International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Performance Evaluation of Routing Protocols (AODV, DSDV and DSR) with Black Hole Attack

Rozy Rana[1], Kanwal Preet Singh[2]

[1]Department of Computer Engineering, Master of Engineering, UCOE, Punjabi University Patiala, India

[2]Department of Computer Engineering, Assistant Professor, UCOE, Punjabi University Patiala, India

Abstract: ***The main goal of this Research paper is to see the simulation and performance factors of routing protocols (AODV, DSDV AND DSR) after attack in NS-2. Routing Protocols specifies how communication between two routers takes place. By this we can specify the choice of the route. We will analyze literature sources related to wireless networks simulators. We will also analyze the Network simulator ns-2 and will give its detailed Description. Therefore we can analyze the performance factors packet delay, packet loss and throughput in nodes after the Black Hole Attack. We will compare these three routing protocols by evaluating on the basis of their performance.***

Keywords: Performance**,** NS-2, AODV, DSDV, DSR, Throughput, Delay

1. Introduction

Wireless Networks are the networks that allow user to access the information electronically. Therefore information can be exchanged electronically with the help of radio waves. Hence services and data can be accessed wirelessly without any knowledge of location. It allows wireless connections for connecting network nodes. It takes place at physical level of OSI model. It avoids the costly process of introducing wire into campuses and building. DSDV, AODV and DSR are the routing protocols used in wireless network. DSDV is destination sequenced distance vector. It is based on Bellman Ford Routing Algorithm. AODV is ad-hoc on demand Distance vector and it maintains the timer based states in each node. The wireless network can be classified into two types: infrastructure and infrastructure less network [2].

1.1 Infrastructure Networks

It consists of network having fixed wired gateways. Here the host which is mobile and it communicates with base station (access point) but within its radius. When it goes out of its range it starts communicating with other access point. Hence it is known as Handoff. Here the base stations are fixed [3]. Infrastructure mode networks offer the advantage of scale, centralized security management and improved reach. The disadvantage of infrastructure wireless networks is simply the additional cost to purchase AP hardware.

1.2 Infrastructure less Networks

Here all the nodes are mobile and they can move in any manner. The range of the host is limited so if it wants to connect the node outside of its range it can communicate the node that will be nearby and send packet to destination. Here node will act as router [3].

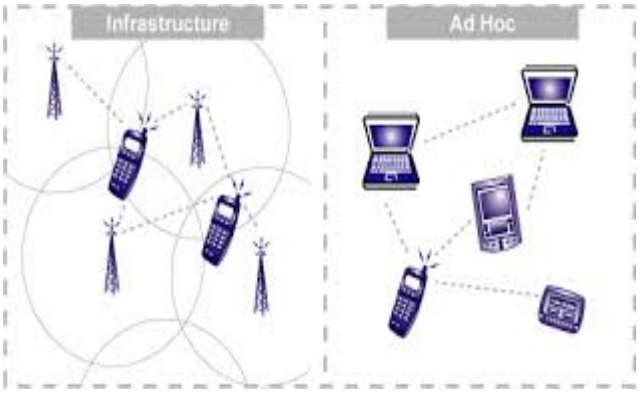

Figure 1: Infrastructure and ad-hoc Network [7]

2. Wireless Routing Protocols

A routing protocol is needed whenever a packet needs to be transmitted to a destination via number of nodes and numerous routing protocols have been proposed for such kind of ad hoc networks. These protocols find a route for packet delivery and deliver the packet to the correct destination. The studies on various aspects of routing protocols have been an active area of research for many years [4].

Ad-hoc networks are divided into Table driven and on-demand routing protocols.

Table driven protocols: In table driven protocols are proactive protocols and it maintains routing table. Proactive protocols are DSDV [5]. In Table Driven routing protocols each and every node is having one or more tables containing routing information to every other node in the network [4].

On-demand routing protocols: on demand routing protocols doesn't maintain any routing table and are active protocols. In these protocols, routes are created as and when required. It invokes the route discovery procedure, when a transmission occurs from source to destination. The route remains valid till destination is achieved or until the route is no longer needed [4]. On demand routing protocols are

AODV [5] and DSR [5]. Three Routing Protocols are DSDV [5], AODV [5] and DSR [5].

