Performance Analysis of Blackhole Attack in MANETs

Vandana
M.Tech Student
Department of Electronics and Telecommunication
Siddaganga Institute of Technology
Tumakuru, India.

Suchitra V
Assistant Professor
Department of Electronics and Telecommunication
Siddaganga Institute of Technology
Tumakuru, India.

Abstract - MANET (Mobile ad-hoc network) is the complex that can be introduced when required, with no foundation or any sort of fixed stations. The hub movement is frequent and the topology must change progressively. MANETs are increasingly presented to the assaults. Among the various types of attacks on mobile ad-hoc network. Blackhole attack is a type of attack on AODV and DSDV. The information parcels are watched and dropped by the blackhole hub. In this type of attack all the data packets are observed and dropped by the blackhole node. Blackhole Detection System to detect blackhole is been proposed and performance analysis is done on the performance metrics to be considered to setup such mobile networks. We use NS-2.35 for the simulation and look at the after effects of AODV without blackhole, AODV with blackhole, DSDV without blackhole and DSDV with blackhole attack. Analyze the reactive and proactive routing protocols for the attack.

Keywords - MANETs, Blackhole attack, AODV, DSDV

I. INTRODUCTION

Mobile ad-hoc network (MANET) is a collection of number of nodes or terminals and that can communicate with each other without any centralized administrator, frequently changes in the topology of the network and the information sharing from nodes to nodes without any fixed infrastructure [1]. In AODV and DSDV protocol, during packet forward, valuable packets may dropped by malicious node present in the network. Link error and malicious packet dropping are the two sources for packet losses in MANET. This packet drop is due to blackhole attack.

Here we have been analyzed for three performance metrics such as end to end delay, energy consumption and the packet delivery ratio for both the protocols.

II. LITERATURE REVIEW

"Resisting Blackhole Attacks on MANETs" about blackhole attack in MANET and BRM (Blackhole Resisting Mechanism) mechanism to resist attack. BRM mechanism provide better efficiency in all metrics of the network than AODV and SAODV [6].

"Gray Hole Attack Detection Prevention and Elimination using SDPEGH in Manet" about grayhole attack and proposes Secure Detection Prevention and Remove Gray Hole (SDPEGH) technique, CRCMD and R (Cluster and Reputation Based Cooperative Malicious Node Detection and Removal Structure) is the existing technique. The performance metrics was analyzed for proposed and the existing systems concluded that the proposed system performance is effective than the existing one [7].

III. ROUTING PROTOCOLS IN MANET

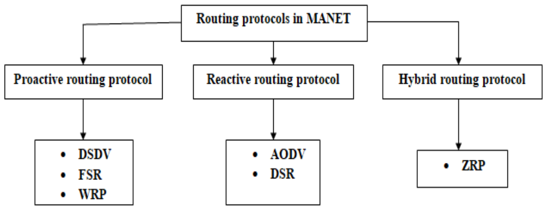
Routing protocols in MANET
Proactive routing protocol
Reactive routing protocol
Hybrid routing protocol
• DSDV
• FSR
• WRP
• AODV
• DSR
• ZRP

Fig 1: Classification of routing protocols in MANET

A. Protocols on Proactive Routing

Proactive routing protocols are table driven routing protocol [2]. This table driven routing protocols aim to maintain routing details from each and every node in the network. And these routing protocols allow each node to store routing information on one or more routing tables.

Example: DSDV, WRP, FSR.

B. Protocols on Reactive Routing

Reactive protocols are also known as on-demand protocols, these protocols generates routes only if needed. When a node needs a path to send information or to send packets to its destination, it initiates the process of path discovery within the network.
Example: AODV, DSR.

C. Protocols on Hybrid Routing

Protocols on hybrid routing are the combination of both proactive and reactive protocols.
Example: ZRP.

AODV routing protocol

In AODV protocol the routes are maintained only between the nodes which need to communicate [5]. Route Requests (RREQ) are forwarded to the nodes. If a route request is re-broadcast by the node, it sets up a reverse path pointing to the source. The destination node receives a Route Request, and that destination node replies by sending a Route Reply (RREP) travels along the reverse path set-up when Route Request is forwarded.

