The Effects of Packet Drop Ratio and End-2-End Delay in AODV and TORA Protocol using Black Hole Attack in NS-2.35 on RHEL6

Dipika Jain, Ms. Sunita Sangwan

***Abstract*— A network is basically a connection between two or more devices such as computers, telephones, mobiles and laptops etc. The connection can be either a wired connection or a wireless connection. Wireless network connection can be an infrastructureless network with no central administrator. Such a wireless network connection is termed as Adhoc networks. When all the nodes in this network are mobile, then the network is said as mobile adhoc networks (MANET). The nodes are mobile and can anytime freely enter or exit the network. The network has a dynamic topology, self-organizing nodes and is multihop in nature. The paper is about the general survey of the routing protocols and the black hole attack. This paper has two major sections, first is about the general MANET and second is the study of network simulator, NS-2 which concludes with the proceeding implementation work showing the effect of black hole attack on AODV and effect of the same on the TORA protocol over end to end Delay and Packet Drop Ratio as the parameters in the third section which is followed by the comparison and conclusion of the work**

***Index Terms*— MANET, Routing Protocols, Black Hole Attack, Network Simulator**

Abbreviation

MANET: Mobile Adhoc Network
AODV : Adhoc On Demand Distance Vector Routing Protocol
TORA : Temporal Ordering Routing Algorithm
DRI : Data Routing Information
E2ED : End to End Delay
PDR : Packet Drop Ratio
RHEL6 : Red Hat Enterprise Linux 6.

I. INTRODUCTION

MANET is an infrastructureless wireless network which consists of a number of nodes moving around in a network. There are various issues that can be discussed in MANET like Routing, Security, Clustering and Load Balancing etc. Before these issues come the routing protocols in MANET.

II. 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.

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 have the characteristics of both the above mentioned protocols 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.

III. Black Hole Attack

One of the active security attacks, Black hole attack is where the data packets are either damaged or stolen before it reach the destination node. The protocols like AODV, DSR, and DSDV etc are prone to such an attack. Black hole attack can be an internal or an external attack. It can further be classified as:

- ➢ Single black hole attack and
- ➢ Cooperative black hole attack

IV. Single Black Hole Attack

A single black hole attack is when one malicious node in the network claims itself as the shortest path to reach the destination node. The source node sends the data packet to this malicious node which is either dropped or delayed by the node. There is no interaction among the source and destination nodes regarding the data packet. There can be several ways to detect this attack in the network. One of them is neighborhood based detection method. In this scheme, the unconfirmed nodes are identified along with a new routing path from source to destination. It uses lower detection time.

Manuscript received July 11, 2015

Dipika Jain, Student , Department of Computer Science & Engineering PDM College of Engineering & Technology B'Garh, Haryana

Ms. Sunita Sangwan, A.P.,Department of Computer Science & EngineeringPDM College of Engineering & Technology B'Garh, Haryana

V. Cooperative Black Hole Attack

The scheme of cooperative black hole is considered when single black hole detection fails. A cooperative black hole is when some malicious nodes collaborate together to behave as the normal route. These nodes hide from the single black hole detection schemes. Several schemes of detecting the cooperative black hole are presented as, DRI table and Cross Checking Scheme, Distributed Cooperative mechanism, Hashed based scheme and Backbone nodes and restricted IP scheme. In the scheme of DRI table and Cross Checking every node maintains a DRI (Data Routing Information) table where bit 1 stands for 'true' and bit 0 stands for 'false'. They maintain table of 'from' and 'through' bits on the data packets. In the scheme of cross checking, the source node sends the request message in order to find a secure route for transfer of data packets to the destination node. The intermediate node generates a reply message to the source node which contains information regarding the next hop node with a DRI table entry. The source node checks this entry with its own DRI table to identify it as a reliable node.

VI. Network Simulator

While survey regarding the Black hole attack in MANET there come across various network simulators which help in simulating the entire network in a system without the use of numerous routers and other infrastructure. The network simulators can be listed as NS-2, NS-3, OPNET and QualNet 5.1 etc.

Network Simulator is a series of discrete event driven network simulators in computer networks. It is generally used in teaching and research areas. NS-2 generates two files namely .tr and .nam files. '.nam' is abbreviated for Network Animator and '.tr' for trace file.

NS-3 is freely available software publicly available under GNU, GPLv2 license for research, use and development. It is used to create an open simulation environment.

OPNET and NetSim etc are proprietary Software available for network simulation.

VII. Related Work

In this section we will discuss about the past work of the authors in some of the papers:

In the year 2014, Ms. Gayatri Wahane and Ashok Kanthe, [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.

In the year 2013, the authors, Nisha, Simranjit Kaur and Sandeep Kumar Arora, [4] analysed the effect of Black hole attack through IDS in MANET. They worked on the effect of attack on network performance using NS-2 simulator. They measured their results using parameters- throughput, PDF and routing load. They proposed the solution to the prevention against the black hole attack using Intrusion Detection System(IDS). They conclude that the value of routing load increases in the presence of black hole attack in the network but drops when IDS is applied to it.

Antony Devassy and K. Jayanthi [13], proposed their work using NS-2 simulator. They has proposed a broadcast method to prevent the black hole attacks imposed by both single and multiple black hole nodes.

