IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 3 Issue 12 December, 2015

The Simulation Effect of Packet Drop Ratio, Graph Throughput and End-2- End Delay in simple TORA and Black Hole Attack in AODV using NS-2.35

Dipika Jain *
Student
Department of Computer Science & Engineering
PDM College of Engineering and Technology, B'Garh
MDU, Rohtak
dipikajain24.12@gmail.com

Abstract

In today's world scenario when we talk about the life of the people, then we can say that the life is so quick and fast, and therefore there are needs for various communicating methods. A good and efficient 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. The wireless network technologies have gained popularity across the world with the widespread use of laptops, smartphones and mobile phones. The uses of letters and pagers have been considered of early years or of the time of forefathers. Mobile devices are considered as tools for nowadays technologies. The mobile computing do not depend on the pre-existing infrastructure such as routers in wired networks or access points in wireless networks instead the use of Mobile Adhoc Networks have come into consideration. When we work on wireless networks, there are three main types namely, Mobile Adhoc Network, Vehicular Adhoc Network and Intelligent Vehicular Adhoc Network.

Here I would like to brief up the details of this paper. In this paper we are showing the simulation effect of the black hole attack on the AODV protocol using Packet Drop Ratio, E2E Delay and Graph Throughput as the parameters. These parameters have been determined over the absence and presence of the black hole attack over AODV protocol and the results are compared with the effective results obtained from the TORA protocols while in the absence of the black hole attack. The black hole attack may be either single hole black hole attack or cooperative black hole attack. Here in this paper, we have given individual graphical representation for the Packet Drop Ratio while have given the comparison results of the End to End delay and Throughput.

Authors may use other parameters for the comparison between the two protocols and can work on the black listing mechanism of the malicious nodes in the network.

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

I. 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.

There are other wireless networks which are used according to the use of user and the area covered. Moreover, any node in the network can anytime enter or exit the formed network. MANET has many characteristics which can be termed as, Dynamic

nature, Multihop Infrastructure, Clustering, Load Balancing and Security.
We learn about security attacks which are Active and Passive attacks. The Black Hole attack, Gray hole attack, Worm hole attack, Jellyfish attack etc are attacks under active attacks.
Here in this paper we learn about the network simulator, the routing protocols, different parameters used in this work. This work is carried out on NS-2.35 in RHEL6 platform.
The Network generally consists of two types of nodes namely the mobile nodes and in every cluster there is one master node. These nodes may travel across the network/ cluster and may enter any other cluster anytime. Thus the nodes are arbitrarily and dynamic in nature.

II. LITERATURE SURVEY

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.

Dipika Jain [21] has proposed her work on the AODV and TORA protocol, worked on Black hole attack using AODV protocol. The author had taken two parameters initially namely the packet drop ratio and End-to-End Delay. Here the tool Network simulator NS-2.35 is used over the Linux platform. It was tested with 3 nodes under normal conditions. The comparison was made between the results of the AODV protocol in its presence and its absence.

Neha Kaushik [5], had made an analytical study on the black hole attack, its types namely the single hole black hole attack and the comparative black hole attack in the tabular representation where the author had studied the recorded results over NS 2.34 Network simulator. She has recorded response for some of the types of routing protocols to study their behavioural changes and response of their effects due to the black hole attack.

Faa-Hue-[15], paper is all about the study of all the categories of black hole attacks. The author had made a theoretical survey regarding the attacks in MANET namely black hole attack, grey hole attack, jelly fish attack etc. Simple and cooperative black hole attacks with the broad classification of the three types of protocols in the network which are namely the pro-active, reactive and hybrid protocols.

III. 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 most popular network simulator 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.

