iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VII **Month of publication:** July 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, July 2017- Available at www.ijraset.com

Efficient Dynamic Data Flow and Black Hole Detection in Manet

A.Vanathi[1] , A.S.S.D.Toyaza[2]
[1,2]*Computer Science and Engineering, Aditya Engineering College Surampalem, India*

Abstract: In Wireless networks, when data packets are being transferred between nodes from a specified node to destination, then source node checks for shortest path to reach destination. In this approach there may be a possibility of occurring attack called BLACKHOLE attack. In Black Hole attack, source node sends Route Request (RREQ) to its neighbor nodes to know which node contains shortest path to reach destination. So malicious node sends Route Reply (RREP) to source node that it has a valid route to destination and then responds with False Route Reply (RREP). Then Source node transmits data to the destination through this malicious node. Then the malicious node absorbs or drops the data packets that are destined for destination. In this, an approach is proposed to detect the malicious node along with Routing tables. It can also show the metric analysis like packets sent, packets Received, Dropped Packets etc. A Runtime frame work for dynamic data flow using Network Simulator2 (ns2) has been proposed to implement black hole attack.
Keywords: MANET, AODV, Black Hole Attack, Network Simulator 2, AWK

I. INTRODUCTION

Wireless network is a computer network that connects one node to another node and allows wireless data connection. MANET (Mobile Adhoc Network) is one of the types in Wireless Network Environment.

A. Manet

[1] MANET is a collection of different types of nodes with different architectures connected to each other. There will be a constant change in network Topology. Each node in the network forwards the packet without the need of central administration as it is adhoc type so that it does not depends upon on the foregoing infrastructure i.e. no need to access routers and other routing devices. Each and every node in this network acts like a router or host.

B. Types of Manets[2]

MANETS are categorized into 2 types

1) Vehicular Adhoc Networks
2) Internet Based Mobile Adhoc Network.
3) *Vehicular Adhoc Networks* (VANETs): are used for transmission among transport system mostly in roadside equipment.
4) *Internet Based Mobile Adhoc Networks* (iMANET): links mobile nodes and established gateway nodes which are transmit or receive stoppages.

C. Challenges of Manet [3]

1) *Black Hole Attack:* Black hole is a node referred as a malicious node that absorbs data packets passed through it. In MANET, a malicious node acts like a Black hole that drops all data packets passing through it. A black hole is a malicious node that falsely sends response for a route request even though it doesn't have any correct route to destination.
2) *Gray Hole Attack:* It also drops DATA packets but node's malicious activity is depends upon specific targeted node from which packets are coming or based on time i.e sometimes it acts as malicious and sometimes as normal node.
3) *Jellyfish Attack:* Here, There may be a chance of packet delay when they are transmitted to destination or it may even change the order of packets in which they are received and sends it in scrambled manner.
4) *Worm Hole Attack:* Here, a link was established called as worm hole link between any two points in the network .As soon as the link is connected the attacker seizes data or may exchange.

5) *Byzantine Attack*: In this type of network, an intermediate node forwards packets through incorrect paths or selective packet droppage that affects routing services. There are some more other attacks like Eavesdropping, Flooding attack etc.

D. Routing Protocols in Manet [4]

1) *Proactive Routing Protocols: These* protocols are used to conserve a record of all nodes and their paths in that network and it also take care of routing table dispensation systematically.

Examples: Optimized Link State Routing Protocol (OLSR) Destination Sequence Distant Vector (DSDV) hese type of protocols have limitations in conserving individual nodes information and it reacts slowly in case of reorganization and in non-fulfillment cases.

2) *Reactive Routing Protocols:* These protocols react to the action to be performed by them when and only another node sends request to it for a particular action.

Examples: ABR- Associativity Based Routing Adhoc On Demand Distant Vector Routing Protocol (AODV), Dynamic Source Routing (DSR) etc., When compared to all other protocols in reactive routing AODV has an advantage of flexibility to the networks which are in dynamic state and it also reduces overhead. Because of these advantages here AODV protocol is proposed.

