An Efficient and Secure AODV Routing Protocol Against Black Hole Attack

Saurabh Sharma[1], Vandana M. Rohokale[2]

[1] *Research Scholar, CSE, GTU PG School, Gujarat, India*
[2] *Dean R&D, ETE, SKNSITS, Maharashtra, India*

ABSTRACT

Mobile ad-hoc network (MANET) is wireless decentralized network, where network nodes move dynamically. The fact that mobile ad-hoc networks (MANET) lack fixed infrastructure and use wireless link for communication makes them very susceptible to malicious attacks. Ad-hoc On-demand Distance Vector (AODV) is one of the most widely used routing due to its dynamic nature that is routing information is exchanged and path finding process is initiated only when path is required by a node to communicate with a destination node. One of the main problem with AODV is that it is vulnerable to Black hole attack. In a Black hole attack, malicious nodes attract data packets and drop them instead of forwarding. During Black hole attack, a malicious node captures packets and not forwards them in the network and advertises itself as having the shortest path to the node whose packets it wants to intercept. In this paper we propose a secure and modified version of the AODV protocol which will encounter the black hole attacks and as it will detect the Black hole node and then prevents against it.

Keyword : *- AODV , MANET, Black hole attack, and Malicious node*

---

1. Introduction

The meaning of Ad hoc in Latin is “for this purpose only”, Mobile Ad-hoc Network abbreviated as MANET is a collection of mobile node which do not have any centralized infrastructure and in which every mobile node will act like router also that can communicate with each other wirelessly. They communicate directly if they are in same communication range else they would require cooperation of each other.

As MANET does not have any fixed infrastructure therefore it can be deployed quickly and will be cost effective. This nature of MANET makes it useful for the deployment in many real life situations ex disaster relief operations, conferences, military rescue missions, and virtual classrooms. [1]

MANET nodes consist of Laptops, PDA, Mobile phones etc. having limited computation, communication and energy resources. Due to having features like open medium, dynamic changing topology, no centralized supervision, limited energy, no strict boundary, and wireless links of MANET it is more vulnerable to attack. [1]

1.1 Applications of MANET

MANET simulation code can be applied in following areas.

- At Local level
- In Military battlefield
- Collaborative networks
- PAN or Bluetooth networks

