INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

The Simulation Effect of Packet Drop Ratio and End-2-End Delay in AODV using Black Hole Attack in NS-2

Dipika Jain
Scholar, Department of Computer Science & Engineering, PDM College of Engineering, B'Garh, MDU, Rohtak, Chandigarh, India
Sunita Sangwan
Assistant Professor, Department of Computer Science & Engineering, PDM Group of Institutions, B'Garh, Haryana, India

Abstract:
In today's world scenario where life is so quick and fast, communication network is required everywhere. There was difficulty in setting up a wired communication system, so the wireless communication system came into use. Further, when we talk about the wireless communication system, it is of two major types, the infrastructural and the non-infrastructural wireless communication network.
Here in this paper, we are showing the simulation effect of the black hole attack on the AODV protocol using Packet Drop Ratio and E2E Delay as the parameters.

Keywords: *MANET, Network Simulator, AODV Routing Protocol, E2E Delay, Packet Drop Ratio*

1. Introduction

Mobile Adhoc Network is a network of mobile nodes which may or may not be connected via a wire. The connection may be a wireless connection or a wired connection. In the network the nodes are free to move in the network and communicate amongst them. It is an infrastructureless wireless network. Moreover, any node in the network can anytime enter or exit the formed network.

2. Network Simulator

The discrete event network system is a set of network elements like routers, links, users and applications. In the simulation of a network there are various simulation models, namely NS2, NS3, OPNET and GloMoSim etc. One of the most popular network simulators is NS2. NS2.35 is nowadays popularly used network simulator. This tool converts a .tcl file into .tr and .nam files.
The network simulator can be described as a software or hardware that predicts the behavior of the network without the presence of the actual network.

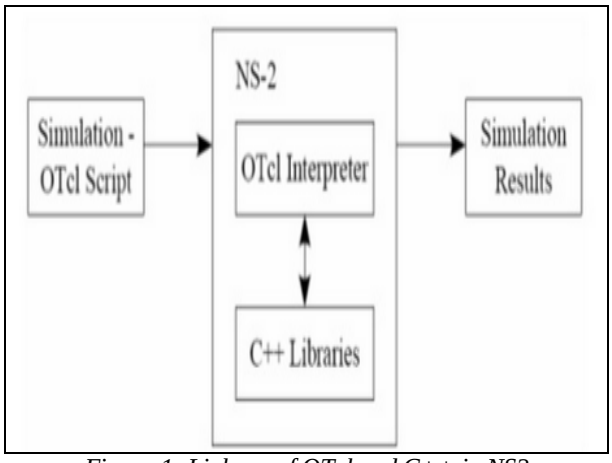

Figure 1: Linkage of OTcl and C++ in NS2

The network was created for 50 nodes with the following values for the simulation parameters.

Routing Protocols	AODV
No. of Nodes	50
Simulation Area	1000 x 1000
Simulation Period	1000ns
Connection Type	CBR
MAC Type	

Table1: Value of simulation Parameters

3. AODV Routing Protocol

The protocols which specify how the routers communicate with each other are termed as routing protocol. There are basically three types of routing protocols, namely the On-demand routing protocol (reactive), the table-driven routing protocol (proactive) and the hybrid routing protocol. AODV is an On-demand or Reactive routing protocol. It is capable for both unicast and multicast routing. This routing protocol builds routes using route request and route reply query cycle.

4. Simulation Parameters

There are several parameters that can be used for the evaluation of the attack. They can be End-to-End Delay, Packet Drop Ratio, Packet Delivery Ratio and Throughput etc. Here the simulation is using two of the parameters: The E2E Delay and the Packet drop ratio.

