East African Scholars Journal of Engineering and Computer Sciences
Abbreviated Key Title: East African Scholars J Eng Comput Sci
ISSN: 2617-4480 (Print) & ISSN: 2663-0346 (Online)
Published By East African Scholars Publisher, Kenya

OPEN ACCESS

Volume-3 | Issue-10 | Dec-2020 | DOI: 10.36349/easjecs.2020.v03i10.003

Review Article

Analysis of AODV, OLSR and ZRP Routing Protocols in MANET under Cooperative Black Hole Attack

Dr. Shankar Ramamoorthy[1*], Er. Preeti Sharma[1], Er. Gagandeep Singh[2], Er. Amanpreet Kaur[2]

[1]Professor, Department of CSE, BGIET Sangrur, Pubjab, India
[2]Assistant Professors, Department of CSE, BGIET Sangrur, Pubjab, India

Article History
Received: 20.10.2020
Accepted: 23.12.2020
Published: 30.12.2020

Journal homepage:
https://www.easpublisher.com

Quick Response Code

Abstract: An ad hoc network (MANET) is a set of different types of mobile nodes these nodes are connected with each other through wireless link. MANET can be developed at any time, at any place with low cost. In MANET protocols are used to connect nodes which are not in direct range of each other. These protocols are mainly of three types i.e reactive (on demand), proactive (table driven) and hybrid routing protocols. This research effort is focused on first the comparative investigation of routing protocols under the cooperative black hole attack to create scenario and simulate and investigate the performance in terms of packet delivery ratio , average end to end delay and throughput.

Keywords: MANET, AODV, OLSR, ZRP, Black hole.

1. INTRODUCTION

A mobile Ad hoc Network (MANET) as its name implies, is a collection of mobile nodes that can communicate with each other without the use of predefined infrastructure or centralized administration. Mobile ad-hoc network have the attributes such as wireless connection, continuously changing topology, distributed operation and ease of deployment. Mobile ad hoc networks (MANETs) face different levels of challenges due to its varying mobile characteristics. The major goal of these networks is to bring the idea of mobility into real-life networks. These networks are known for their infrastructure less characteristics. The nodes are free to move anywhere and hence the communications links may be broken at any moment.

2. ROUTING PROTOCOLS

In MANET routing protocols are used for communicate. They are classified into different categories according to the methods used during the route discovery and route maintenance procedures.

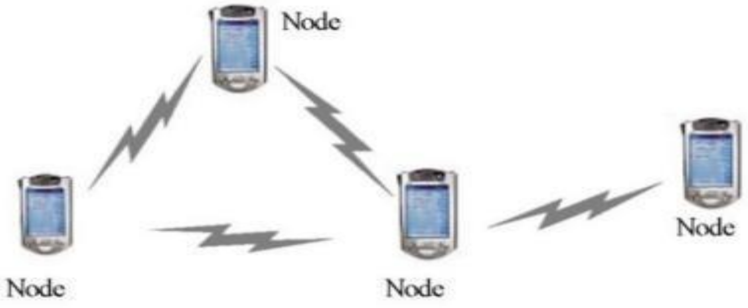

Figure I: Mobile Ad hoc network (MANET)

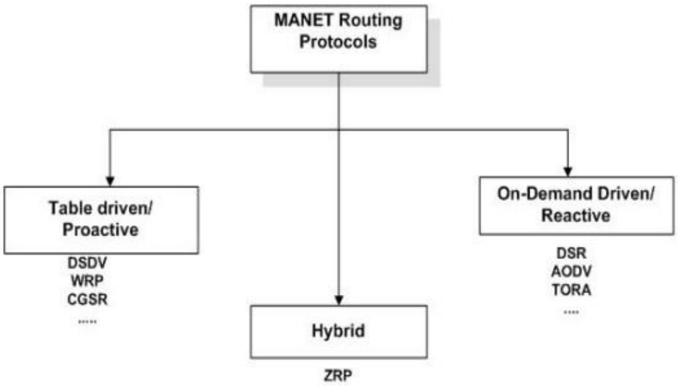

Figure II: Routing Protocols in MANET 2.1 AODV (Ad hoc on demand distance vector)

The Ad-hoc On-Demand Distance Vector (AODV) routing protocol [1, 4] is designed for use in ad-hoc mobile networks. AODV is a reactive protocol: the routes are created only when they are needed. It uses traditional routing tables, one entry per destination, and sequence numbers to determine whether routing information is up-to date and to prevent routing loops. An important feature of AODV is the maintenance of time based states in each node: a routing entry not recently used is expired. In case of a route is broken the neighbours can be notified. Route discovery is based on query and reply cycles, and route information is stored in all intermediate nodes along the route in the form of route table entries. The following control packets are used: routing request message (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used for detecting and monitoring links to neighbors.

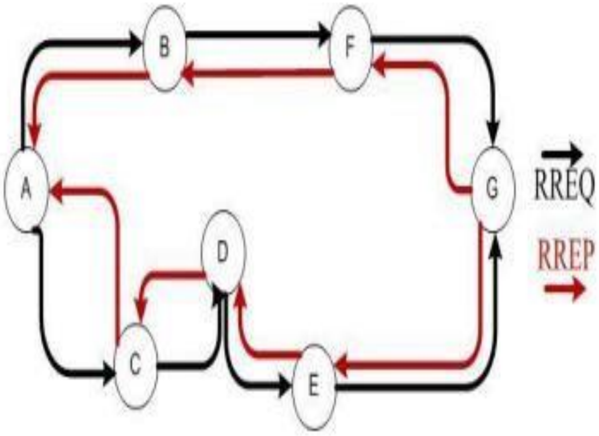

Figure III (a): AODV Route Discovery

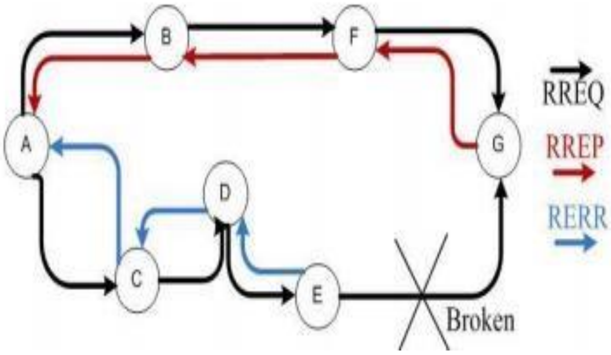

Figure III (b): Route Error Message in AODV

2.2 OLSR (Optimized Link State Routing)

Optimized Link State Routing Protocol, OLSR [4] is developed for mobile ad hoc networks. It is well suited to large and dense mobile networks. It operates as a table-driven, proactive protocol, that is, it exchanges topology information with other nodes of the network regularly. Each node selects a set of its neighbour nodes as “multipoint relays” (MPR) [2], [6]. MPRs, are responsible for forwarding, control traffic, declaring link state information in the network, provide an efficient mechanism for flooding control traffic by reducing the number of transmissions required.

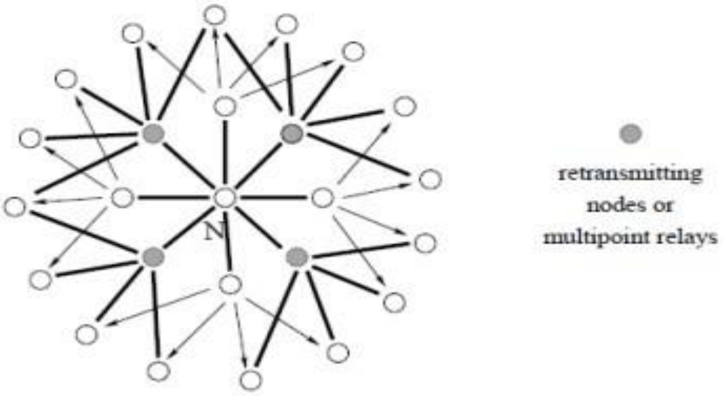

Figure IV: Topology graph of network

2.3 ZRP– Zone Routing Protocol

ZRP (Zone outing Protocol) is a wireless Ad hoc routing protocol uses both proactive routing and on-demand routing policies [4]. Proactive routing uses needless bandwidth to maintain routing information, while reactive routing involves route acquisition latency. Reactive routing also inefficiently floods the entire network during route establishment phase. The aimof Zone Routing Protocol (ZRP) is to trace the problems by joining the best properties of both approaches. ZRP can be called as a hybrid reactive/proactive routing protocol [5].