2.1 DSDV

DSDV is Destination sequenced distance vector. It is a based on Bellman Ford Shortest Path Algorithm [3] and is a table driven routing scheme. Hence an improvement made to bellman ford algorithm by using sequence number so that it cannot form loops. Here each node maintains routing table that will list all available destinations, next hop to reach destination and metric. Destination node generates the sequence number to distinguish new nodes from stale ones.

2.2 AODV

It is Ad-hoc on demand vector. We calculate the route on its demand. Aodv maintains routing table and it maintain one entry per destination. Here routes are discovered when they are needed and maintained for the time they are required and routes are not maintained from each node to every other node in the network [2].

2.3 DSR

It is a pure on demand routing protocol. It reduces bandwidth overhead. It allows the network to be self organized and self configured. It uses source routing because source is responsible for providing the whole path. Here intermediate nodes are not responsible for providing any information related to destination. What path source will choose depend entirely on source. It is working on two parts: 1. Route Discovery 2. Route Maintenance.

3. NS-2

NS-2 is Network simulator and it is a discrete event driven network simulation tool. It is used to study the changing nature of communication networks. It is an open source and freeware. We can implement in C++ and OTCL programming languages. It supports different protocols, traffic and routing types. It provides users with a way of specifying protocols and simulating the behaviors. The result of simulation will be a trace file which will contain all events. It is developed by UCB.NS-3 is newest version of network simulator and it has been written in C++ and python. Also NS-3 doesn't support NS-2 Functionality. Some models in ns-3 we still take from ns-2.Because of Missing functionality and totally different API, we still prefer NS-2. It is portable and it can work on windows and UNIX.

3.1 NS-2 Programming Languages

To have a powerful and fast simulator we make use of programming languages in NS-2. Programming language like object oriented C++ we use it to form core of ns-2 which is used to handle header, algorithms and packets. For network scenario creation we uses object Tcl and it allows fast modifications. Languages like O Tcl and C++. Interact with each other through Tcl/C++.

1. OTcl is the language that is having goal to explore number of scenarios. It compromise between speed and abstraction level that has been offered to user. Iteration is also important feature in OTcl.
2. Whereas C++ object oriented we can use it for algorithm implementation and byte manipulation. With the help of this language we can achieve fast execution.

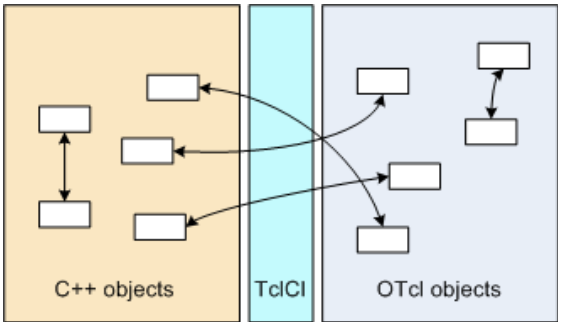

Figure 2: Tclcl [8]

There are several characteristics of Tcl/OTcl languages and that are

1. Faster development.
2. Graphic interface
3. Compatibility
4. Flexibility for integration
5. Scripting language.

For OPNET, we need a license to use it and whereas NS-2 is open source and freeware. Hence open source option makes it attractive option than others. Complex requirements can be easily tested in NS-2. Modularity approach also makes it better. Whereas in NS-3 there is limited no. of Models and contributed codes in NS-3 as compare NS-2.

3.2 Structure of NS2

a) NS-2 is an object oriented discrete event simulator.
b) Back end is C++ event scheduler.
c) **Source code:** Most procedures are written in C++ code in NS-2.
d) **Scripting language:** It uses TCL as its scripting language and when it add object it become OTcl.
e) It imports C++ code to TCL [2].
f) It implements TCP and UDP protocols.