3) *AODV Routing Protocol:* Adhoc on Demand Vector is a routing protocol for adhoc based networks. This protocol algorithm creates a route between nodes only when routes are requested by source node in order to transfer data. If a network is using this protocol routes are active only whenever data transfer takes place or path will time out when data transfer stops. Nodes can enter and leave the network as according to their wish.

E. Manet Simulators [5]

1) *NS2 (Network Simulator2*): NS2 is a simulator used to analyze the events that occurred in a particular interval of time and records the changes that are occurred. Different type of protocols like TCP and UDP are used for routing.
NS2 use C++ and Tcl languages.
2) *NS3 (Network Simulator3):* NS3 is advanced version of NS2.Ns3 can be implemented in windows 8.1 and later versions. NS3 was implemented in Python and C++ languages. C++ is used to implement simulation & core model.
3) *OPNET:* OPNET is used to develop an environment which is used to model the nodes connected in a network. C is the main language used in OPNET and also Graphical User Interface.
4) *OMNeT++:* This simulator is also for simulating networks, and it is also helps to model the scenario like allocating resources and time to execute processes. It uses an eclipse based IDE for simulation purpose.
5) *NETSim:* It supports an object oriented approach for simulating data and voice based communication. NetSim uses java and HTML.
6) *JSIM:* JSIM means Java Simulator. It mainly focuses on fields like physiology and bio-medicine.
7) *REAL:* It is used to study the dynamic behavior of data flow and controls the data in the form of packets that are routed with destination address. It is used to specify and observe the behavior of networks and it uses C as a programming language.
8) *GLOMOSIM:* It stands for global mobile information system simulator for large and wire line communication network. It is a C based Simulation tool.

II. LITERATURE SURVEY

A. Black Hole Attack

In black hole attack, a node requests other nodes that have shortest path to the destination node. Then other nodes will reply to that node request which are having shortest path. This node advertises its availability of modern routes without examining its routing table. So then attacker node will always have a chance for replying to the route request and thus obstruct the data packet and preserve it. When this route is fixed, now attacker node can drop all the packets or forward it to the uncertain address.

B. How Black Hole Attack is Implemented

AODV protocol is used for routing purpose. There are 2 types of black hole attack implementation in AODV.

1) *Internal Black Hole Attack:* This type of black hole attack consists of internal nodes which are malicious nodes that outbreak in between the routes of specified source and destination. Whenever this malicious node gets the chance, then it actively

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, July 2017- Available at www.ijraset.com

participates in route to obstruct data transfer. Whenever data is being transferred this node performs its attack on data. This is an internal attack because node itself belongs to the data route.

2) *External Black Hole Attack:* This attack can be implemented as follows:

a) The node which wants to attack detects the route in which data transfer is going to take place and notifies the destination address.

b) A route reply packet (RREP) along with the destination address will be sent.

c) RREP will be sent to the nearest node which is available in its range that belongs to the current route. If route is available, then reply is also sent to the source as it sent request for the routes.

d) The updated information received along with the route reply will allows the source node to update its routing table.

e) Then source node selects its newly available data to transfer data.

f) The data which is passing through the route in which malicious node is there, then it drops data packets.

C. Marjan Kuchaki rafsarjani, Zahra Zahed Anvari, Shahla Ghasemi proposed detection [6]

The whole data that is to be transmitted will be splitted into k identical parts. Then this number of parts will be sent to destination by source in the form of message. Not only to destination these parts will also sent to the nodes that present in between source and destination. After confirming that destination node had received the count of splitted parts source starts to transmit data. It will set a timer throughout the transmission of data between source and destination. If source gets a message from destination that it had received less amount of packets than it was sent then it indicates that black hole attack was occurred.

D. Jagdish J. Rathod, Prof. Amite. M. Lathigra Proposed Detection [7]

In this proposed system the node which wants to transmit the data S sends route request packet (RREQ); nodes within its transmission range, the node which exists in that route receive the RREQ and resend RREQ to their adjacent nodes until a node having a valid route to the destination. This node sends RREP to the source node on the reverse path of RREQ. The malicious node M sends RREP with higher sequence number to the source; another RREP is sent by Destination having genuinely higher sequence number. As malicious node sends RREP with higher sequence number than the normal node, Source node chooses path through malicious node to transfer data packets and therefore malicious node can drop some or all received packets which degrades the performance of the network.