2.3.1 Architecture

The architecture of Zone Routing Protocol is basically based on the concept of zones, in which a large network is partitioned into number of zones and a routing zone is defined for each node separately, and the zones of neighbouring nodes overlap. The routing zone has a radius r denoted by hops. The zone thus includes the nodes, whose distance from the node is at most r hops. Figure1 illustrates that, the routing zone of S consists of the nodes A–I, but not K. In the illustrations, the radius is pointed as a circle around the node. It should however, be noted that the zone is not a physical distance; rather it is defined in hops.

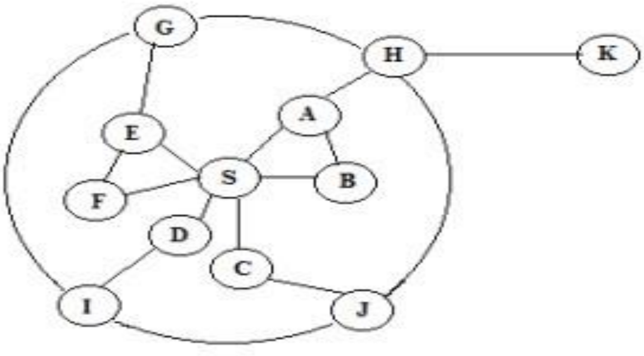

Figure V: Example routing zone with r=2

The nodes of a zone are partitioned into horizon nodes and interior nodes. Horizon nodes are those nodes whose minimum distance from the centre node is exactly equal to the zone radius r. The nodes whose, minimal distance is comparatively less than radius rare interior nodes. The nodes having distance equal to zone radius rare horizon nodes and nodes with distance more than radius rare exterior nodes. In Figure 1, the nodes A, B, C, D, E and F are interior nodes, the nodes G, H, I and J are horizon nodes and node K lies outside the routing zone. The node G can be reached in two ways, one with hop count 2 and another with hop count 3. The node is said to be within the zone, because the shortest path is less than or equal to the zone radius [6].

3. BLACK HOLE ATTACK

Black holes refer to places in the network where incoming traffic is dropped without informing the source that the data did not reach its intended recipient. In Black hole Attack a node uses the protocol and advertises itself as having the shortest path to the destination node where the packet is destined to. Black hole attack can occur when the malicious node present in the network is intended to attack directly the data traffic and intentionally drops, delay or alter the data traffic passing through it [7]. In black hole attack, black hole node acts like black hole in the universe, it consumes all the traffic towards itself and doesn't forward to other nodes. There are two types of black hole attack.

3.1 Single Black Hole Node

In the Black hole attack with single malicious node, only one node will act as malicious node in a zone. Other nodes of the zone will be authentic.

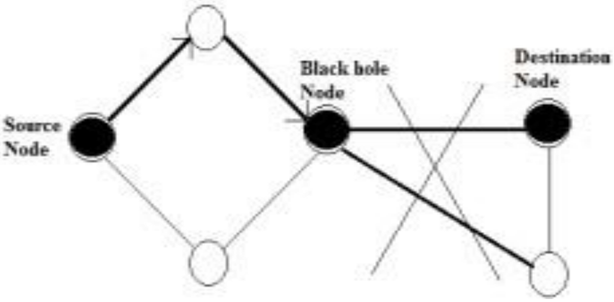

Figure VI: Single malicious node

3.2 Collaborative Black Hole Attack

In Collaborative Black Hole Attack multiple nodes in a group act as malicious node. It is also known as Black Hole Attack with multiple malicious nodes.