1.2 Protocols in MANET

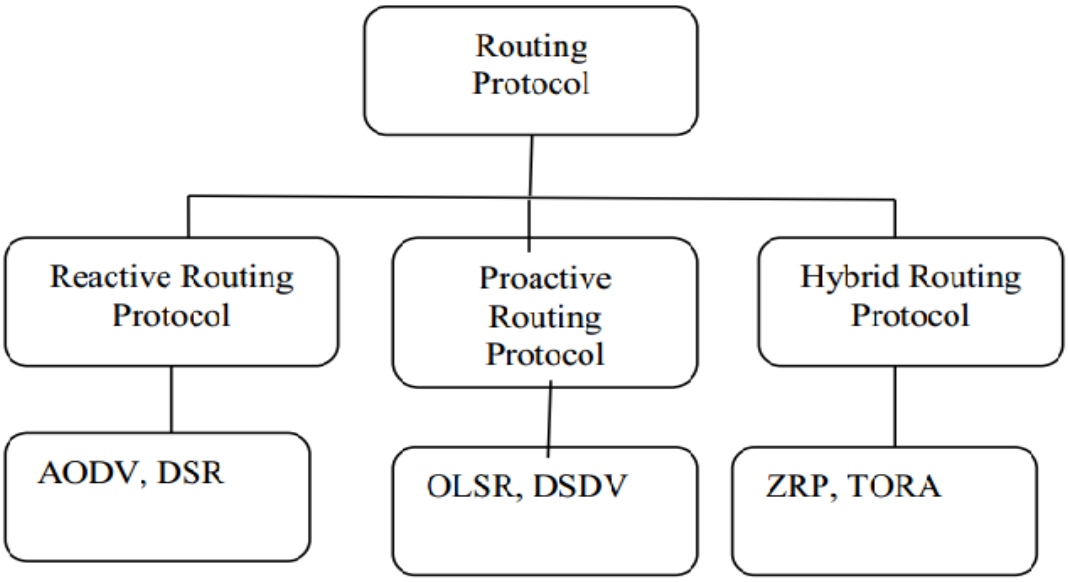

Fig -1: Routing Protocols

2. Overview of AODV Protocol

The AODV or Ad-hoc On-demand Distance Vector protocol is used in system because it takes least congested route instead of the shortest route, It supports Multicast and unicast packet transmissions for nodes. [5] The AODV routing protocol is used by mobile nodes in an ad hoc network. It gives an quick adaptation to dynamic link conditions, low processing and low network utilization, memory overhead, and determines unicast routes to destinations within the ad hoc network. The destination sequence numbers is used to ensure loop freedom at all times avoiding problems (such as "counting to infinity") associated with classical distance vector protocols.

2.1 Blackhole Attack

Blackhole attack is kind of DOS attack. In this attack malicious node attempts to fool down the sender node by giving an impression that, it is all legitimate node by sending the false reply message to the sender. The malicious node will reply with the very high sequence number so that the sender node would think that malicious node is the destination node or it has a new and fresh node to destination [3].

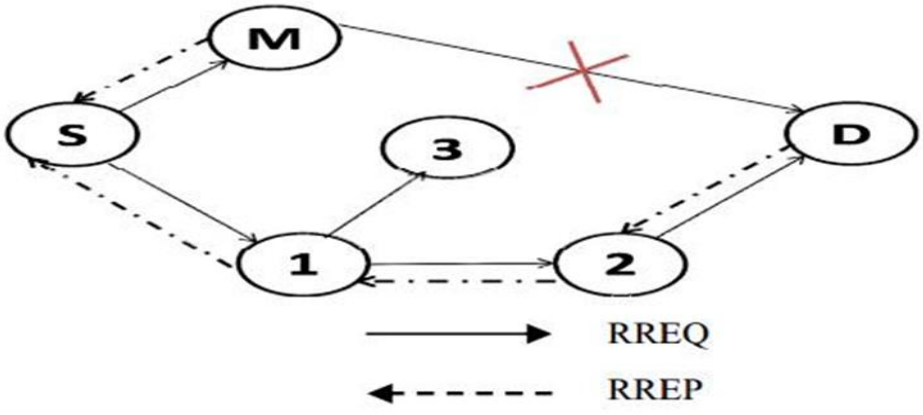

Fig -2: Black hole Attack

2.1 Existing System

The problem with the existing system is that whenever a black hole node is present there it will not be able to recover from the communication loss and drop of data packets and the detection of malicious node is not possible. The blackhole attack is very serious problem in MANET as it drops the packet and can cause network establishment failure. Many solutions to prevent and detect the blackhole attack has been proposed but they are not efficient. The packet delivery ratio very badly affected by the blackhole nodes. So there was a need of a model which can overcame this problems and can enhance the packet delivery ratio of the system.

3. Proposed System

The proposed model introduces a new concept for detection and prevention against black hole attack. In addition we have also provided and addition security check by comparing the destination sequence number against as the malicious node have very high sequence number which is nearly not possible for a system.