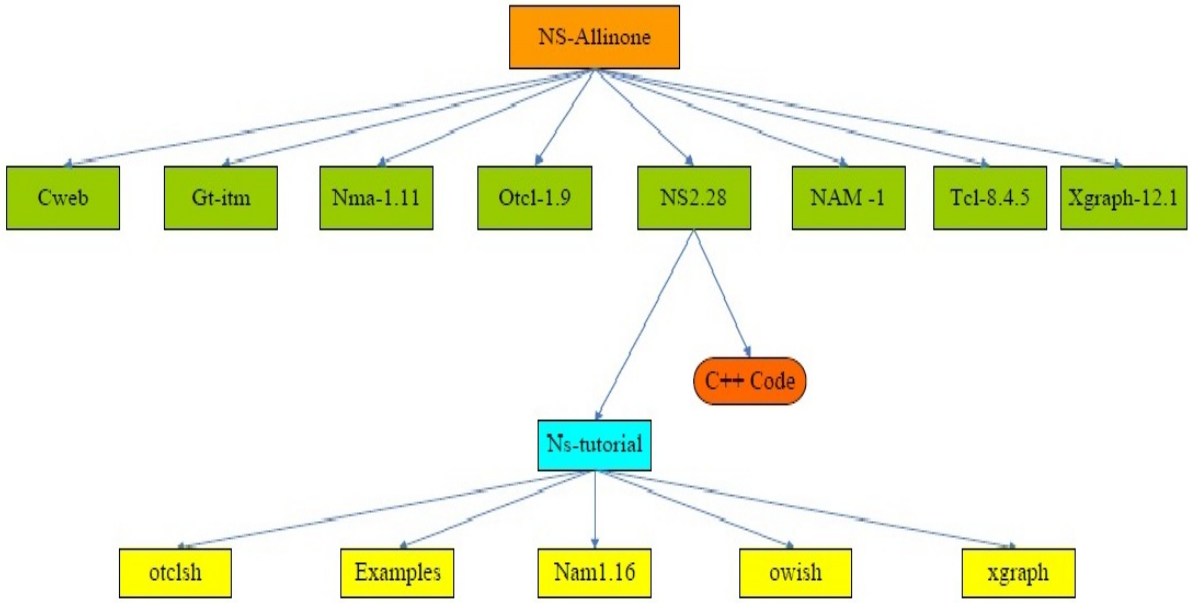

Figure 3: NS-2 Structure [8]

4. Black Hole Attack

In order to advertise itself for the packet it wants to intercept or having shortest path to Destination, malicious node uses its routing protocol in case of black hole attack.

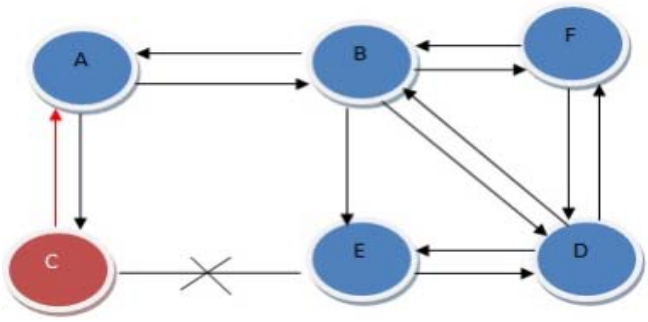

Figure 4: Black Hole Attack [11]

The sender node sends or advertises availability of fresh routes instead of checking its routing table. Malicious node will reply the route request and thus intercept the data packet and retain it.

5. Performance Evaluation Factors

Scalability of routing protocols provides increase in traffic rate and network rate without degrading the network performance. This research paper helps us to analyze three routing protocols. So AODV, DSDV and DSR are the three protocols that we are going to analyze.

5.1 Throughput

It determines the throughput for each node and thus ns-2 helps in calculating byte received.

5.2 Packet Loss

It helps in calculating packet that is transmitted. It also calculates packets that are not received.

5.3 Packet delay

It calculates the last time packet receives and no of all packets received.

