International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X;pISSN:2321-2241 Volume: 3; Issue: 6; December -2014

Blackhole Attack Generation, Analysis and Detection in a Multihop Wireless Network

Aman Kapoor [1], Rinchen Sharma [2] , Akriti Mahajan [3], Jatinder Gupta [4]
[1,2,3,4] Graduate, School of Electronics and Communication,
SMVD University, Katra
[1]amankapoor0098@gmail.com, [2] rinchen2210@gmail.com,
[3]akritimahajan.india@gmail.com , [4]gupta.jatin619@gmail.com

***Abstract*— this paper is an outcome of our final year project in which we generated a blackhole attack by making a node as blackhole node and then detecting it. This was done using the network simulator 'QualNet'. Blackhole is one of the security threat in which traffic is redirected and the packets are dropped instead of forwarding them. For secure transmission and communication some security measures needs to be adopted.**

***Keywords* —blackhole, network attack, QualNet, blackhole generation, blackhole detection.**

I. INTRODUCTION

Wireless networks are gaining popularity day by day because of its mobility, simplicity, affordable and ease of installation. Wireless networks are susceptible and exposed to attack because of its borderless nature. Moreover, hacking tools are largely available in the market and online[2].These tool which are usually meant to be used by penetration testers and for educational purposes are being misused and abused by underground or even novice hackers. An attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset[3]. Thus, such attacks on the networks must be detected in time for secure communication.

Blackhole attack is a type of denial-of-service attack in which a node which is supposed to relay packets instead discards them[4]. The packet drop attack or the blackhole attack can be frequently deployed to attack wireless ad hoc networks. Because wireless networks have a much different architecture than that of a typical wired network, a host can broadcast that it has the shortest path towards a destination. By doing this, all traffic will be directed to the host that has been compromised, and the host is able to drop packets at will. In our project we have created a wireless network of n number of nodes using QualNet, generated blackhole attack in it, analyzed it for AODV and DSR protocols and in the end detected the blackhole attack and the blackhole node.

We find that in earlier researches, blackhole attack was generated but no detection is there by changing the backend code of the simulator QualNet. Also analysis was done with AODV and DSR protocols individually but was not compared much. We analyzed the effects of black hole attack in the light of Network load, throughput and end-to-end delay.

II. EXPLANATION

Ad-Hoc On Demand Distance Vector Protocol (AODV) and Dynamic Source Routing Protocol (DSR) are reactive protocols. The fact they are known as reactive protocols is, they do not initiate route discovery by themselves, until they are requested, when a source node request to find a route. These protocols setup routes when demanded.

For generating the blackhole attack, one or more than one node among the total nodes in the network has to the blackhole node so that when the source tries to sent packets, if the blackhole node is in the neighborhood of the source node it replies to the route request message conveying that it has the shortest path to the destination node and after receiving the packets, drops them. To create a node blackhole backend code of the simulator QualNet was altered for AODV and DSR files separately.