Manju, Harpreet Kaur and Varsha Saini [6], proposed their work using Qualnet 5.1. They analysed the performance of Proactive, Reactive and Hybrid Routing Protocols.

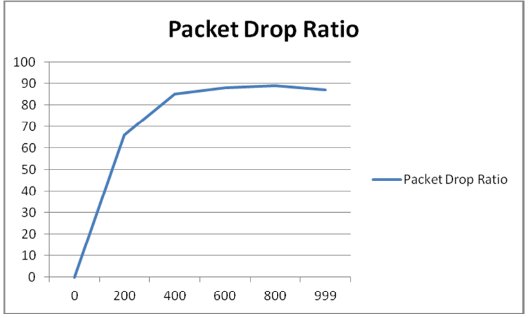
In July 2013, Jasvinder and Monika Sachdeva, [8] proposed effects of E2E delay, throughput, network load on AODV in the absence and presence of the black hole attack. The work is simulated using 45 nodes moving at a constant speed of 10m/sec. It is observed that larger number of nodes affect the performance of the network using OPNET simulator.

In August 2013, Ravi Kumar and Prabhat Singh, [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.

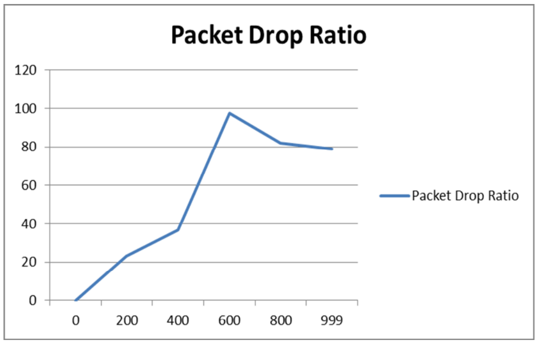
VIII. Simulation Results

In this section of the paper, the graphical results of the simulation are been presented so as to analyze the work in a better way. The results are generated in four cases as AODV without attack, AODV with attack, TORA without attack and TORA with attack respectively.

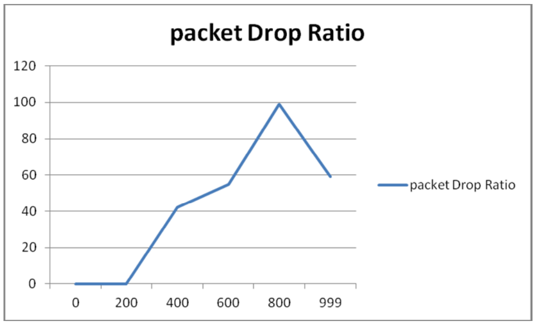
The results of AODV protocol without the Black hole attack is given by the graph below:



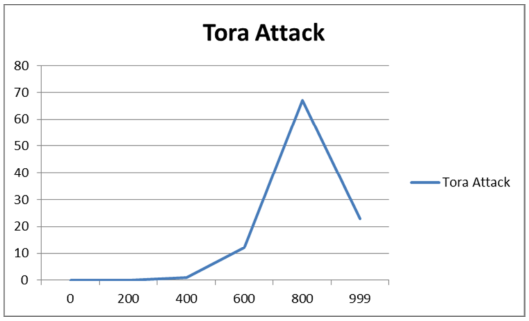
The result on the AODV after the Blackhole attack is as given below:



When we compare the above results with TORA we see the result in TORA as:



The above graph shows the packet delivery ratio in TORA protocol withut the Black Hole Attack while the graph for with Black Hole Attack in TORA Protocol is given below:



we can see the results directly from the graphs. Similar results have been recorded for the parameter End to End Delay over all the above four cases as mentioned above for the packet drop ratio.

IX. Comparision of Results

When we come across the comaprision of the effects of the Black hole Attack in AODV and TORA protocols, there is a gradual difference that canbe observed seeing their performance graphs. In AODV Protocol, using packet delivery Ratio parameter we observe that there is a tremendous increase in the beginning and later the performance remains almost stable showing no much deviation. While after the attack in AODV we can observe that there is regular change in the performance of the protocol with the change in time. Similarly when we observe TORA protocol without attack, it is showing no change at the beginning but later it is changing with the change in time. Moreover if we look through the compilation of the two protocols, the performance of AODV is faster than that of TORA.

Conclusion & Future Work

The paper is about the use of a network simulator for the deployment of the network. There are some simulators that are the open source while others are proprietary software. The paper is about the use of the network simulator to implement the black hole attack in AODV and TORA protocols, observe and compare the effects of the attack using various parameters. We record the working of its Effects on the two protocols using NS-2.35 in RHEL6. Comparing the effects of security attacks using ZRP, OLSR and DSR etc can be deployed as future work. The authors can also work on the field of black listing the black node in the network.

References

[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] Manjeet Singh and Gaganpreet Kaur, “A surveys of attacks in MANET”. International Journal of Advanced Research in Computer Sciences and Software Engineering (IJARCSSE), Vol.3, Issue.6, June 2013.

[12] 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.

[13] Antony Devassy and K. Jayanthi, “Prevention of Black hole Attack in Mobile Ad-hoc Networks using MN-ID Broadcasting”. International Journal of Modern Engineering Research, Vol.2, Issue.3, May-June 2012.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.