6. Black Hole Attack NAM File

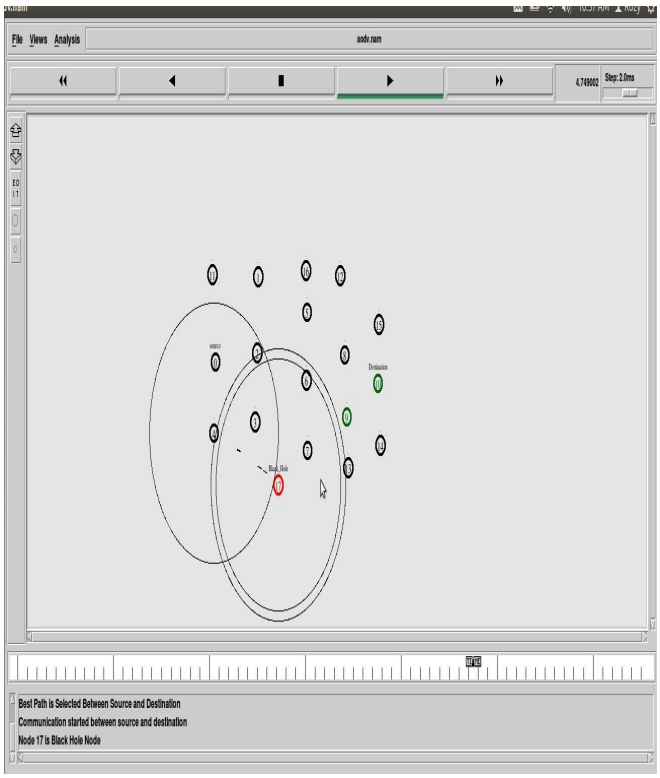

Figure 5: Black Hole attack on Node 17

7. Simulation Result

7.1 Packet Delay: The X-graph for delay is

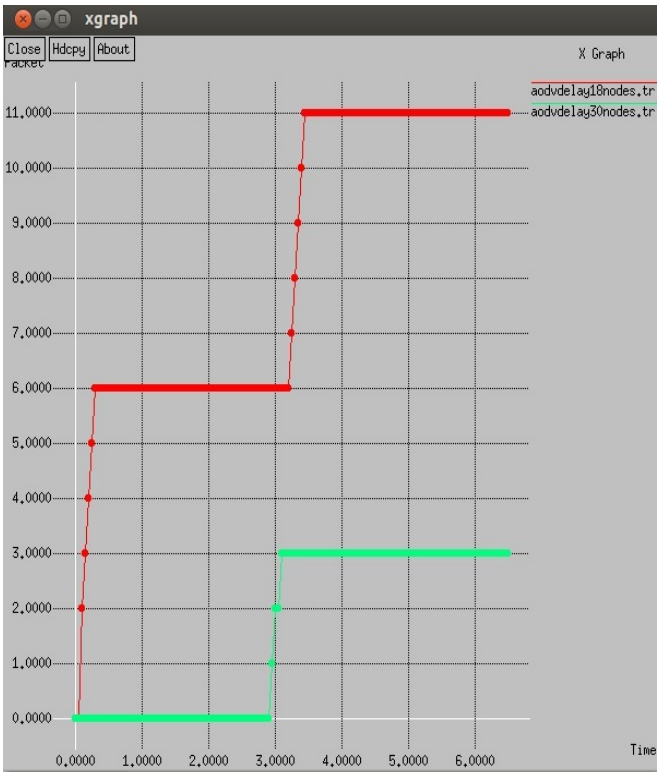

Figure 6: Delay in case of AODV with Black hole Attack