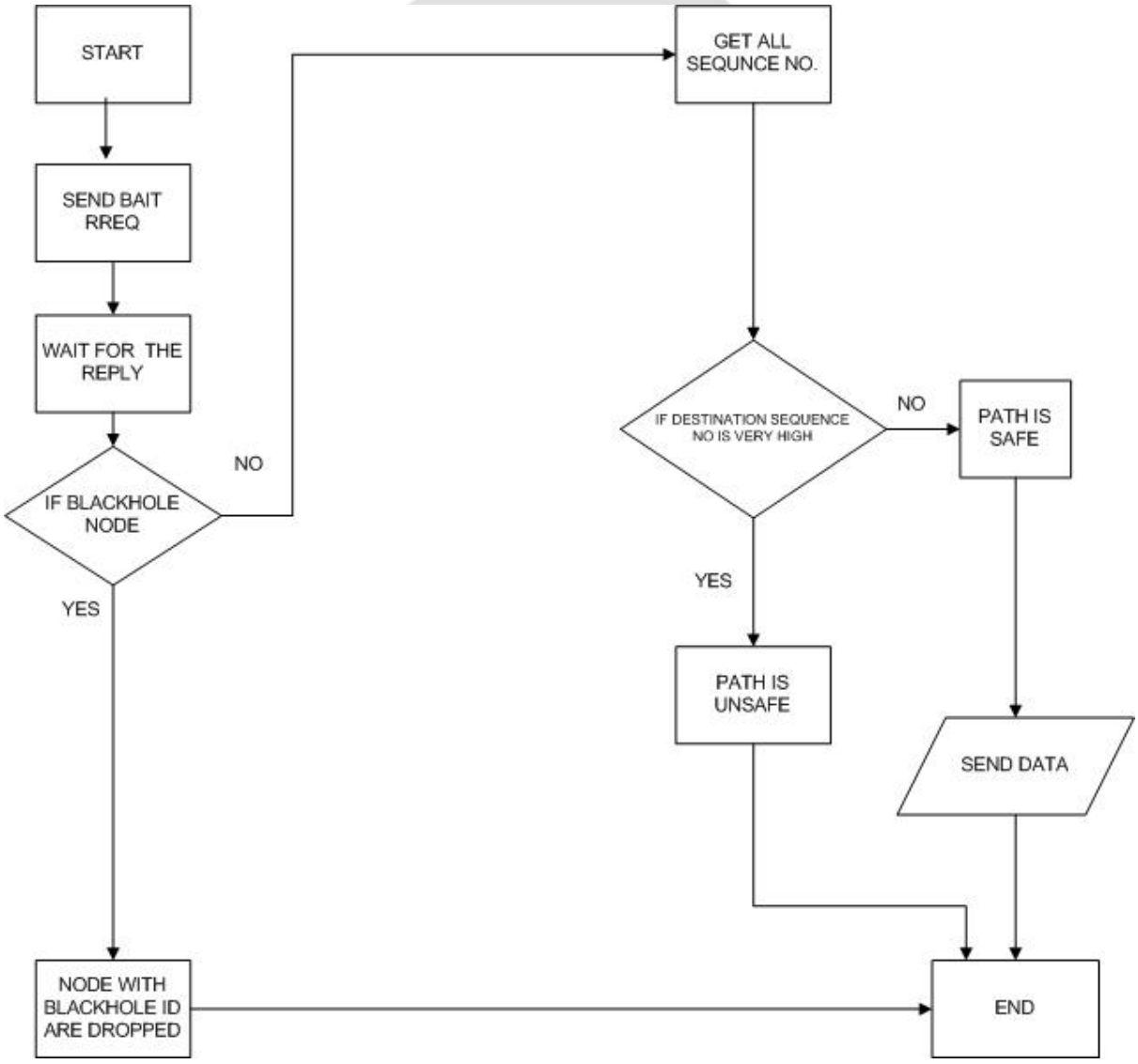

Fig -3: Proposed System

3.1 Implementation

For the implementation we are using NS-3 simulator for the simulation purpose and Net Anim-3.107 for viewing the simulation of nodes and their metadata.Here we are simulating AODV routing protocol with creating 25 nodes which are trying to ping the destination as node no.56 which does not exist in network.
The steps are as follows:
srb@ubuntu:~/Desktop/ns-allinone-3.25/ns-3.25$ CXXFLAGS="-Wall"
srb@ubuntu:~/Desktop/ns-allinone-3.25/ns-3.25$ ./waf --run scratch/aodv_ping

The output of the simulation is shown below:

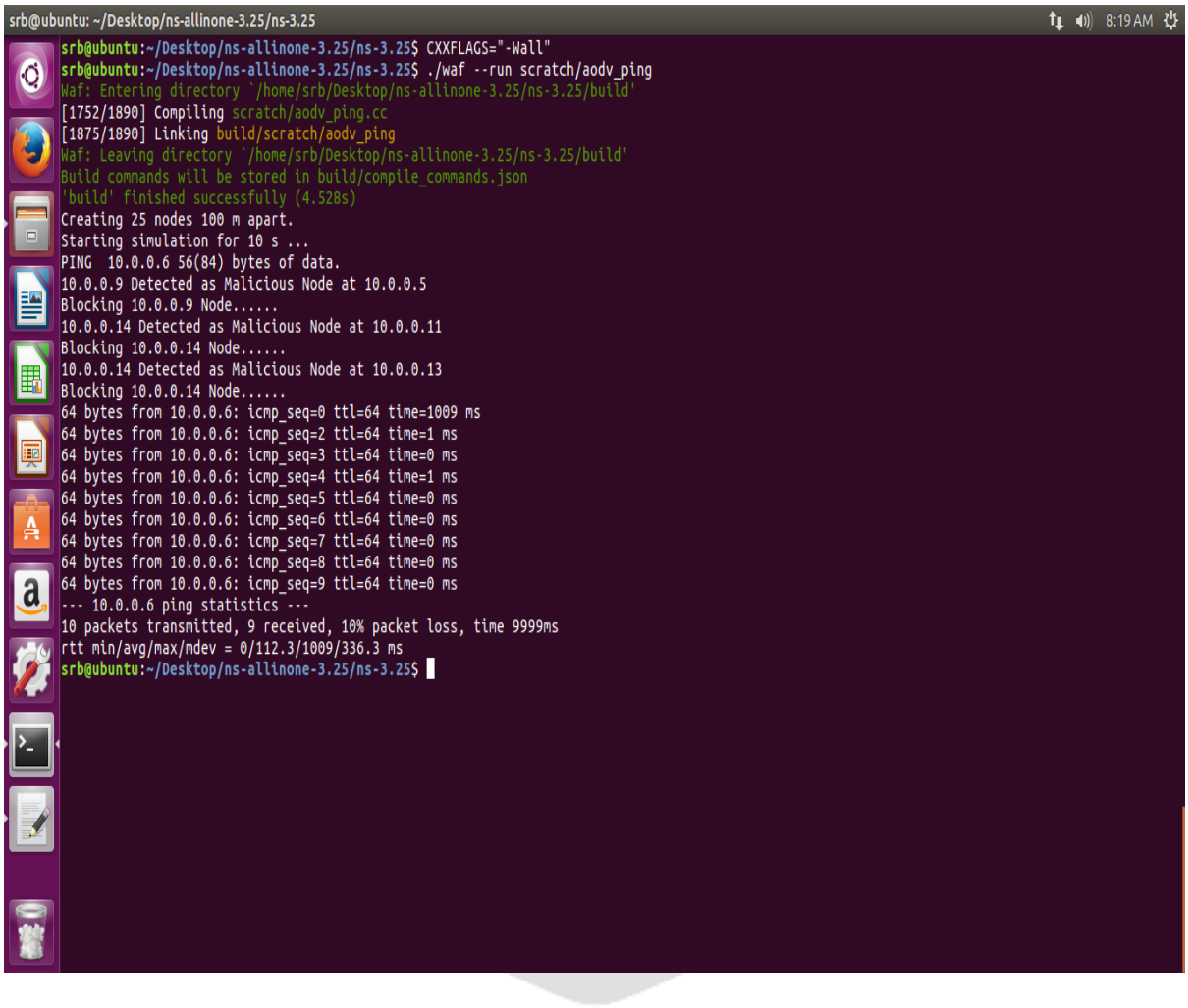

Fig -4: Output of the simulation of 25 nodes on 2 blackhole node

Here in this scenario, we are detecting and blocking the malicious node. We have defined node 8 and 13 having IP 10.0.0.9 and 10.0.0.14 as malicious which is giving RREP to the neighbour without looking into its routing table