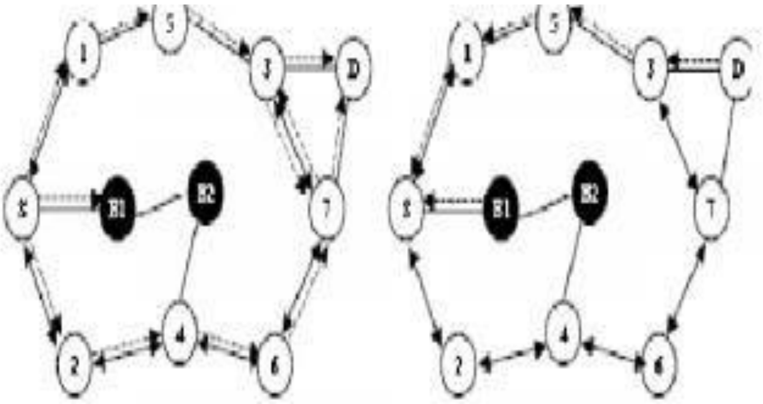

Figure VII: Multiple malicious nodes

4. RELATED WORKS

1. Mistry *et al.*, (2010) Proposed modified AODV protocol and justified the solution with appropriate implementation and simulation using NS-2.33
2. Shivahare *et al.*, (2012) Compared AODV, DSR and DSDV under black hole attack for parameters such as Route Discovery, Network overhead, periodic broadcast and node overhead.
3. Gupta *et al.*, (2013) Proposed an algorithm Secure Detection Technique (SDT) for ZRP protocol which can be used to prevent black hole attack in MANETs.
4. Satveer *et al.*, (2013) Compared FSR, DYMO and LANMAR to evaluate their performance under black hole attack over various parameters.
5. Singh *et al.*, (2014) Stimulated and analysed the performance of AODV, DSR and TORA for E-Mail application under black hole attack.
6. Arora *et al.*, (2014) studied and analysed the performance of MANET Routing protocol like DSDV, DSR, AODV, OLSR and ZRP with and without black hole attack.

6. NS 2 SIMULATION

NS2 Simulation Ns2 is most widely used simulator by researchers; it is event driven object oriented simulator, developed in C++ as back end and OTcl as front end. If we want to deploy a network then both TCL (Tool Command Language) as scripting language with C++ to be used.

Simulation Parameters

For simulation, we use NS2 network simulator. Mobility scenario is generated by random way point modal by taking 50 nodes in simulation area of 1500*1500 m. WE use the following parameters.

Parameters	**Value**
Simulator	NS 2
Routing protocols	AODV , OLSR and ZRP
MAC layer	802.11
Packet size	512 bytes
Terrain size	1500*1500
Nodes	50
Mobility Modal	Random waypoint modal
Data traffic rate	CBR
No. of sources	5,10,15,20,25,30
Simulation duration	30 sec
CBR Traffic Rate	8 packet / sec
Maximum speed	0-20 m/sec (30 sec pause time)

7. CONCLUSION

In future the study will be performed on the decided values of parameters, mentioned in this paper and the effect of these parameters on the various performance matrices i.e packet delivery ratio, average end to end delay and throughput will be noticed.

REFERENCES

1. Prabhu & Subramanium. (2012). “Performance comparison of routing protocols in MANET. *International journal of Advanced research in computer science and software engineering*, 2(9), 388 -392.
2. Arunima, P., & Ashok, V. (2012). A Review evaluation of AODV protocol in MANET with and without black hole attack. *International journal of emerging technology and advanced engineering*, 2(11), 673-677.
3. Muzamil, B., & Raghu, V. M. (2013). Improved performance of DSDV, AODV and ZRP under black hole attack in MANETS. *IJECT*, 4(4).
4. Dadhania, P., & Patel, S. (2013). Performance evaluation of routing protocol like AODV and DSR under black hole attacks. *Performance Evaluation*, *3*(1), 1487-1491.
5. Verma, M., & Barwar, N. C. (2014). A Comparative Analysis of DSR and AODV Protocols under Blackhole and Grayhole attacks in MANET. *International Journal of Computer Science and Information Technologies*, *5*(6), 7228-7231.
6. Arora, N., & Barwar, D. N. (2014). Evaluation of AODV, OLSR and ZRP Routing Protocols under Black hole attack. *International journal of Application in Engineering & Management*, *3*(4), 2319.
7. Singh, L., Kaur, N., & Singh, G. (2014). Analysis the Performance of MANET Protocol under Black Hole Attack for E-Mail Application. *International Journal of Computer Applications*, *103*(12).