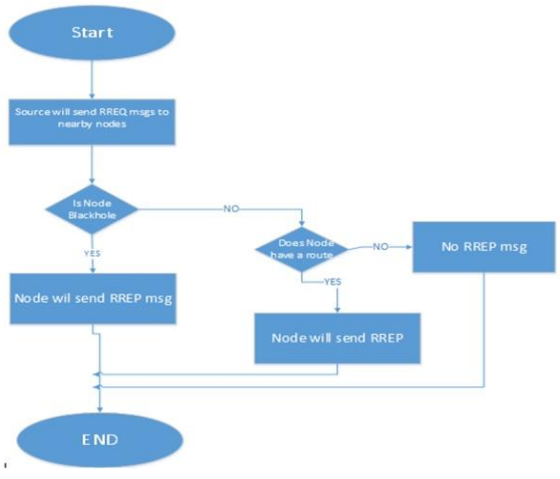


Figure 1. Basic flow chart for generation of attack

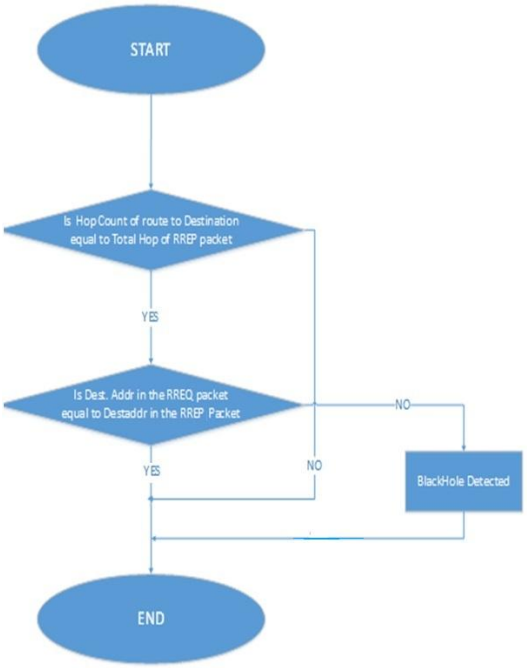


Figure 2. Basic flow chart for detection of attack

III. PERFORMANCE ANALYSIS

A. Simulation Tool

The tool used for the simulation study is QualNet 5.1. QualNet is a network and application based software used for network management and analysis.[1] QualNet is defined as state-of-the-art simulator for large, heterogeneous networks and the distributed applications that execute on those networks.

The following QualNet features provide a unique capability for accurate, efficient simulation of large-scale, heterogeneous networks:

• Robust set of wired and wireless network protocol and device models, useful for simulating diverse types of networks.

• Optimized for speed and scalability on one processor, QualNet executes equivalent scenarios 5-10x times faster than commercial alternatives.

• Designed from the ground-up as a parallel simulator, QualNet executes your simulation multiples faster as you add processors.

• A robust graphical user interface covers all aspects of the simulation, from scenario creation and topology setup, integration of custom protocols, through real-time execution of network models from within the GUI, animation, to post-simulation statistical analysis

B. Network Creation and Analysis

The Scenario taken into account for the below results is of 20 nodes with 5 nodes as source and 5 as destination and others act as intermediate nodes.

Source nodes: 2, 5, 12, 16, and 19.

Destination nodes: 4, 10, 13, 15 and 18

Blackhole node: 17.

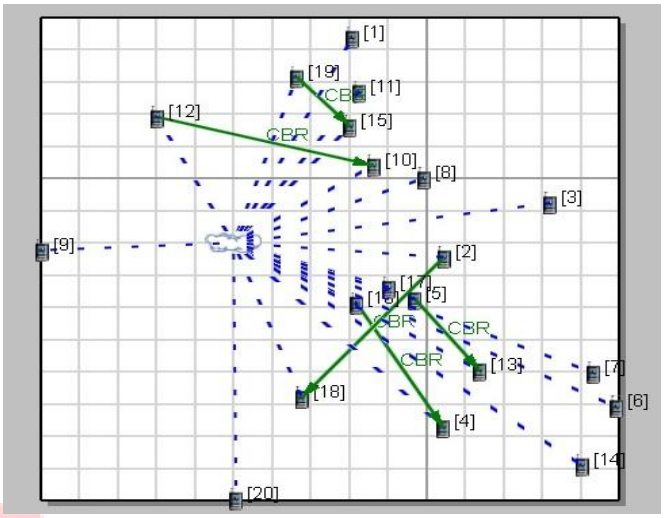


Figure 3. Scenario created in QualNet

Devices like cell phones are nodes with their number as superscripts. The symbol cloud is to make the network connection wirelessly. Dashed blue lines represent wireless connection between nodes. Green arrows represent the constant bit rate between source and destination nodes.

C. Performance metrics

The performance metrics chosen are:-

1. The packet end-to-end delay is the average time in order to traverse the packet inside the network. This includes the time from generating the packet from sender up till the reception of the packet by receiver or destination and expressed in seconds. This includes the overall delay of networks including buffer queues, transmission time and induced delay due to routing activities. Different application needs different packet delay level. Voice and video transmission require lesser delay and show little tolerance to the delay level.
2. The second parameter is throughput; it is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet. It is represented in bits per second or packets per seconds. In MANETs throughput is affected by various changes in topology, limited bandwidth and limited power. Unreliable communication is also one of the factors which adversely affect the throughput parameter.
3. The third parameter is average jitter. In the area of packet communications Jitter is referred to as Packet Delay Variation (PDV). It is the difference in the one way end-to-end delay values for packets of a flow.

Instantaneous PDV is the difference in packet transfer delays for successive packets – this is what is usually called Jitter. Often Jitter is measured in terms of a time deviation from the nominal packet inter- arrival times for successive packets.

D. Simulation Setup

SIMULATION PARAMETERS

Examined protocol	AODV
Simulation time (s)	30 seconds
Simulation area (m)	1500*1500 meters
Number of nodes	varied
Traffic type	TCP/IP
Performance parameters	Packet End to end delay, average jitter throughput, total number of packets received
Pause time (s)	100 seconds
Mobility (m/s)	10 m/s
Packet size (bytes)	512 bytes
Data rate	2 kbps
Mobility model	Random waypoint

Figure 4. Simulation Parameters

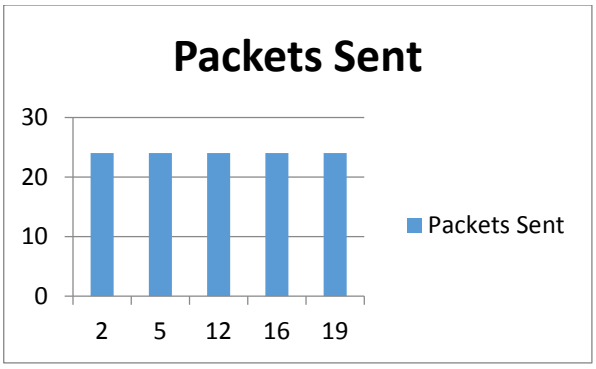
IV. RESULTS

The simulated results are provided below as bar graphs which give the variation in network nodes while under blackhole attack and without blackhole attack for AODV protocol and compared result figures for AODV and DSR protocols.

A. RESULTS FOR AODV PROTOCOL

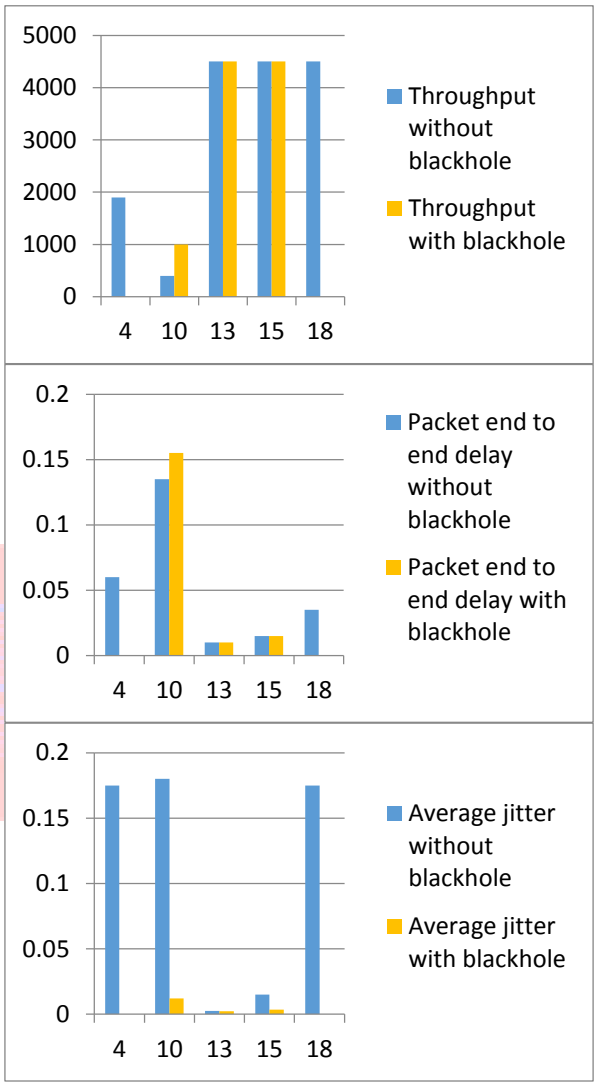
X-Axis represents node number
Y-Axis represents metric value

1. ANALYSIS OVER THE CLIENT END



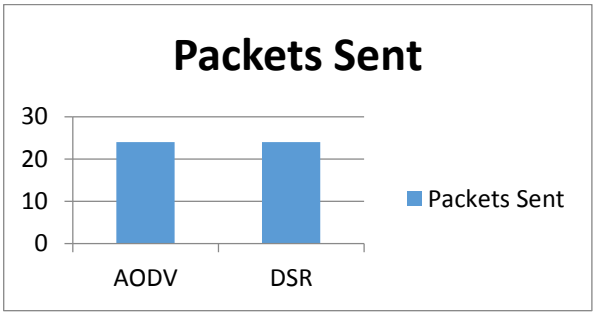
.