STEPS : srb@ubuntu:~/Desktop/ns-allinone-3.25/netanim-3.107$ ./NetAnim

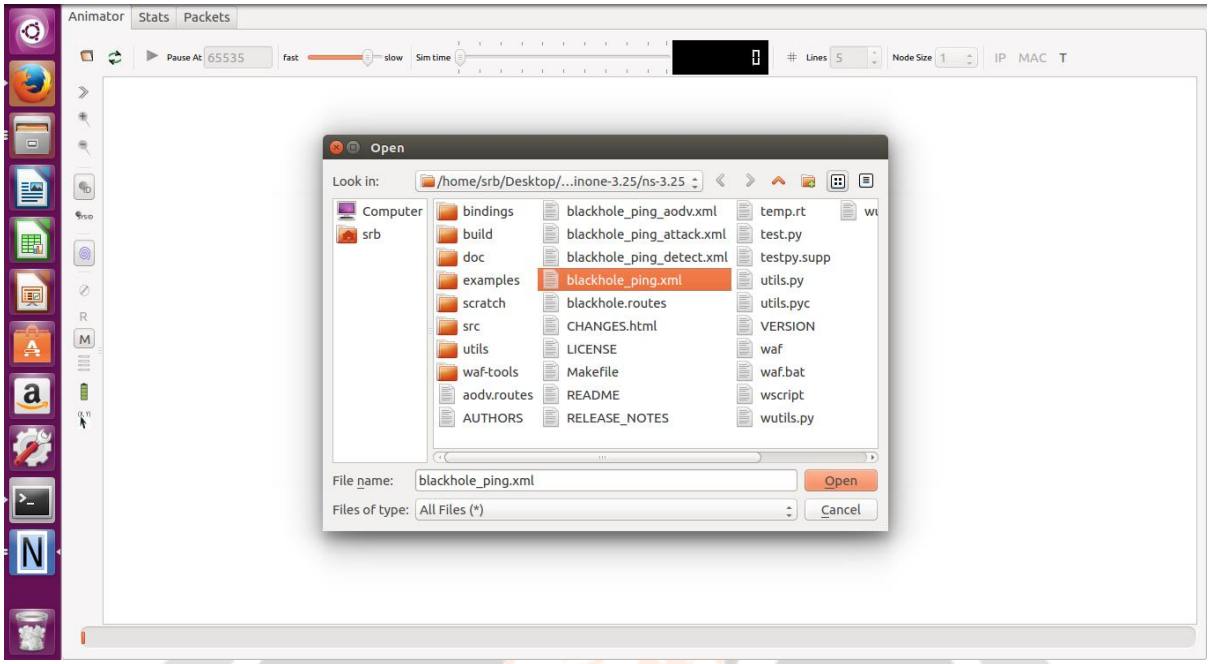

Fig -5: Generated Net-Anim xml file

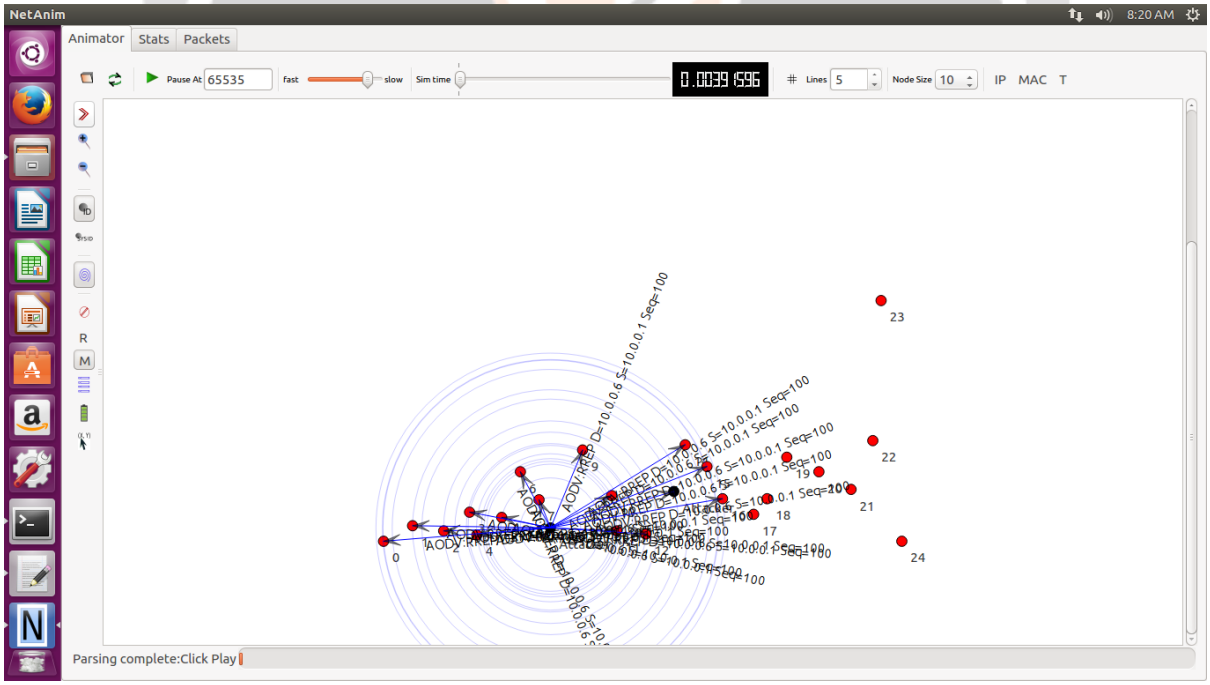

Fig -6: Net-Anim Simulation on first blackhole node

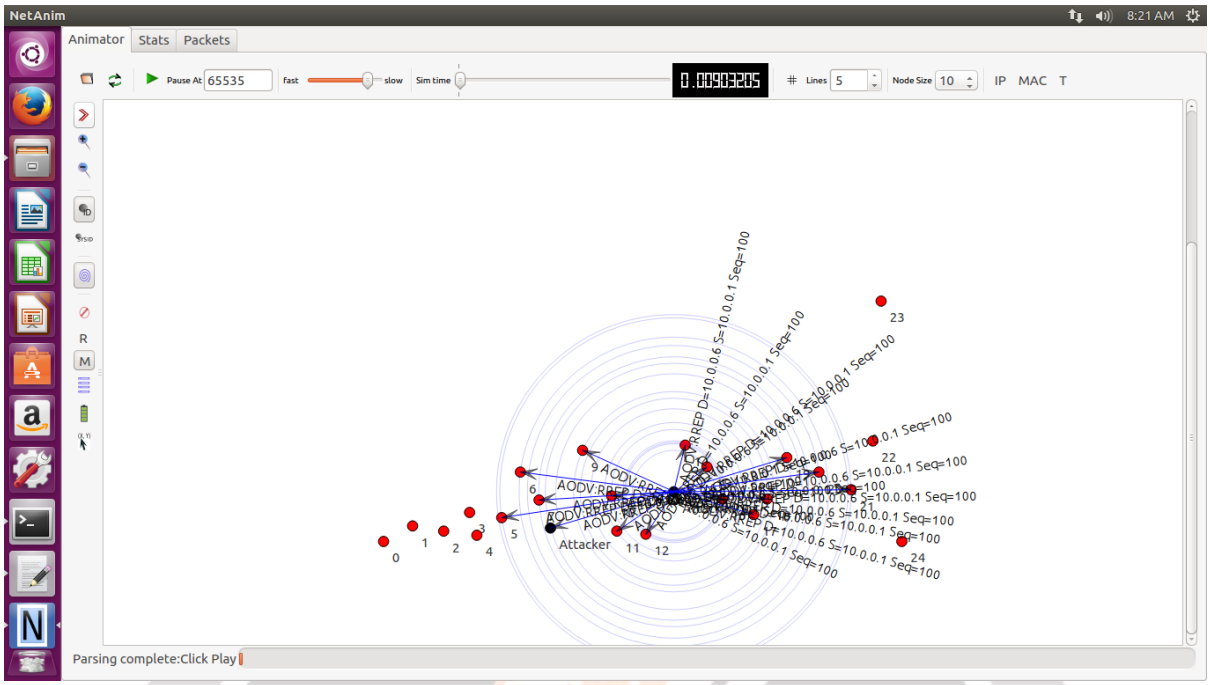

Fig -7: Net-Anim Simulation on second blackhole node

3.2 Implementation of mechanism 2

Implement AODV routing protocol with creating 25 nodes which are trying to ping the destination as node no.56 which does not exist in network using mechanism 2.