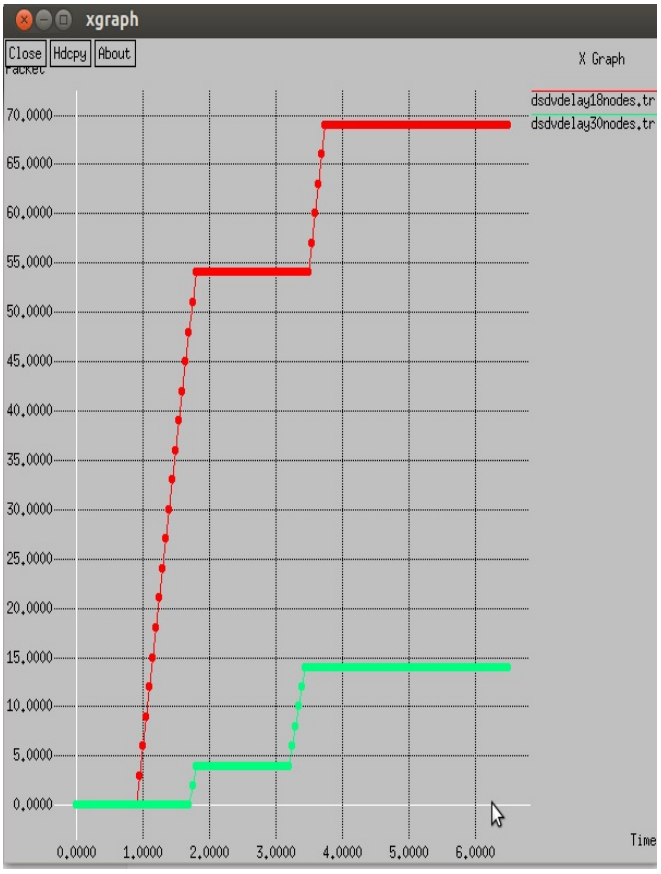

Figure 7: Delay in case of DSDV with Black hole Attack

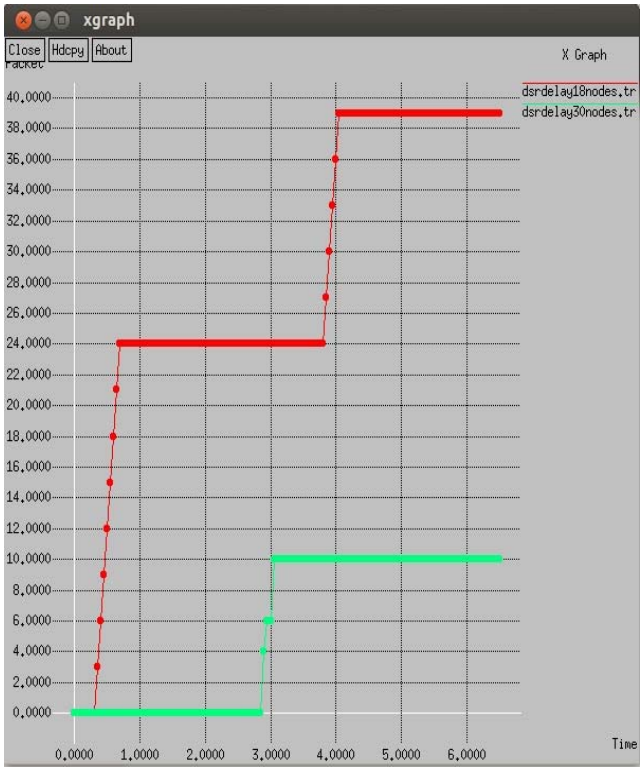

Figure 8: Delay in case of DSR with Black hole Attack

7.2 Throughput: The X-graph for throughput is

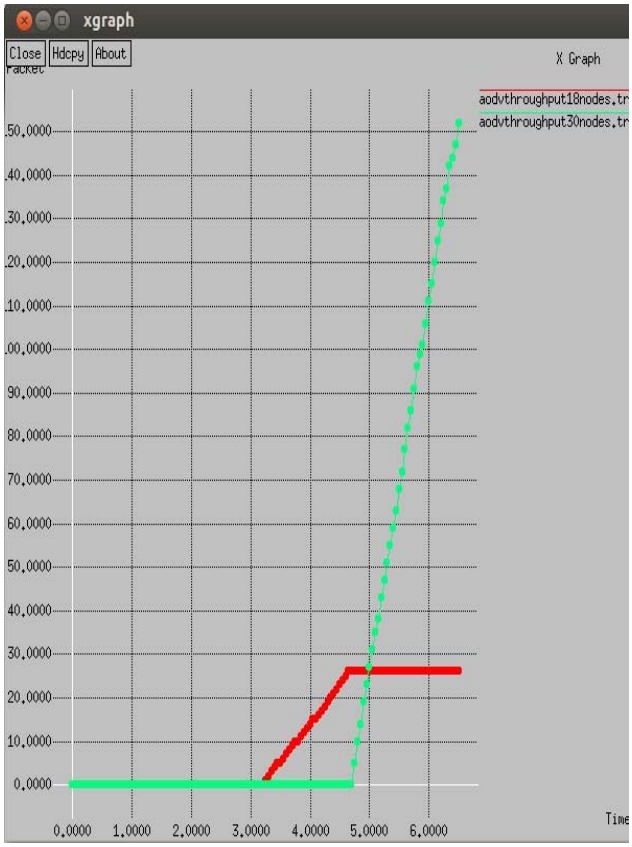