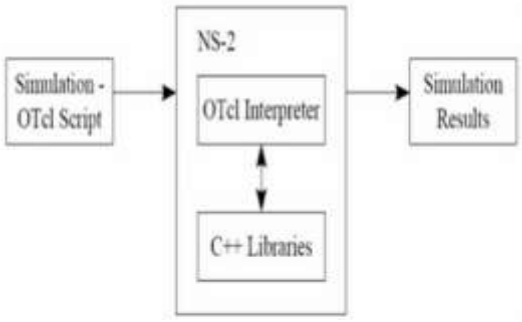

Fig1.1: Linking OTcl and C++ in NS2 tool

The network was created for 20 nodes with following values for the simulation parameters.

Table 1.1

THE TABLE OF PARAMETERS

Routing Protocols	AODV and TORA
No. of Nodes	20
Simulation Area	1000 x 1000
Simulation Period	1000ns
Connection Type	CBR
MAC Type	802.11

IV. ROUTING PROTOCOLS

There are several routing protocols in MANET which are divided into three categories based on their tendency of finding routes. These categories are Reactive Routing Protocols, Proactive Routing Protocols and Hybrid Routing Protocols.
Here the three protocols have been discussed precisely.

Reactive Routing Protocols are named as an on demand routing protocol or demand driven reactive protocol which gets active only when nodes want to transmit data packets to other nodes. They are AODV and DSR etc.
Proactive Routing Protocols are named as table driven routing protocol which maintain the table for the routes in the network. They are OLSR and DSDV etc.
Hybrid Routing Protocols retain the characteristics of both the above mentioned protocols which are namely the Reactive Routing Protocol and Proactive Routing Protocol. These protocols not only maintain table for the already routed paths but also find routes when required. They are ZRP and TORA etc.

The nodes in the network transfer data packets to other nodes and these data packets are sometimes attacked by intruders.
There are various Attacks in the network which can be classified as active and passive attacks. Black hole attack, Gray hole attack, Jelly fish attack and Worm hole attack are some of the security attacks in MANET.

Here we briefly discuss about the AODV protocol which is classified under Reactive Routing Protocol

V. 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.

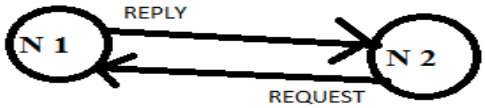

Fig: When the node N2 sends the request message to node N1, then Node N1 sends reply response to the node N2.

VI. 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 three of the parameters: The E2E Delay, Throughput and the Packet drop ratio.

A. 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 of AODV protocol without the Black hole attack is given by the graph below:

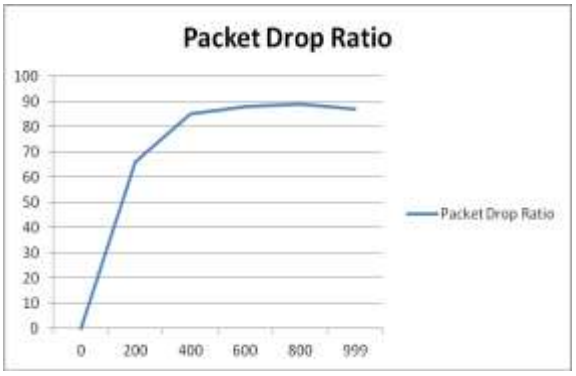

Fig1.2: PDR in Absence of Black hole Attack

The result on the AODV after the Blackhole attack is as given below:

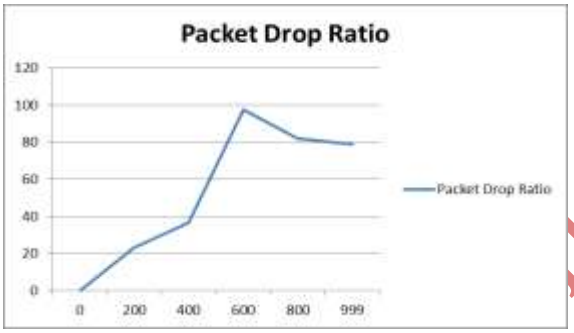

Fig 1.3: PDR in Presence of Black Hole Attack

The results with TORA we see the result in TORA as in the graph shown below:

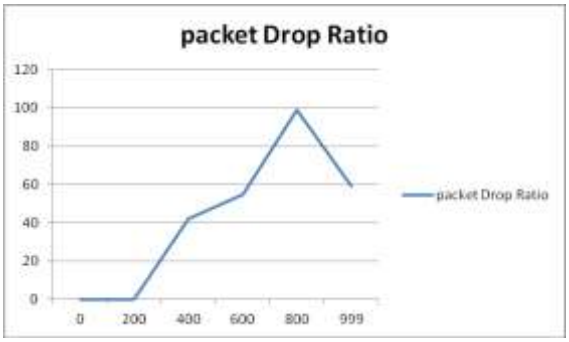

Fig 1.4: PDR in TORA Protocol

B. 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 in table 1.3:

Table 1.3

Time in sec	aodv.tr	Blackaodv.tr
200	7541.78	23.3
400	12053.37	36.68
600	11278.27	97.57
800	11031.76	81.92
999	11888.15	79.04

The results can be shown graphically as below:

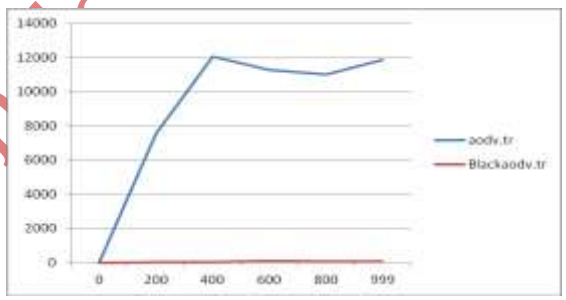

Fig 1.5: Comparision of E2E Delay in AODV protocol

C. THROUGHPUT

The average number of data packets that were delivered to the destination.

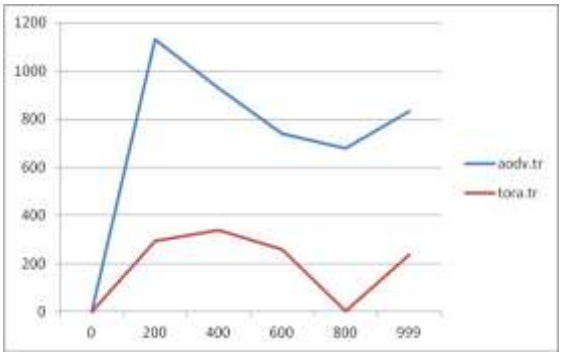

Fig 1.6: Comparision of Graph Troughput in AODV Protocol

VII. PREVENTION METHODS

It is said that "Prevention is better than cure". So it is suggested that a researcher/developer take preventive measures before hand so as to be safe. There are various methods that may be used for preventing Blackhole attacks in AODV protocols. Selectively some techniques are as given below:

It can be IDS, Intrusion Detection System, where the nearby node detects the abnormality in the network and broadcasts the message informing all the nodes about the abnormality of any node present in the network.

Second can be CMAS, Check-point Multihop Acknowledgement Scheme, where the intermediate node is randomly chosen as the checkpoint node which is responsible for detecting the defected node or the malicious node in the network.

The mobile nodes are as the name suggests are randomly moving from one place to another within the network or even they may move outside the network.

VIII. CONCLUSION & FUTURE WORK

This paper is about the simulation effect of Black hole attack in AODV protocol using Packet Drop Ratio, Graph Throughput 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 also measured and analyzed. The work on ZRP, OLSR and other protocols can be considered as future work. The author may find the Black Listed node in the network and broadcast the same in the network.

IX. REFFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] Dipika Jain, Ms. Sunita Sangwan, "The Effects of black hole attack on AODV and TORA protocols: A Review", IJETT, Vol. 20, No. 1, Feb 2015.