III. PROPOSED METHOD

A. Detection

Proposed system includes dynamic environment working, it considers users choice to enter number of nodes they want and also user has to select source and destination for data to be transferred. In this method node that want to transmit data referred as source node sends a route request (RREQ) to nodes which exists in its transmission range, when intermediate node receive the RREQ and forwards RREQ to their neighbors until a node having valid route to the destination is noticed. Then this node sends RREP to the source node. Then malicious node assume as M sends RREP to source by pretending that it has shortest route to destination. Then source sends data through that malicious node as it has shortest path. In this case data may lose or may exchange. In this process malicious node was created randomly and whenever data passed through this node data packets are dropped at that node resulting in displaying routing tables and metrics like packets sent, packets received and dropped packets.

B. Prevention

Here Routing tables are maintained at each and every node with fields node name, from node-indicates 1 when data from any node is received before or indicates 0 if there is no such case

Through node-indicates 1 if this node has transferred any data to other nodes before or indicates 0 if there is no such case.

Suspicious –indicates when there is no confirmation in detecting whether it was suspicious or normal based on combination of from node and through node fields

In the above manner by maintaining routing tables black hole attack can be prevented based on those table values.

IV. MAIN CONSTRUCTION

A. Node Creation

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, July 2017- Available at www.ijraset.com

To create a node in NS2, the syntax to be followed is set nodename [$ns node]

B. Dynamic Node declaration

Here numbers of nodes are declared dynamically, user's choice to pass number of nodes the user needs.

C. Dynamic Node Creation

Here number of nodes to be created is entered by user choice then the network will be created with the chosen number of nodes. We can also set the color of nodes.

D. Link Establishment

Here using rand (), it generates some random value based on that value the nodes will take their appropriate positions in the network.

E. Packet Transmission

This scenario describes how data is being transmitted between nodes in a wireless network. Data packets are transmitted based on the bit rate.

F. Black Hole Attack

A network of some nodes based on the users choice will be created with specified source and destination. A malicious node which is technically termed as black hole is randomly generated and drops or absorbs the packets which pass through it.

G. AWK

Awk is a programming language used to process text files named after its authors who developed it.

A: Alfred aho
W: peter Weinberger
K: brian Kernighan
In ns2 AWK script file is used to process the trace files

AWK uses some of the following things to represent the status of a node and its related information.
In trace files each line starts with one of these three letters:

S-send packet
R-received Packet
D-Dropped packet

Node status given to each number in trace files and these are used in AWK scripts for processing:
$1 indicates ACTION status of a node.
$2 denotes the time taken to start transmission of data or whole data transfer
$3 is used to identify the node in a network among other nodes.
$4 represents the layer in which transmission takes place.
$5 indicate flags
$6 represents Sequence number of the data packets.
$7 indicates type of the packet
$8 is used to know the size of the data packet
For AWK files .tr files must be given as input which are generated after executing .tcl scripts

V. EXPERIMENTAL SETUP

For the simulation of MANET NS2 tool is used .Installed the ns2 tool in VMware workstation under Windows 7 operating system.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, July 2017- Available at www.ijraset.com