Figure 9: Throughput in case of AODV with Black hole Attack

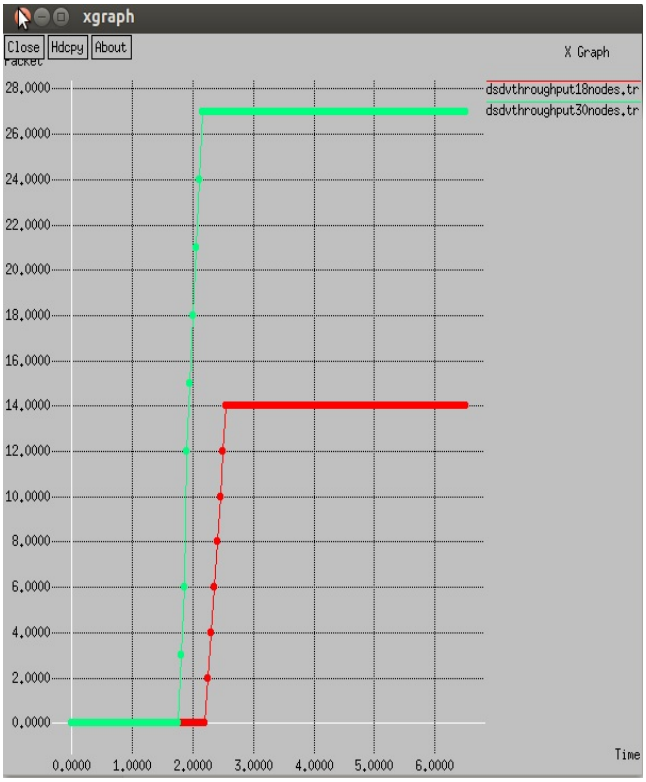

Figure 10: Throughput in case of DSDV with Black hole Attack

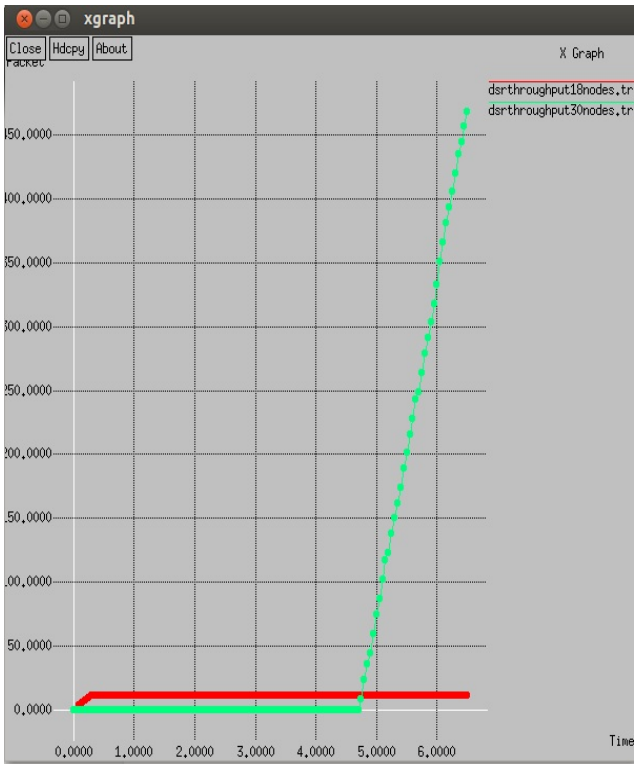

Figure 11: Throughput in case of DSR with Black hole Attack.