srb@ubuntu:~/Desktop/ns-allinone-3.25/ns-3.25$ CXXFLAGS="-Wall"

srb@ubuntu:~/Desktop/ns-allinone-3.25/ns-3.25$ ./waf --run scratch/aodv_ping

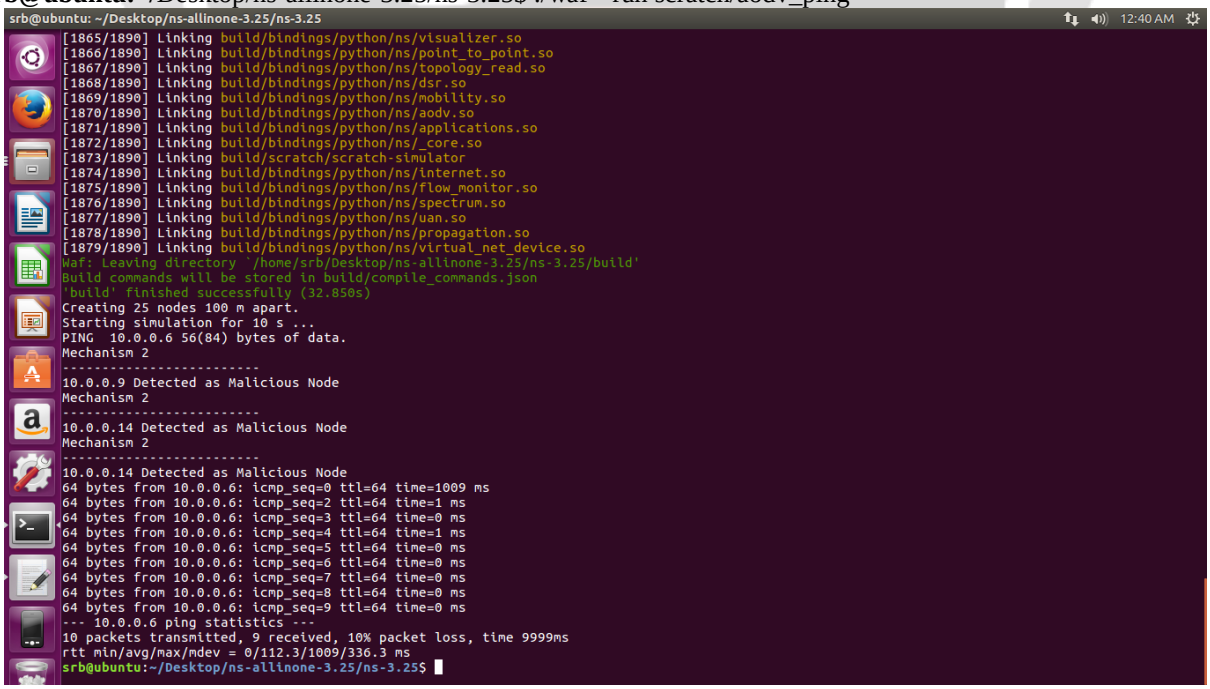

Fig -8: Output of the simulation of Mechanism 2

4. Performance Analysis and Comparison

The ratio of the number of data packets delivered to the destination nodes and the number of data packets sent by source nodes.