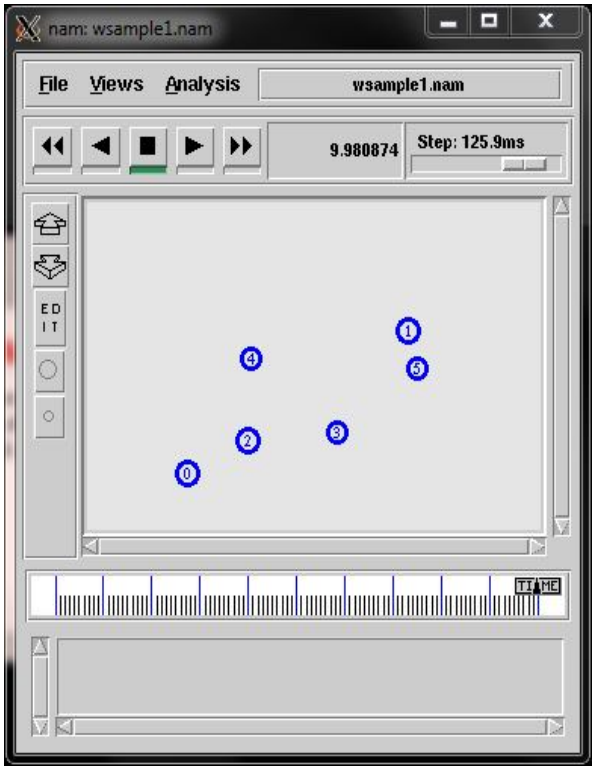


Fig 1: Dynamic Node Creation

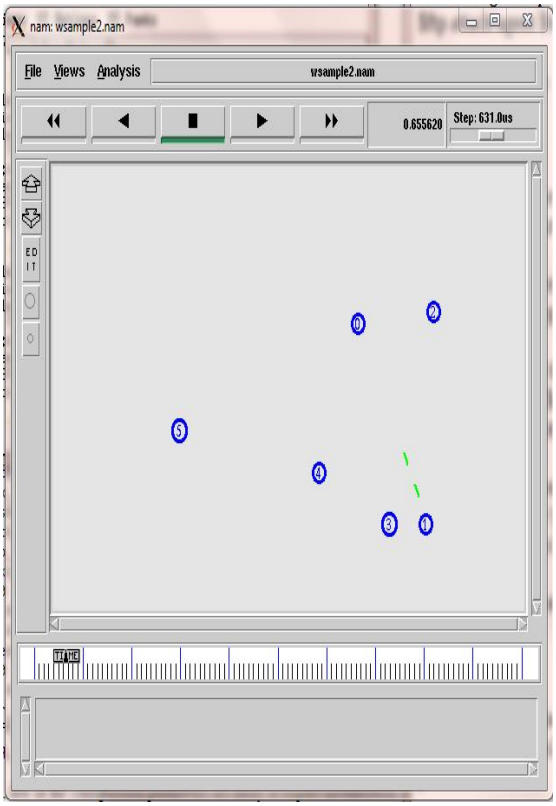


Fig 2: Data Transmission between nodes 0 and 1

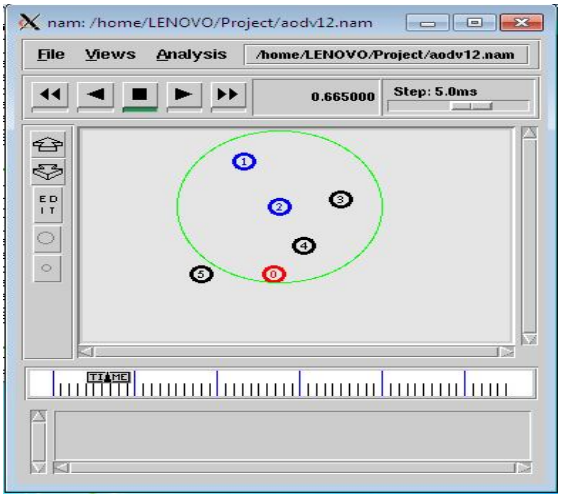


Fig 3: Attacker Node Creation

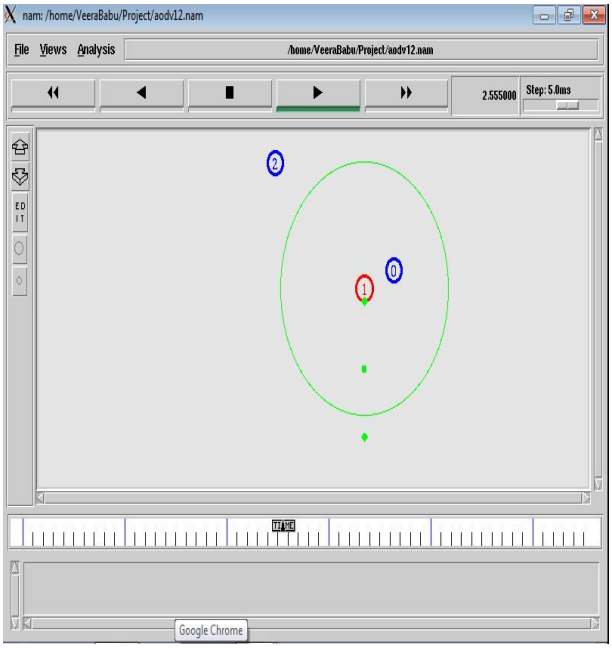


Fig 4: Packet Dropping at Malicious node

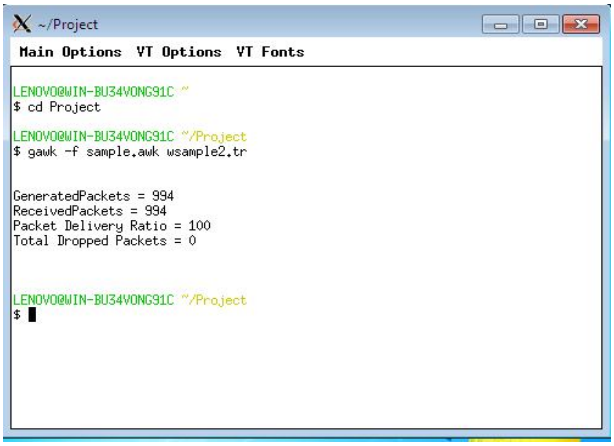


Fig 5: Metric Analysis for data transmission

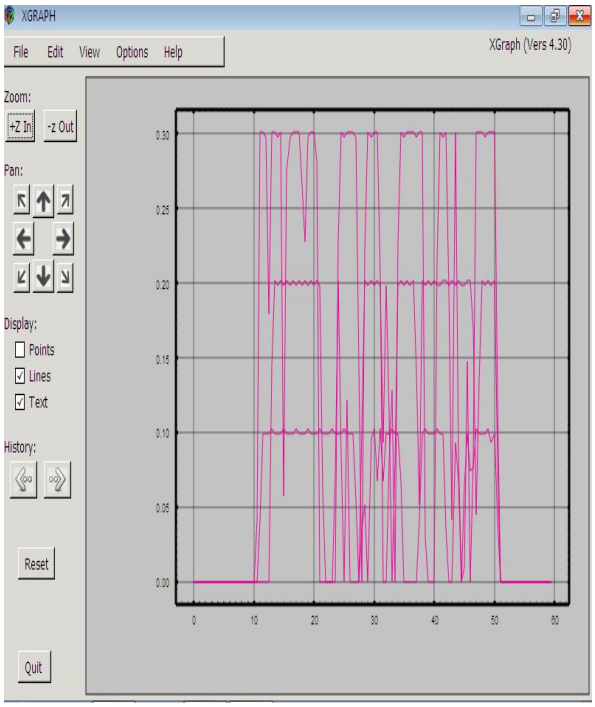


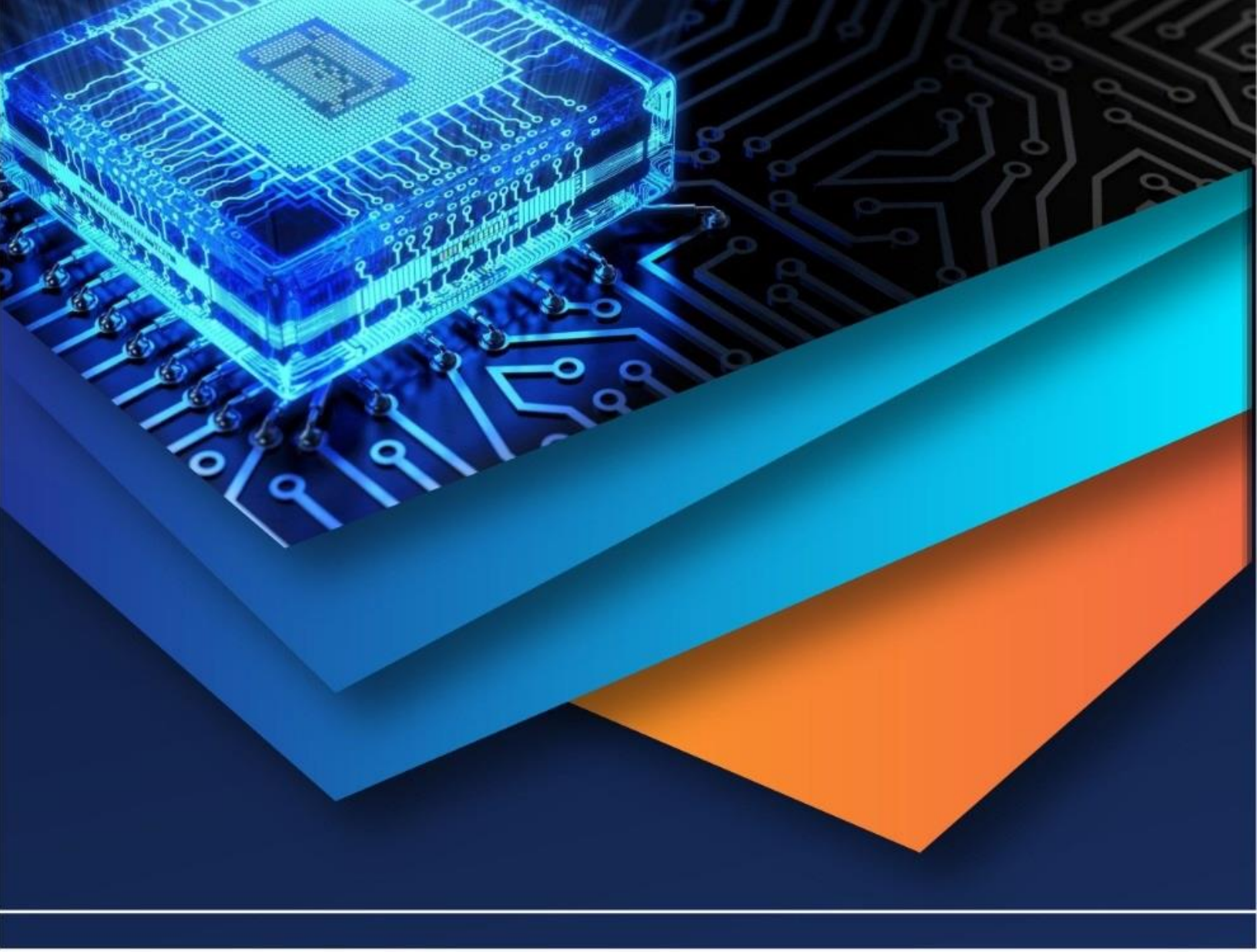
Fig 6: XGRAPH showing bandwidth ratio

VI. CONCLUSION

As usually wireless networks are more prone to severe attcks. To transmit data in wireless networks securely more security prevention mechanisms should be taken. Whatever implemented in this paper was done in a simulator called Network Simulator2. So, here an approach is proposed to detect black hole attack by using AODV reactive routing protocol and dynamic data flow that results in generating routing tables. And also packet metrics are analyzed using AWK scripting. Here a method is proposed that deals with how to prevent the black hole attack in wireless environment. This paper can help you in future to prevent black hole attack in wireless environment.

REFERENCES

[1] https://arxiv.org/ftp/arxiv/papers/1111/1111.4090.pdf
[2] http://wirnet.blogspot.in/2009/09/types-of-manet.html
[3] http://searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks
[4] https://en.wikipedia.org/wiki/List_of_ad_hoc_routing_protocols
[5] ns3simulation.com/listofnetworksimulatrs/
[6] A Survey of various Methods of Preventing and Detecting Attacks on AODV-based MANET Jagdish J. Rathod, 2Prof. Amit. M. Lathigra
[7] Comparative study of reactive routing protocol (AODV, DSR, ABR and TORA) in MANET Mr. L Raja 1 , Capt. Dr. S Santhosh Baboo2



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY