Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 85 (2016) 325 – 330

Procedia Computer Science

International Conference on Computational Modeling and Security (CMS 2016)

Comparative Analysis of Black Hole Attack in Ad Hoc Network Using AODV and OLSR Protocols

[a]Praveen K S, [b]Gururaj H L*, [c]Ramesh B

[a,b]Research Scholar, Department of Computer Science and Engineering, Malnad College of Engineering, Hassan-573202, India,
[c]Professor, Department of Computer Science and Engineering, Malnad College of Engineering, Hassan-573202, India

Abstract

Security is an essential factor in wireless ad-hoc network to have safety in transmitting data packets between two wireless sensor nodes. The nodes posses a unique characteristics and it leads to consequential challenges to security design. Comparing to other wireless networks WSN has more security problem; this may be due to its nature of broadcasting messages, resources and their environment. One of the traditional and main attacks of WSNs is Black Hole Attack**.**

Keywords: Mobile ad hoc network (MANET); BlackHole Attack; AODV; OLSR.

1. Introduction

Ad-hoc network consists of dynamic nodes with router functions. The important sector of ad-hoc network is routing protocols, because network topologies keep on changing according to the movement of active nodes [5].

Black Hole is an active and routing attack method where attacker node promotes itself as a best node path to reach the destination and all other nodes. In this attack, the attacker node waits until neighboring nodes initiate the RREQ packet. When the attacker node gets the request it sends a fake reply packet RREP with a new sequence number.

* Gururaj H L: Tel.:+91 9686418942
*E-mail address:*gururaj1711@gmail.com

Peer-review under responsibility of the Organizing Committee of CMS 2016
doi:10.1016/j.procs.2016.05.240

The source thinks it is the active and best node to reach the destination. So, it ignores the other nodes and sends all its data packets through attacker node. The malicious node accepts all the incoming data packets and drops it. It does not forward it to other nodes. As all the data packets are concentrated at a single node hence is called as 'Black hole' and the region is called as 'Black region' [1] [2] [4]

2. Related Work

We have two types of routing protocols in ad-hoc network, Table-driven type (proactive) Routing protocols and On-demand (reactive) Routing protocols. The two main routing protocols we are focusing here are AODV (Ad-hoc On demand Distance Vector) which comes under the on demand type of routing, and the other one is OLSR (Optimized Link State Routing) which comes under Table-driven type of routing.

2.1 AODV:

AODV is one of the on demand and typical routing protocol. To avoid the link breaks in the routing, this protocol will be used. It has symmetrical path between the nodes. AODV has routing table and sequence number for the nodes. The sequence numbers are assigned by the destination node to obtain the freshness of routing information [1] [2] AODV uses Client-server method that is Request-reply method for finding a valid path between sources to destination. The source node broadcast RREQ (route request), the neighboring node receives a route request and routing table gets updated. Finally the RREQ reaches destination node, after receiving the RREQ destination node creates a RREP (route reply) and unicast a route reply in the optimal path choose by the destination. The communication starts between the nodes when the RREP reaches the source. If the links get fail the respective nodes create a message called RERR (Route Error) [7] [8].

2.2 OLSR:

OLSR is a table driven, proactive link state protocol. As it is a proactive Routes are predefined hence by reduces the delay. Control messages are periodically exchanged. Few messages are sent to neighbor for enabling route discovery and some control messages are flooded, this message contains topology information [9]. Every node in the network discovers its links with neighbor nodes and each node keep on flooding the link state messages. Each node calculates the best next hop for other nodes and MPR (Multi Point Relays) which are subsets if neighboring nodes. The main idea of MPR is reduce the flooding of broadcast messages in the network by minimizing duplicate retransmission messages. So the numbers of transmission messages are reduced [10]. There are four different kinds of messages

1. HELLO (Hello)
2. TC (Topology control)
3. MID (Multiple interface Declaration)
4. HNA (Host or Network Announcement)

OLSR is an optimized routing protocol for Mobile Ad hoc Network because messages are compacted and reduces the number of retransmission to flood these messages [3]. The black hole attack is an active and routing attack method which affects the network security and depletes the performance of the network [1]. The performance of AODV, OLSR, and ZRP Protocols are compared and AODV outperforms compared to OLSR and ZRP for different performance metrics [5].

3. Performance Metrics

NS2 is an event simulator mainly intended to network research. NS is an interpreter of TCL scripts of the users; they work along with C++ codes. It uses Object Oriented Tool Command Language to evaluate user simulated Scripts. TCL and C++ are totally compatible with each other.

3.1 Packet-to-Delivery Ratio (PDR): The ratio of the packets delivered to destination when compared to that of the packets sent from the source. The below equation gives the formula to evaluate PDR:

$$\text{PDR}= \text{Number of packets received}/ \text{Number of packets sent} \quad (1)$$

3.2 Average Throughput: Throughput is the total number of packets sent successfully from sender to receiver in a specified time.

$$\text{Throughput}= \text{Packet Size}*\text{Received packets}*8/100 \quad (2)$$