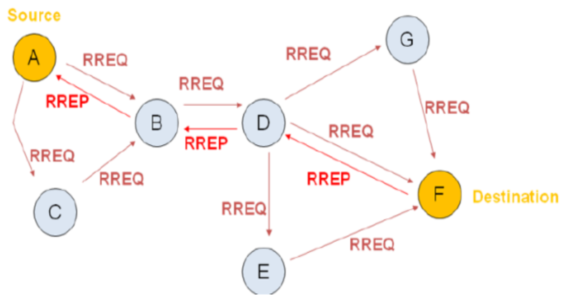

Fig 2: AODV route discovery

DSDV routing protocol

DSDV is known as Distributed Bellman-Ford or RIP (Routing Information Protocol). Every node maintains a routing table in the network contains all available destinations, the next node to reach the destination and it also contains the number of hops to reach the destination. In order to preserve topology, update table regularly to all neighbours.

DSDV is proactive routing protocol (Table Driven Routing Protocol) each node in the network maintains routing information for all known destinations and it is important that to update the routing information regularly. Also if there is no improvement in network topology, traffic overhead retains routes that are never used. DSDV allows rapid reaction to changes in topology, makes immediate route advertisements about major changes in routing table.

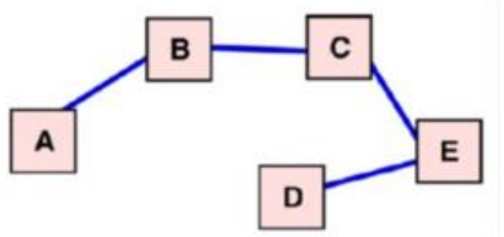

Fig 3: DSDV route discovery

MANETs are easily harmed by the attacks or more vulnerable to attacks [3] [4]

IV. TYPES OF SECURITY ATTACKS

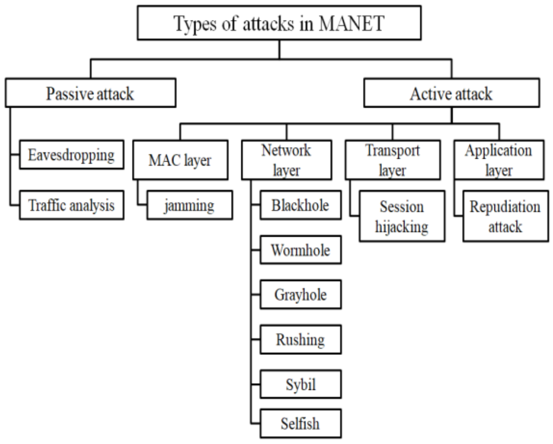

Fig 4: Types of attacks in MANETs

A. Passive Attack

Passive attacks are the assault that would not properly connected with the network [3]. Hackers leak information shared without altering it. Such assaults are hard to trace so because system activity itself is not impacted.

B. Active Attack

An successful attack attempts to alter or harm the data exchanged there within the network by interrupting the normal functioning of the network [4]. Active attacks may occur indoors or outdoors.

External attacks are conducted by nodes that are not part of the network. External attacks come from compromised network nodes. Because the intruder is already a part of the network, internal attacks are more serious and hard to detect than external attacks.

V. SYSTEM ARCHITECTURE

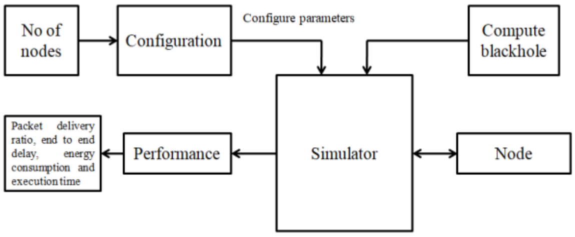

Fig 5: System Architecture

In fig 5 each module performing below operations such as,

Configuration: It takes the number of nodes as input and the configuration parameters are supplied to the simulator in the mentioned architecture during the configuration network..

Simulator: Simulator is used for simulating network behaviour such as power consumption and sending data between nodes in the network.

Node: The ad-hoc network consists of node collection and the data is transferred from source to destination node using intermediate nodes.

Sink node: All data packets are received from nodes via this node. Users use these data gathered to analyze their targets.

Blackhole node: Blackhole node reflects a serious assault on the network routing protocol. The malicious node in this attack fakes other nodes by announcing a shortest false route to the destination. The malicious node then absorbs additional traffic, and continuously drops the packets.