4.1. Packet Drop Ratio

The total number of packets dropped during the simulation is termed as the packet drop ratio.
It can be also termed as the difference between the total number of packets send and the total number of packets received.
PDR= Total no. of packets send – total no. of packets received.
The results are recorded as in the table below:

Time in sec	aodv.tr	Blackaodv.tr
200	0	22
400	4	18
600	15	24
800	5	14
999	12	17

Table 2: value of the performance of Packet Drop Ratio with and without attack in AODV protocol

4.2. End-2-End Delay

It can be defined as the average time taken by the data packets to reach the destination.

$$\text{E2E Delay} = \frac{\sum (\text{arrive time} - \text{send time})}{\sum \text{Number of connections}}$$

The results are recorded as in the table below:

Time in sec	aodv.tr	Blackaodv.tr
200	29.17	23.3
400	35.75	36.68
600	103.72	97.57
800	101.82	81.92
999	122.55	79.04

Table 3: value of the performance of End to End Delay with and without attack in AODV protocol

5. Literature Review

In this section we will discuss some research work that has been already done by various authors.
Jasvinder et al., [8] proposed effects of E2E delay, throughput, network load on AODV in the absence and presence of the black hole attack. The work is simulated using 45 nodes moving at a constant speed of 10m/sec. It is observed that larger number of nodes affect the performance of the network using OPNET simulator.
Nital Mistry et al., [16] proposed the improved AODV protocol on NS-2 simulator ver.2.33 using single detection type. Simulation was performed with 25 nodes and 300s as the simulation time. The result showed improvement of Packet Delivery Ratio (PDR) by ~80% that lead to rise in end to end delay.
Ravi Kumar et al,. [10] proposed the effects of four parameters, End-to end delay, throughput, Packet Delivery Ratio and control overhead with different number of nodes taken as 10, 20, 30, 40 and 50, different pause time taken as 0s, 30s, 90s, 120s and 150s, and different network size. It was simulated using NS-2 (2.34) simulator. It concluded that DSR is better in terms of PDR when network size is less than 600*600 sq. m. As the network size goes beyond this, OLSR is better in terms of throughput and PDR.
Er. Pragati et al,. [11] proposed the simulation of AODV, LEACH and TORA protocols using parameters: End-to-End delay, Packet Delivery Ratio and Packet loss on NS-2 simulator. It was concluded that the packet delivery ratio was better for AODV but with the increased number of nodes, PDF in TORA increased. It was also calculated that average end to end delay increased in TORA as the number of nodes in the network were increased. Packet loss in TORA increased due to delay.

Ms. Gayatri Wahane et al,. [1] proposed an algorithm for detection of cooperative Black hole attack. This introduced the concepts of maintenance of data routing information table (DRI) and cross checking of a node. It was concluded that the proposed algorithm works well in case of detecting the cooperative black hole attack and ensuring a secure as well as a reliable route from source to destination. The work was simulated using throughput, average end-to-end delay, dropped packets and packet delivery fraction metrics on NS-2 simulator.

6. Conclusion & Future Work

This paper is about the simulation effect of
Black hole attack in the AODV protocol using Packet Drop Ratio and End-to-End Delay as parameters. The results have been indicated and recorded using these parameters. There is a gradual increase in the efficiency of the parameters when we analyze the results for the attack in AODV protocol. The result and analysis of these parameters on TORA protocol are to be measured and analyzed. The work on ZRP, OLSR and other protocols can be considered as future work.

7. References

i. Ms. Gayatri Wahane and Prof. Ashok Kanthe, "Technique for Detection of Cooperative Black Hole Attack in MANET". IOSR Journal of Computer Science (IOSR-JCE), e-ISSN: 2278-0661, PP.59-67, 2014.
ii. Ravinder Kaur and Jyoti Kalra, "A Review Paper on Detection and Prevention of Black Hole in MANET", International Journal of Advanced Research in Computer Science and Software Engineering", Vol.4, Issue 6, PP.37-40, June 2014.
iii. Irshad Ullah and Shahzad Anwar, "Effects of Black Hole Attack on MANET using Reactive and Proactive Protocols". International Journal of Computer Science Issues (IJCSI), Vol.10, Issue.3, No.1, 152-159, May 2013.
iv. Nisha, Simranjit Kaur and Sandeep Kumar Arora, "Analysis of Black Hole Effect and Prevention through IDS in MANET". American Journal of Engineering Research (AJER), Vol.02, Issue.10, pp-214-220, 2013.
v. Neha Kaushik and Ajay Dureja, "A Comparative Study of Black Hole Attack in MANET". International Journal of Electronics and Communication Engineering and Technology (IJECET), Vol.4, Issue.2, pp-93-102, March-April 2013.
vi. Harjeet Kaur, Manju Bala and Varsha Sahni, "Performance Evaluation of AODV, OLSR and ZRP Routing Protocols under the Black hole attack in MANET". International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE), Vol.2, Issue.6, June 2013.
vii. Harjeet Kaur, Manju Bala and Varsha Sahni, "Study of Black Hole Attack using different routing protocols in MANET". International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE), Vol.2, Issue.7, July 2013.
viii. Jasvinder and Monika Sachdeva, "Effects of Black Hole on an AODV Routing Protocol through the using OPNET simulator". International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue.7, July 2013.
ix. Vipan Chand Sharma, Atul Gupta and Vivek Dimri, "Detection of Black Hole Attack in MANET under AODV Routing Protocol". International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue.06, PP-438-443, June 2013.
x. Ravi Kumar and Prabhat Singh, "Performance Evaluation of AODV, TORA, OLSR, DSDV Routing Protocols using NS-2 Simulator". International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), Vol.2, Issue.8, August 2013.
xi. Er. Pragati and Dr. Rajender Nath, "Performance Evaluation of AODV, LEACH and TORA protocols through simulation". International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, Issue.7, July 2012.
xii. Kamini Maheshwar and Divakar Singh, "Black Hole Effect Analysis and Prevention through IDS in MANET". European Journal of Applied Engineering and Scientific Research, 1(4), 84-90, 2012.
xiii. Antony Devassy and K. Jayanthi, "Prevention of Black Hole Attack in Mobile Adhoc Networks using MN-ID Broadcasting". International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.3, PP-10170-1021, May-June 2012.
xiv. Shrevin Ehrampoosh and Ali Mahani, "Securing Routing Protocol: Affection on MANET's Performance". International Journal of Communications and Information Technology (IJCIT), Vol.1, No.1, pp.7-15, Dec 2011.
xv. Fan-Hsun Tseng, Li-Der Chou and Han-chieh Chao, "A survey of Black hole attacks in wireless mobile adhoc networks". Human Centric Computing and Informational Sciences, A SpringerOpen Journal, 2011, 1:4.
xvi. Nital Mistry, Devesh C Jinwala nad Mukesh Zaveri, "Improving AODV protocol against Black Hole attacks". Proceedings of International Multi Conference of Engineers and Computer Scientists, Vol.II, March 17-19, Hong Kong, 2010.
xvii. Payal N. Raj and Prashant B. Swadas, "DPRAODV: A Dynamic Learning System against Black Hole attack in AODV based MANET". International Journal of Computer Science Issues (IJCSI), Vol.2, PP.54-59, 2009.
xviii. Latha Tamilselvan and Dr. V. Sankarnarayanan, "Prevention of Cooperative Black Hole attack in MANET". Journal of Networks, Vol.3, No.5, PP.13-20, May 2008.
xix. Mohammad Al-Shurman and Seong-moo yoo and Seungjin park, "Black hole attack in Mobile adhoc networks". AMCSE¨04, April 2-3, Huntsville, AL, USA, 2004.
xx. Bo Sun, Yong Guan, Jian Chen and Udo W. Pooch, "Detecting Black Hole attack in Mobile adhoc Networks". The Institute of Electrical Engineers, Michael Faraday House, Six Hill Way, Stevenage SGI 2AY, EPMCC 2003.