7.3 Packet Loss: The X-graph for Packet Loss is

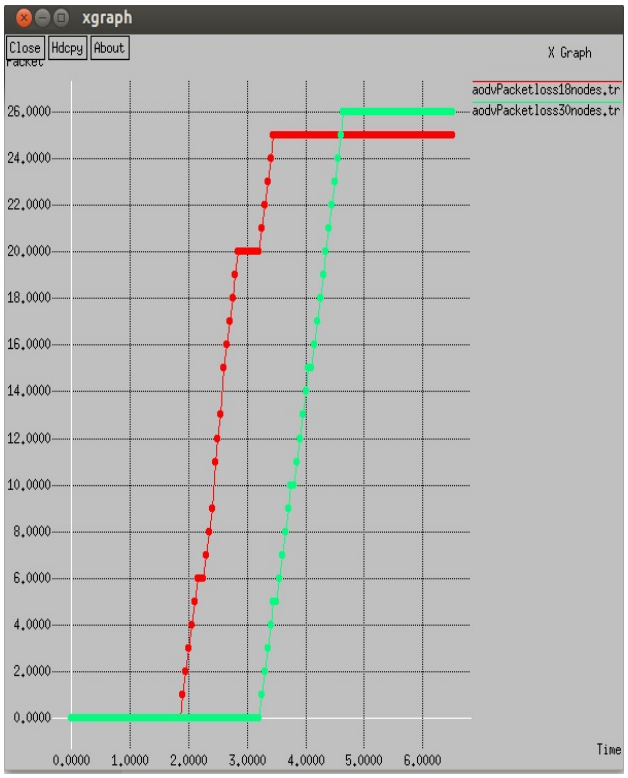

Figure 12: Packet Loss in case of AODV with Black Hole Attack

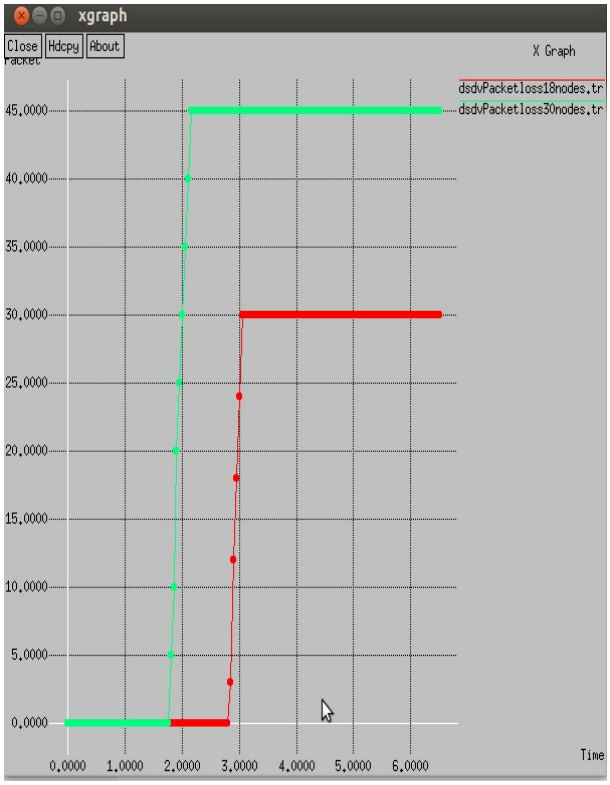

Figure 13: Packet Loss in case of DSDV with Black hole Attack

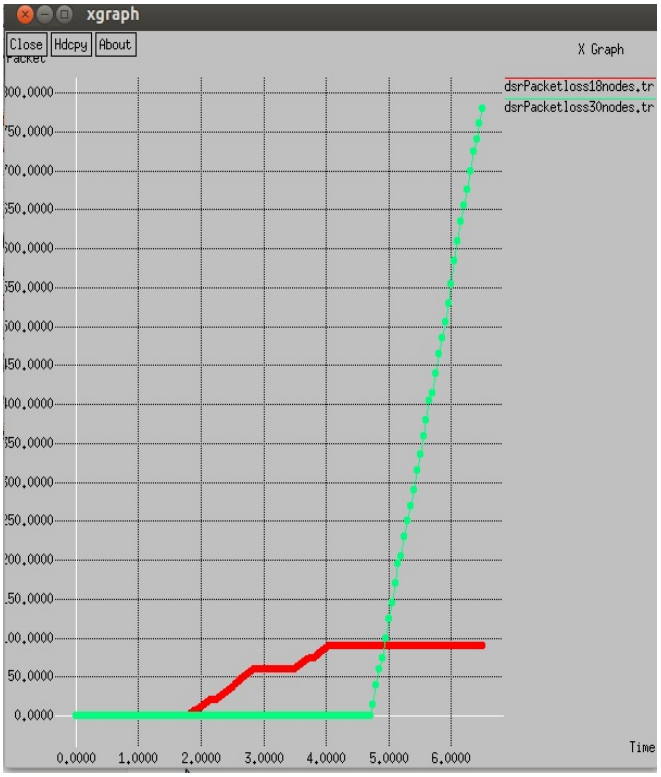

Figure 14: Packet Loss in case of DSR with Black hole Attack

8. Conclusion

Here we evaluated three routing protocols with respect to packet loss, packet delay and throughput with black hole attack. These are used for evaluation of performance factors. Throughput, packet loss and packet delay tells the reliability of protocols. In a network the routing protocol should be reliable and efficient.

The choice of intended protocol depends upon the network used. The following conclusions are drawn on the basis of experimental observations and analysis:

1. DSDV has more delay in case of 18 Nodes. While AODV and DSR has less delay in case of 18 Nodes as compare to DSDV. AODV has low Delay in case of 30 Nodes. DSDV has high delay in case of 30 Nodes as compare to DSR and AODV.
2. DSDV and DSR has low throughput in case of 18 Nodes as compare to AODV. AODV has high throughput in case of 18 Nodes. AODV has low Throughput than DSR in case of 30 Nodes. DSDV has very low throughput than DSR and AODV.
3. DSR has high Packet Loss in case of 18 Nodes. While AODV has low Packet Loss in case of 18 Nodes as compare to DSDV and DSR. DSR has High Packet Loss in case of 30 Nodes. AODV has low Packet Loss than DSDV and DSR.

There are three different scenarios packet delay, loss and throughput. There is a Need to analyze other routing protocols like TORA and GRP under black hole attack. A strategy need to be created to eliminate such type of behavior from black hole attack

9. Scope for Future Work

1. Investigation of other routing protocols like TORA and GRP under Black Hole Attack. We need to analyze other routing Protocol to see if they are Performing Better than each other by comparing them.

2. Investigation of the Prevention Techniques for Black Hole Attack for all Routing Protocols in NS-2 and then Comparison.

References

[1] Abdalla Gheryani, *Design and Simulation of Wireless Network using NS-2*, ICCSIT, April 2012
[2] Shilpa Shukla, *STUDY & ANALYSIS of DSDV, AODV & DSR*, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 5, May 2013, ISSN: 2319-5940
[3] D. Sunil Kumar, *A Simulation Based Study of AODV, DSR, DSDV Routing Protocols in MANET Using NS-2*, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 3, March 2012, ISSN: 2277 128X
[4] Sunil Taneja and Ashwani Kush, "A *Survey of Routing Protocols in Mobile Ad Hoc Networks*", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, pp. 279-285,August 2010.
[5] P. Chenna Reddy, Dr. P. Chandrasekhar Reddy, "Performance Analysis of Adhoc Network Routing Protocols", Academic Open Internet Journal, SSN 1311-4360, Volume 17, 2006
[6] NS-2, the ns Manual (formally known as NS Documentation) available at "http: //www.isi.edu/nsnam/ Ns/doc."
[7] Wireless Ad-hoc Network," http: //en.wikipedia.org/wiki/Wireless_ad_hoc_network ".
[8] Yinfei Pan, Design Routing Protocol Performance Comparison in NS2: AODV comparing to DSR as Example
[9] Yaser khamayseh, A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks, International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 1, April 2011
[10] Mehdi Medadian, Khossro Fardad, "Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol", European Journal of Scientific Research ISSN 1450-216X Vol.69 No.1 (2012), pp.91-101
[11] Sushil Kumar Chamoli, Santosh Kumar, Deepak Singh Rana, "Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks", Int.J.Computer Technology & Applications,Vol 3 (4), 1395-1399
[12] Dr. S. Tamilarasan, "Securing AODV Routing Protocol from Black Hole Attack", International Journal of Computer Science and Telecommunications [Volume 3, Issue 7, July 2012]
[13] Abhilasha Sharma, Rajdeep Singh, Ghanshyam Pandey, "Detection and Prevention from Black Hole attack in AODV protocol for MANET", International Journal of Computer Applications (0975 – 8887)
[14] Govind Sharma, Manish Gupta, "Black Hole Detection in MANET Using AODV Routing Protocol", International Journal of Soft Computing and Engineering (IJSCE)