2. ANALYSIS OVER THE SERVER END

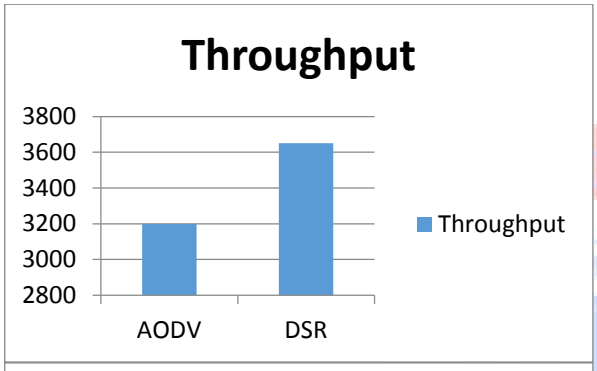


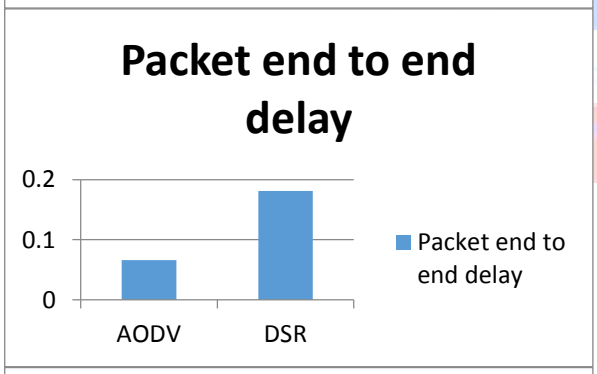
B. COMPARED RESULTS FOR AODV AND DSR PROTOCOLS WITH BLACKHOLE

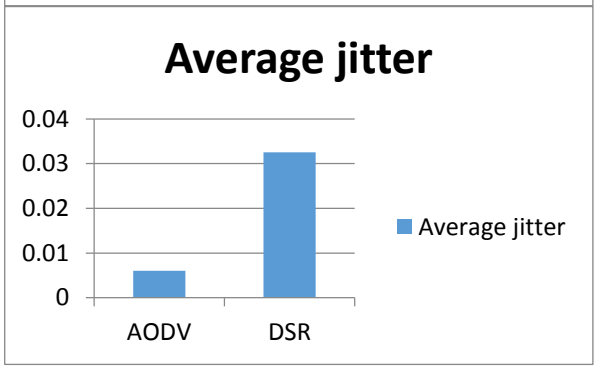
1. ANALYSIS OVER THE CLIENT END



2 ANALYSIS OVER THE SERVER END







V. Conclusion

- By making node no 17 as the blackhole node. No packet is received by the node 4 and 18.
- Node no 10 and 15 are not affected by the blackhole as node no 17 is not in the neighborhood of the source nodes 12 and 19.
- Node no 17 is in the neighborhood of the source node 5 but is not affected by it as node no 13 is in direct neighbor hood of 5.
- A network with DSR protocol is less affected by blackhole attack than a network with AODV protocol.

VI. Future Improvements

For future improvement, we will compare the results for a reactive, proactive and hybrid routing protocols. We will also provide an algorithm to prevent the blackhole attack in a wireless network.

Acknowledgment

The satisfaction that accompanies the successful completion of any tasks would be incomplete without the mention of the people who made it possible and whose encouragement and guidance was a source of inspiration during the course of the project.

We owe our sincere gratitude to our project guide Mr. Ashish Suri, who helped us to carry out this project successfully.

References

[1] https://www.ee.iitb.ac.in/~prakshep/IBMA_lit/manual/manual244.html, last visited 29, May, 2014

[2] Noor Mardiana Mohamad and Hassan Wan Haslina, "Wireless Networks: Developments, Threats and Countermeasures".

[3] Stallings William, "Computer Security : Principles and Practice", Chapter 2.

[4] Ullah Irshad, Rehman Shoaib Ur, "Analysis of Black Hole attack On MANETs Using different MANET Routing Protocols", June 2010.