet from router to router till the data packets reaches the system destination.

The routing protocol utilizes routing algorithms and software to conclude most favorable network data transfer and broadcasting tracks between network nodes. Router communication is making possible by the routing protocols and generally considering network topology.

A routing protocol is also called as the routing policy.

Routing protocols are of following three types:
1. Proactive routing protocols,
2. Reactive routing protocols,
3. Hybrid protocols.

Now there some attacks on these routing protocols likewise black hole attacks, wormhole attack, Hello Flood attack, Sybil attack. In Black hole, falling every data packets going via it such as substance and force disappears from the space in a black hole. In wormhole, more than one attacking node are disturb routing by shorten the network, thus disturbing normally flow of the packets. In hello flood attacks, with a commanding transmitter the aggressor node floods the network with a great superiority route. In the Sybil attack, as pretending that it consisting of various nodes in the network this attack clears with itself by faking numerous identities.

There are some prevention techniques to prone these attacks for example- AODV, Packet lease, SMAC (Sensor MAC) etc. In Ad hoc On-Demand detachment Vector, The data and availability of network services are the issues that have to be achieved to provide a protected data transfer. For detecting against wormhole attacks a method called packet leash. A leash is the several data on which is attached with packet designed to confine utmost permissible broadcast distance of packets.

Review of Literature

Many researchers introduce the routing protocols and described in following section.

N.KOHILA, R.GOWTHAMI [1] describe the routing protocols are given below

Proactive Routing Protocols:

The table determined routing protocols are the proactive routing protocols. The data about the network topology even without require it contain by node, in which every node is used for maintaining for routing table in proactive routing protocols. This feature is useful for incurs significant singling traffic, datagram traffic, and also for power utilization. Whenever the changes in network topology in mean time the routing tables are updated. For large network these types of protocols are not used because to keeps node entries for each and every node in the routing table we use many singles nodes. These protocols are suitable for preserve different number of routing slabs changeable from protocol to protocol. There are different types of protocols are following:
Example: DSDV, CGSR, WRP etc.

Dynamic Destination-Sequenced Distance-Vector Routing Protocol (DSDV):

In DSD routing protocol, each one mobile node in the network maintain a routing slab. The number of hops and the list of all existing goals contains by each of the routing slabs. The objective node is originated by each slab entry is tagged with a succession figure. The routing slab supports to maintaining the topology details of the network by periodic transmission. If there is new modification which is important for the routing information, the modifications are broadcasted instantly. By use of distribution or multicasting the promoting is done.

Wireless Routing Protocol (WRP):

WRP distinct as the set of spread straight path algorithms that determine the path using information about the length and second-to-last hop of the straight path to every purpose and is belongs to the common class of path-finding algorithms. This protocols decreases the amount of case in which a temporary routing loop may occur.

Cluster Gateway Switch Routing Protocol (CGSR):

In the place of a plane network, this is a clustered mobile wireless network. The cluster heads are chosen using a cluster head collection algorithm for structuring the network into split but in interconnected troops. CGSR protocol gains a circulated processing method in the network by forming numerous clusters. The normal selection of cluster heads may resource ambitious and affect the routing performance, this the one disadvantage of this protocol. CGSR has the same transparency as DSDV. In the communication range of two or more cluster heads the nodes are the gateway nodes which are used inside the communication.

Reactive Routing Protocols:

This is also known as on demand routing protocols. In Reactive Routing protocol on demand bases the route is discovered nodes initiate route invention

whenever it is needed. When the source node sees the route store enemy in the path from source to objective if the route is not presented the it begins the route invention.

Dynamic Source Routing (DSR):

This is a type of reactive protocol which is based on the source route access. The protocol is basis which the source begins route invention for the bond state algorithm. The routes from source to objective are recognize by the senders and also involves the location of in-between nodes to the route data in form of packet. DSR was considered for multi bound networks for minute diameter.

Ad Hoc On-Demand Distance Vector Routing (AODV):

AODV is basically an upgrading of DSDV. In AODV it reduces the various communicate by generating routes based on demand, which are not in the case for DSDV. The neighboring transmits the data in the form of packet to nearby and the procedure runs until when the packet extends the goal. The intermediary nodes record the address of the neighbor for that the initial file of the transmit packet is received throughout the process of forwarding the route request. The record is saved in rote tables, which helps to build a back pathway. The respond is sent using the reverse pathway.

Associativity-Based Routing (ABR):

Associativity Based routing protocol describe a recent routing "degree of association stability" for an Ad Hoc networks. For association degree stability of mobile nodes a route is elected in this routing protocol. To show the broadcast each node generates the signals. After receiving the signal message, the neighbor node also updates associatively slab. Signal node is amplified of the associatively mark of the receiving node for each signal node. Associatively mark of the receiving node of the high value with the node beaconing way that the node is comparatively stationary.

Signal Stability–Based Adaptive Routing Protocol (SSA):

SSA protocol seeking for steadiest routes by the ad hoc network. For signal strength and position stability they perform on demand route invention. SSA detects weak and strong channels in the further classified into two supportive protocols:

- The Dynamic Routing Protocol (DRP) and
- The Static Routing Protocol (SRP).

DRP uses two tables:

- Signal Stability Table (SST) and
- Routing Table (RT).

Hybrid Routing Protocol:

The hybrid protocol is compromise between the proactive routing protocol and reactive routing protocols. On one hand the large transparency and less latency in the reactive protocols. Therefore this protocol is accessible to reduce imperfection of both the proactive and reactive protocol. Hybrid routing protocol is permutation of both the above describe protocol.

This protocol is utilizes the route detection method of reactive protocol and the table preservation method of proactive protocol. Hybrid protocol is appropriate for large network where large numbers of nodes are active.

Aniruddha Bhattacharyya, Arnab Banerjee [2] introduces the classification of attacks which porn the routing protocols.

Classification of Attacks:

Attacks are divided into two types- DATA traffic attacks and CONTROL traffic attacks.

Table 1: Types of Attacks

DATA traffic attacks	Control traffic attacks
-Black-Hole	- Worm-Hole
-Cooperative Black-Hole	- HELLO Flood
- Gray-Hole	-Cache Poisoning
- Jellyfish	-Sybil

Data Traffic Attack:

This attack deals with dropping of the nodes information packets passing through the attacks and the forwarding delay of information packets. Some attacks select tp prey packets for dropping and while some of attacks to drop all the packets irrespective of dispatcher nodes.

Black-Hole Attack:

In the black hole type of attack, a node is behaves likes a black hole named as nasty node, the data packets are dropped and passed during it as like matter and energy vanish from our space in a black hole.

Cooperative Black-Hole Attack:

This attack is comparable to above define black-hole attack, however in cooperative attacks many nasty node is used to interrupt the network concurrently. This is one of the most brutal data traffic attack and it completely interrupt the process of an ad hoc network.

Jellyfish Attack:

Jellyfish this attack is lightly dissimilar from black-hole & Gray-hole attack. The jellyfish attack is delays the place of dropping the data packets rashly.

Control Traffic Attack:

Due to its elementary feature, like open standard, spread nodes, independence of nodes involvement in the network, lack of federal ability which can apply safety on the system, spread coordination and collaboration of the MANET is obviously susceptible to attacks.

Worm Hole Attack:

Worm hole, in planetary term, in which it is, connects two isolated points in space through the shortcut route. The identical process is happen in which more than one attacking node can interrupt routing by malfunctioning the network in the MANET, so flow of packets are disturbed.

HELLO Flood Attack:

In this attack, with a commanding transmitter the aggressor node floods the network with a great superiority route. Therefore each node delivers their data packets towards this node in thought that this rout is much better to target.

Cache Poisoning Attack:

Normally in AODV, every nodes save some of the most current broadcast routes till the time up befall for every entry. So every route stays for the equal time in node's memory. If routing attacks is done by some nasty nodes will wait in node's route table till the time up befall for a better route is found.

Sybil Attack:

Sybil as pretending that it consisting various nodes in the network this attack clears with itself by faking numerous identities. Therefore a single node can play the role of multiple node which can be supervise or obstruct multiple node at the same time. If these attacks can be done on the blackmailing attacks, then the level of the interruption can be high. The identities are created in the system shows the achievements of the Sybil attacks.

Conclusion and Result

We see in AOVD, without removal of blackhole and with removal of blackhole, the generated packets, received packets, dropped packets in the form of table.

Table 2: Generated, Received and Dropped Packets

	Generated packets	Received Packets	Dropped Packets
Blackhole_0	7416	6475	513
Blackhole_1	3869	2978	860
With blackhole removal_0	7416	6475	513
With blackhole removal_1	6152	4872	504

Table 3: Packet Delivery Ratio

	Packet Delivery Ratio
Blackhole_0	87.311
Blackhole_1	76.97
With blackhole removal_0	87.311
With blackhole removal_1	79.193

In this table we see Packet Delivery Ratio with or without removal of blackhole.

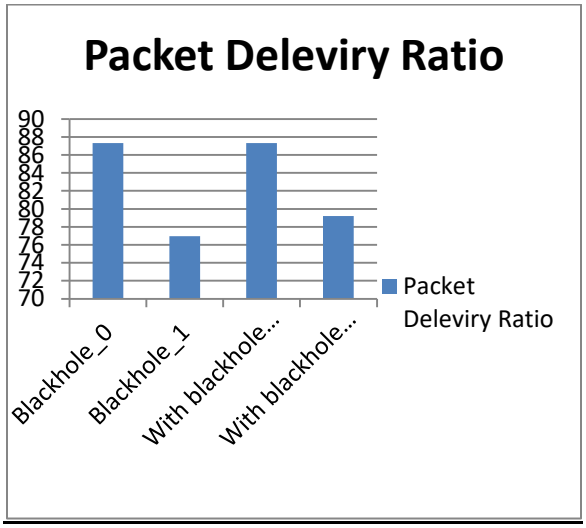

Figure 1: Chart on Packet Delivery Ratio

In this table we see the Loss ratio with blackhole removal and without blackhole removal.

Table 4: Loss Ratio

	Loss Ratio
Blackhole_0	12.688
Blackhole_1	23.029
With blackhole removal_0	12.688
With blackhole removal_1	20.806

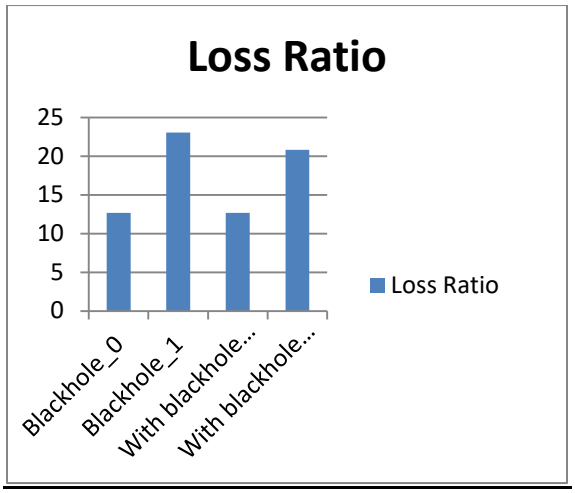

Figure 2: Variations on Loss ratio

In this table we see the Average End-to-End Delay with black hole removal and without black hole removal.

Table 5: Average End-to-End Delay

	Average End-to-End Delay(ms)
Blackhole_0	2.074
Blackhole_1	2.136
With blackhole removal_0	2.074
With blackhole removal_1	2.119

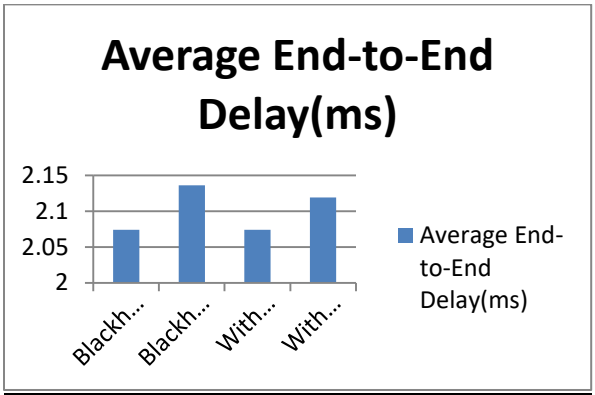

Figure 3: Chart on Average End-to-End Delay

In this table we see the Routing overhead with black hole removal and without black hole removal.