VI. BLACKHOLE ATTACK

Using the AODV protocol, the mobile ad-hoc network faces a blackhole attack in which a malicious node or blackhole node absorbs the network attack and all data packets are lost.. The fig 6 shows that the node B is the node of malicious node or the node of blackhole. Once node A broadcasts node D's RREQ message to set a path for data transmission, node B immediately responds to node A with a false RREP message indicating that it has the highest node D sequence number, as if it originates from node D.

Node A believes node D is 1 hop count behind node B, and discards the newly obtained RREP packet from node C or E. node A will then start sending all data packets to node B. Node A is optimistic that these packets will reach node D but node B will drop all packets of the data. The node of malicious node or the node of blackhole takes all the routes upto itself. This prevents any information or packet being forwarded to any other nodes. The network operation is hampered because the packets are easily consumed by the blackhole node B.

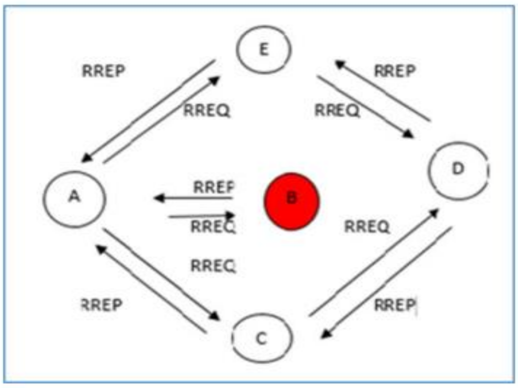

Fig 6: A single blackhole attack in MANET

Table 1: Simulation Parameters

Parameter	Value
Simulator	NS-2 (Version 2.35)
Type of Channel	Wireless Channel
Radio Propagation Model	TwoRayGround
Network Interface Type	WirelessPhy
MAC Type	802_11
Interface Queue Type	DropTail/PriQueue
Link Layer Type	LL
Antenna	OmniAntenna
Maximum Packet in ifq	50
Area (M*M))	900*900
Number of Mobile Nodes	10-100
Source Type	UDP
Routing Protocol	AODV, DSDV

Steps involved in blackhole attack

Step1: Initialize network parameters to create a network.

Step2: Initialize blackhole nodes.

Step3: Select source node and start sending the packets from source to destination using AODV protocol.

Step4: During the data transmission blackhole node absorbs all the valuable data packets.

Step5: That valuable packets are dropped by the blackhole node. The blackhole node restricts the transfer of complete information from source to the destination.

RESULTS

Here we simulate the same tcl script without blackhole attack using AODV protocol. AODV protocol with a blackhole attack, DSDV without blackhole attack and DSDV with blackhole attack. We simulated our model for 10 to 100 nodes. Then we compared the Performance Metrics such as the End to End delay, energy consumption and Packet Delivery Ratio (PDR) of the scenarios.

