International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2015): 6.391

Intrusion Detection and Response System in AODV for Mobile Adhoc Network

Manpreet Kaur[1], Manoj Kumar[2]

Yadavindra College of Engineering, Talwandi sabo, Bathinda, Punjab, India

Abstract: ***Mobile Adhoc network is dynamic topology network in which all nodes can cooperate with each other for data transmission. But some nodes are not cooperative they drops some data packet which is called gray hole attacks. In the past, various techniques are used for detecting these attacks. In the proposed approach we use a gray hole intrusion detection system (G-IDS) for detecting gray hole attack. The G-IDS node monitors the traffic in network and it checks the activity of each node in the network. When it detects that at any node the difference of packet forward and packet receive is greater than threshold value then it sends the alert notification to all nodes about this malicious node. Then all nodes block this malicious node from the network. The proposed approach is compared with the existing approach on the performance parameters. The result in packet delivery ratio, packet loss rate and average throughput prove that this technique is better than other existing techniques.***

Keywords: MANET, Gray hole attack, Gray hole intrusion detection system

1. Introduction

A Mobile Adhoc Network is collection of independent mobile nodes that are connected with each other without any fixed infrastructure [1] .The nodes are cooperating with each other for transmitting the data packets [2]. The different routing protocols are used for routing the data packets like Adhoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR) [3]. Due to dynamic behavior of network malicious nodes easily enter in the network and drop the data packets. If malicious node drops all packets it is called black hole attack and if it drops only selective data packets it is called gray hole attacks. In black hole attack malicious node enters in network during route discovery process when source node broadcasts the route request message to all nodes in the network then malicious node sends fake reply message to source nodes claims that having shortest path through it and attracts all the data traffic and drops all data packets. In gray hole attack malicious node behaves normal in the route discovery and when path is established through gray hole node then it drops some packets of data [4]. Various intrusion detection techniques are used to detect the malicious node in the network [5, 6, 7] and Intrusion response system is used to response the intrusion that is detected by intrusion detection system in the network [8]. In this paper for detecting the gray hole attack Gray hole Intrusion Detection System (GIDS) is used with the AODV protocols.

The rest of this paper is organized as follows: Section 2 discuss the related work on routing security in MANET. Section 3 defines the proposed mechanism used for proposed work. Section 4 defines the simulation parameters that are used for the execution of the proposed work. Section 5 defines the performance analysis of the proposed mechanism. Section 6 concludes the paper and future scope of the work.

2. Related Work

In [9] author proposed new technique for detect gray hole attack in MANET. In this technique source node first sends the message about the total no of packets sent by the source to the destination after transmission if destination node does not receive the actual number of packet that is sent by the source node then destination node finds the malicious node through detection process. The destination node sends the query request to neighbour nodes at two hopes from it and waits for query reply. In query reply packet information is about the packets sent by the node to its next hope. When it receives query reply from neighbour nodes then checks its previous node transfer all the packets that is received from its previous node. If it has found that at previous node some data packets are lost then it alerts the IDS nodes for the malicious node. The IDS node monitors the attacker node and removes it from the network.

In [10] author proposed intrusion detection for detecting packet drop attacks in MANET. It detects gray hole and black hole attacks. In both attacks malicious node sends fake route reply during the route discovery process that having a shortest path to the destination node when data is transfer through that node then it drops the data packet. In this proposed mechanism monitoring nodes detect all nodes activity in the network it checks incoming and outgoing packets at each node. If incoming and outgoing packets are not same then the node is detected as attacker node and data is resend through a new route.

In [11] author proposed intrusion detection system for detect attacks. In which one node is selected as cluster head node for monitors the network. The system is work in four modules .in first module cluster is formed and one node is choose header node that is selected according to the battery power. In second module two nodes are selected for communication and data packets encrypted at the sender node and AODV protocol is used to transfer of data transmission. In third module gray hole attack node is find and in last data packet is decrypted and acknowledgement is send. The different parameters are calculated for the proposed system.

In [12] author proposed approach is based on Sequence number for mitigate gray hole attacks. In proposed scheme

two new fields are added in the routing table node status and reply time. Node status defines the node is normal node or malicious node and reply time is the last reply for destination node. A node is detected as malicious node if there is large difference between the node reply destination sequence number and in the routing table than the threshold value. Then a bait request packet is sent to the detected malicious node with non existing destination if the malicious node sends the reply for that destination. Then the node is declared as malicious node and nodes discards all reply packets from that node.

In [13] author proposed intrusion detection system to mitigate smart gray hole attack in MANET. In this approach a special node G-IDS (Gray hole intrusion detection system) is used for detecting smart gray hole attack. G-IDS node monitors the nodes transmission in the network. It checks the number of packet received by node and number of packet forwarded by node. If there is difference between the received and forwarded packets then the node is a malicious node and G-IDS sends the alert message to all the nodes and places that node in black list table. The source node deletes the entry of this node from the routing table and discovers new route.

3. Proposed Mechanism

In proposed work MANET has been designed for communication from sources to destination via intermediate nodes. In MANET security is main concern. In our proposed work gray hole and black hole attacks are detected and prevented by designing an algorithm that works based on AODV routing protocol. In our proposed work G-IDS node monitors the nodes activity in network. G-IDS node is selected randomly from the network. The node that have packet delivery rate is more selected as G-IDS node. GIDS node checks the packet loss rate at each node if packet loss rate is greater than threshold value then the node is detected as malicious node. G-IDS broadcast the alert message to all nodes. In the alert message contains the information about gray hole node.

4. Simulation

NS-3.2 simulator is used for proposed methodology. In an area of 750*750 m, 20 normal nodes executing AODV routing protocols were randomly distributed, and maximum of two malicious node, performing smart gray hole attack, are randomly located. In each scenario, all nodes were located in different positions and moved with different mobility speed of 5, 15, 25 m/s. the important parameters are listed in table.

Table 4.1 Simulation parameters

Parameters	*Value*
Dimension	750*750m
Total number of nodes	20
Simulation time	500 s
Traffic type	CBR
Packet size	512 bytes
Connection	UDP
Mobility model	Random waypoint
Mobility speed	5,15,25 m/s
Protocol	AODV

Network performance is calculated through following performance matrices.

- Packet delivery rate: It is calculated by the packet received by the receiver divided by total number of packets sent by the sender.
- Packet loss rate: It is calculated by the total number of packet drop during communication divided by total number of packet sent by sender.
- Average Throughput: it is amount of data per time unit that is delivered from one node to another via a communication link. It is measured in unit of bits per second.

5. Results and Discussions

5.1 Packet delivery rate

In figure 1 packet delivery rate is shown with different mobility speed of nodes. In existing approach packet delivery rate is 96.55, 96.56, and 95.68 % respectively with different mobility speed 5, 15, 25 m /s. In proposed approach packet delivery rate is 99.79, 97.24 and 98.14%. It can be seen from the figure that proposed approach gives better result than the basic approach.

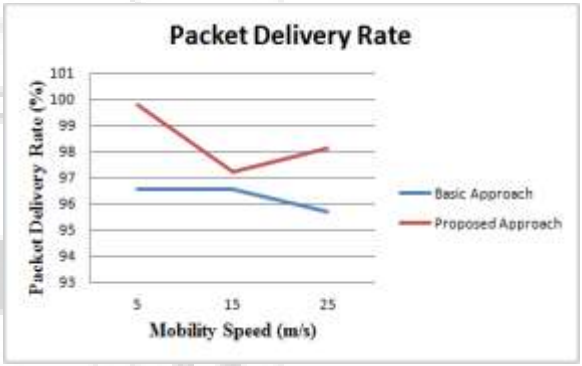

Figure 1: packet delivery rate

5.2 Packet loss rate

In figure 2 packet loss rate is shown with different mobility speed of nodes. In existing approach packet loss rate is 3.45, 3.44, and 4.32 % respectively with different mobility speed 5, 15, 25 m /s. In proposed approach packet loss rate is 0.21, 2.76 and 1.86 %. It can be seen from the figure that proposed approach gives better result than the basic approach.

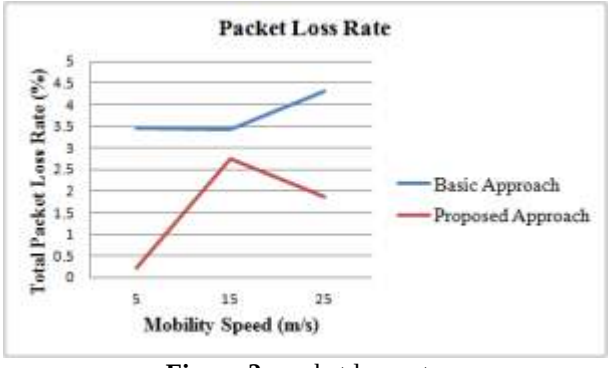

Figure 2: packet loss rate

5.3 Average Throughput

In figure 3 average throughput rate is shown with different mobility speed of nodes. In existing approach average throughput is 19.30, 19.32, and 19.15 kbps respectively with different mobility speed 5, 15, 25 m /s. In proposed approach average throughput rate is 115.86, 78.91 and 54.88 kbps. It can be seen from the figure that proposed approach gives better result than the basic approach.

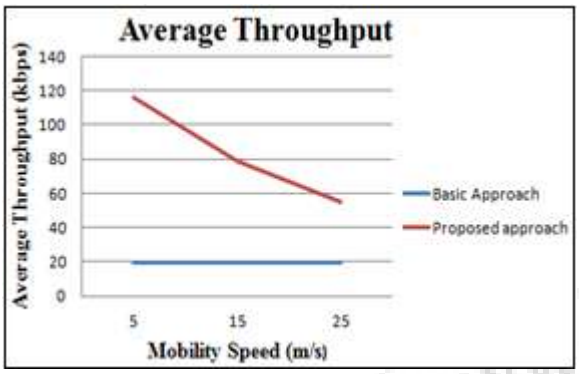

Figure 3: Average throughput

6. Conclusion

In MANET, nodes are cooperating with each other for data transmission in network. Some nodes are not cooperative for transmission and it drops the packets of data. When it drops the all packets of data it is called black hole and if it drops only selective data packets it is called gray hole attack. Two types of gray hole attack is performed in sequence based gray hole attack malicious node reply with false route and drops selective data and in smart gray hole attack malicious node act as normal node in route discovery process and when data transmission is performed it drops selective data packets. Various techniques are used for detects the gray hole attack in recent years. In proposed technique we use a G-IDS (gray hole detection system). In which G-IDS covers some simulation area and monitors the data traffic in this area. Proposed approach prevents and mitigate gray hole attack in the network. The Simulation results show that the performance of our proposed approach is better than existing techniques in different parameters measurements packet delivery ratio, packet loss ratio, and throughput.

In future other machines like neural network and soft computing must be proposed and implemented for same problem in which result is better than the Mobile Adhoc networks. The proposed approach is then compared with its existing counterpart and compared on the basis of other performance parameters.

References

[1] Mahima Chitkara and Mohd. Waseem Ahmad, "Review on MANET: Characteristics, Challenges, Imperatives and Routing protocols", International Journal of Computer Technology Mobile Computing, Volume 3, Issue 2, February 2014.
[2] Aarti and Dr. S.S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.
[3] Muhammad Safdar et al, "Comparative Study of routing protocols in Mobile Adhoc Networks", International Journal of Computer Science Trends and Technology (IJCST), Volume 4, Issue 2, March-April 2016.
[4] Bobby Sharma, " A Distributed Cooperative Approach to Detect Gray hole attacks in MANETs", In proceeding of WCI, ACM, 10-13 August 2015.
[5] Adnan Nadeem, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attack", IEEE Communication surveys, 2013.
[6] Rizvi et al, "A Review on Intrusion Detection System", International Journal Of Advance Research in Computer Science and Management Studies, Volume 3 Issue 3, March 2015.
[7] Sheenam and Sanjeev Dhiman, "Comprehensive Review: Intrusion Detection System and Techniques", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 18, Issue 4, July-August 2016.
[8] Zakira Inayat et al, "Intrusion Response System: Foundation, Design and Challenges", Journal of Network and Computer Applications, 2016.
[9] Mohanpriya M. & Krishnamurthi, "Modified DSR Protocol for Detection And Removal of Selective black hole attack in MANET", Elsevier Computer and Electrical Engineering, 2014.
[10] Shivani Uyyala & Dinesh Naik, "Anomaly based Intrusion Detection of Packet Dropping attacks in Mobile Adhoc Networks", International conference on Control, Instrumentation, Communication and Computation Technologies, 2014.
[11] Rahul Funde & Pankaj Chandre, "Dynamic Cluster Head Selection to Detect Gray Hole Attack using intrusion detection system in MANETS ", ACM, 25-27 September 2015.
[12] Rutvij H. Jhaveri & Narendra M. Patel, "A Sequence number based bait Detection Scheme to thwart gray hole attack in Mobile Adhoc Networks", Springer Wireless Networks, 21 April 2015.
[13] Shashi Gurung & Siddhartha Chauhan, "A novel Approach for mitigation Of Gray hole attack in MANET", Springer Science & Business Media, 26 August 2016.