Table 6: Routing overhead

	Routing overhead
Blackhole_0	0.778
Blackhole_1	0.758
With blackhole removal_0	0.778
With blackhole removal_1	0.755

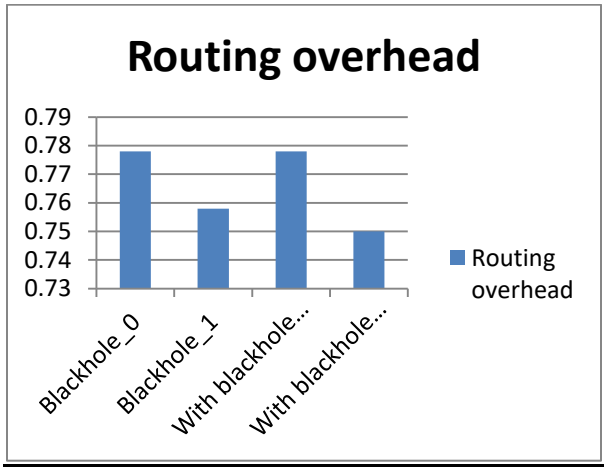

Figure 4: Variations in Routing overhead

Observation

In this thesis we study about the VANET, that how the VANET work its performance and its applications in various sectors. When we deal with the VANET we use routing protocols while using routing protocols some attacks occurs on it like blackhole, whormhole, jellyfish etc. So in this we study about blackhole attack.

In this blackhole attack in AOVD, without removal of blackhole and with removal of blackhole, we see the generated packets, received packets, dropped packets. We study the performance of AOVD with removal and without removal of blackhole and see the value of Packet Delivery Ratio, Loss Ratio, Average End-to-End delay and Routing overhead.

- In Packet Delivery Ratio, form this we found that for no blackhole and with blackhole removal no change in PDR means it don't degrade performance. But in case one blackhole PDR increases with using blackhole removal algorithms.
- In Loss Ratio, from this we found that for no blackhole and with blackhole removal no change in Loss Ratio means it doesn't degrades performance. But in case one blackhole Loss Ratio decreases with using blackhole removal algorithms.
- In Average End-to-End delay, we found that for no blackhole and with blackhole removal no change in Average End-to-End delay means it doesn't degrades performance. But in case one blackhole Average End-to-End delay decreases with using blackhole removal algorithms.
- In Routing overhead, we found that for no blackhole and with blackhole removal no change in Routing overhead means it doesn't degrades performance. But in case one blackhole routing overhead decreases with using blackhole removal algorithms.

Reference

[1] N.KOHILA, R.GOWTHAMI "Routing Protocols in Mobile Ad-Hoc Network" IJCSMC, Vol. 4, Issue. 1, January 2015.
[2] Aniruddha Bhattacharyya, Arnab Banerjee, Dipayan Bose "Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques", November, 2007.
[3] Mangesh A. Suryawanshi, Priyanka G. Bharude, Harish B. Mahale, Bhagyashri A. Hiwarale "Detection and Prevention of Black hole Attack in MANET" (IJSETR) Volume 06, Issue 05, May 2017.
[4] Shivani, Pooja Rani " Cooperative Black Hole Attack Prevention by Particle Swarm Optimization" (IJARCCE) Vol. 5, Issue 10, October 2016.
[5] Patel Pooja B, Patel Manish M, Patel Megha B "Jellyfish Attack Detection and Prevention in MANET: A Review" (IJAREST) Volume 4, Issue 3, March-2017.

[6] Jyoti Thalor, Ms. Monika "Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review" (IJARCSSE) Volume 3, Issue 2, February 2013.
[7] Tapalina Bhattasali, Rituparna Chaki, Sugata Sanyal " Sleep Deprivation Attack Detection in Wireless Sensor Network" (International Journal of Computer Applications) Volume 40– No.15, February 2012.