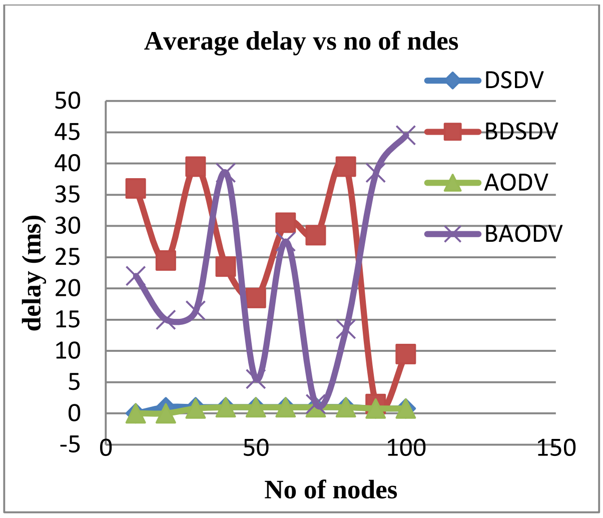

Fig 7: End to end delay vs. number of nodes

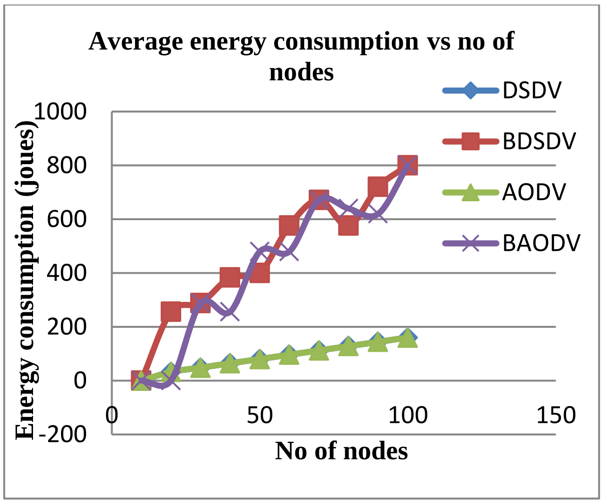

Fig 8: Energy consumption vs. Number of nodes

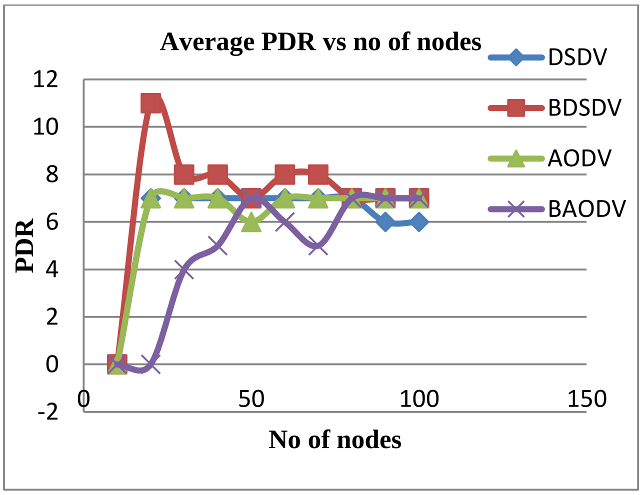

Fig 9: Packet delivery ratio vs. Number of nodes

Fig 7, Fig 8 and Fig 9 shows number of nodes executed for 10 to 100 nodes, time delay in normal AODV and DSDV is almost same but the delay increases in DSDV with blackhole attack than the delay in AODV with blackhole attack. Energy consumption in AODV and DSDV is same but the energy consumption is more in DSDV with blackhole than in AODV with blackhole. PDR is less in DSDV when compare to AODV and the PDR is more in DSDV with blackhole than in AODV with blackhole.

CONCLUSION

In mobile ad-hoc networks blackhole attack affect more in DSDV protocol than in AODV protocol. And a secure sequenced is a mechanism that provides better results as compared to the AODV protocol and other secure AODV protocols. This is a better approach to detect the blackhole nodes form the mobile ad-hoc networks. The key sharing mechanism is to prevent blackhole attack.

In future the scheme can be apply on real test beds and work can be done to combine the scheme with other security schemes to get better results.

REFERENCES

[1] [1] Chintan Patel, Vyomal N. Pandya, Milind Shah “Survey of Reactive Routing Protocols for MANET” IOSR-JECE ,Volume 5, Issue 5 (Mar. - Apr. 2013).

[2] [2]K.P.Manikandan,Dr.R.Satyaprasad, Dr.K.Rajasekhararao “A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks” (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011

[3] [3] Kulbir Kaur Waraich et al “Security against DDoS Attacks in MANETs” International Journal of Computer Science and Mobile Computing, Vol.3 Issue.3, March- 2014, pg. 1024-1030

[4] [4] Aniruddha Bhattacharyya, Arnab Banerjee, Dipayan Bose “Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques” Department of Computer Science & Engineering, Institute Of Engineering & Management, Saltlake

[5] [5] S. Taruna and G.N. Purohit “Scenario Based Performance Analysis of AODV and DSDV in Mobile Adhoc Network” Part II, CCIS 132, pp. 10–19, 2011.

[6] [6] Mohamed A. Abdelshafy,Peter.J.B.King “Resisting Blackhole Attacks on MANETs”, 2016 13th IEEE Annual Consumer Communications &Networking Conference (CCNC)

[7] [7] Marepalli Radha, M. Nagabhushana Rao “Gray Hole Attack Detection Prevention and Elimination using Sdpegh in Manet”,Volume-8 Issue-3,February 2019 .

[8] [8] Kuldeep Singh,Amanat Bopari, Vrinda Handa, Sudesh Rani “Performance Analysis of Security Attacks and Improvements of Routing Protocols in MANET ”, ISBN: 2015 IEEE .

[9] [9] Mohamedh,A,Abdulshafy,Peter J.B.King “Analysis of Security Attacks on AODV Routing ”, International Journal of Computer Applications 2013 IEEE .