Packet delivery ratio = (Re*ceived packet* / *Sent packet*)∗100%

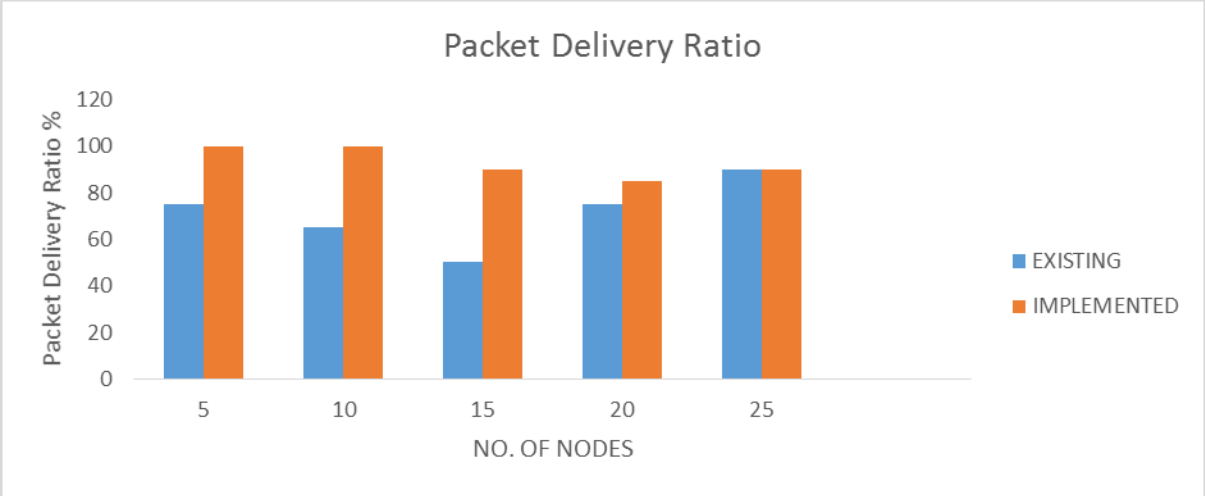

Chart -1: Performance Analysis and Comparison Graph

The above graph shows the improvement in the packet delivery ratio of the existing system. The implemented system enhances the packet delivery ratio quite successfully.

5. CONCLUSIONS

The blackhole attack is a serious threat that need to be resolved but at the same time the methods proposed should also be efficient. The methods and techniques that were discussed are not sufficient and do not satisfy the need. The method which we have proposed will first detect the blackhole node and then it will be prevented. Along with all these we have been able to successfully implement the proposed system which enhances the packet delivery ratio of the system.

6. REFERENCES

[1]. Sakshi Jain, Dr. Ajay Khuteta, "Detecting and Overcoming Blackhole Attack in Mobile Adhoc Network" 2015 IEEE.

[2]. Ashish Kumar Jain, Vrinda Tokekar, "Mitigating the Effects of Black hole Attacks on AODV Routing Protocol in Mobile Ad Hoc Networks", 2015 International Conference on Pervasive Computing (ICPC).

[3]. Gaurav Singal, Harshit Garg, Vijay Laxmi, Manoj Singh Gaur, Chhagan Lal, "Impact Analysis of attacks in Multicast Routing Algorithms in MANETs", IEEE 2016.

[4]. Mr. Ankit D. Patel, Mr. Kartik Chawda, "Blackhole and Grayhole Attacks in MANET", ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India. IEEE 2014.

[5]. Subhashis Banerjee, Mousumi Sardar, and Koushik Majumder, "AODV Based Black-Hole Attack Mitigation in MANET", ACM 2014.

[6]. Araghi, T. K., Zamani, M., Manaf, A. B. A., Abdullah, S. M.,Bojnord, H. S., & Araghi, S. K. (2013). A secure model for prevention of black hole attack in wireless mobile ad hoc networks. In 12th WSEAS international conference on applied computer and applied computational science, Malaysia.

[7]. Bhatia T, Verma AK (2013) Security issues in MANET: a survey on attacks and defense mechanisms. Int J Adv Res Comput SciSoftw Eng 3(6):1382–1394.

BIOGRAPHIES

	Saurabh Sharma PG Scholar – at – GTU PG School in IT Systems & Network Security , **Ahmedabad , Gujarat** BE – at LDRP – ITR (GTU) in **Computer Engineering, Gandhinagar , Gujarat**
	Dr. Vandana M. Rohokale Doctorate in Wireless Communication at Aalborg University, Aalborg, Denmark under supervision of Prof. Ramjee Prasad on 2nd Sept 2013. Master Of Engineering in "E & TC Engineering" (M.E. Electronics) from RIT Rajaramnagar, Sangali from Shivaji University, Kolhapur, Maharashtra, India in Jan. 2007with first class. Bachelor Of Engineering (B.E Electronics) from AVCOE Amrutnagar Sangamner, from Pune University in Nov.1997 with first class.