Detection And Prevention Of Distributed Denial Of Service Attack Using Choke Packet

Mariyam Fatima, Jameel Ahmad, Shish Ahmad

Abstract— Security is the most important theme which needs to be given uttermost importance. The MANET is more prone to security threats because of its dynamic nature. One of the attacks in MANET is the DDoS attack. DDoS attack is a type of attack in which certain nodes floods the target system by sending the packets with high speed resulting in the denial of services of the authorized users. In this paper, a novel scheme is proposed to deal with DDoS attack in the MANET. The proposed approach implements a choke packet technique to detect the malicious node i.e. the node which does not decrease its data transmission speed even after receiving the choke packet from the receiver end, is marked as a malicious node and also digital signature technique is used for verifying the malicious nodes. The simulation is performed on NS-2.

Index Terms— Choke packet, Digital Signature, DoS, DDoS, MANET

1 INTRODUCTION

AMANET is a multi-hop self-configuring and self-healing network in which different nodes are linked wirelessly which does not depend upon accessible secure set-up. Each node in this network is free to move and can also change its linkage with different nodes at times (Vrince Vimal and Madhav J. Nigam, 2017). Every node behaves as a router when they ahead traffic to another identified node in the MANET. A MANET is extra unguarded to heterogeneous attacks due to absence of centralized administrator and dynamic path set up nodes to transmit the packets in short span of time (Sandeep et al., 2017). MANETs should provide more awareness against loss of energy in the nodes as well as transmission power (Pai et al., 2017). The most common routing protocols that are used in MANET have sociable and collaborative environment but because of the presence of malicious and selfish nodes, MANET becomes more vulnerable to security threats (Parveen Kakkar and Krishan Saluja, 2016). The most commonly used routing protocols in MANETs are proactive, reactive and hybrid protocols (Atifa et al., 2015). It is used in many sectors such as the military sector, disaster relief situation, airports, etc (Neha Sharma and Anand Singh Bisen, 2016). MANET is extra unguarded to several attacks because of the following reasons:

First, there is no administrator to detect the misbehaving node. Second, MANET has limited power, so the nodes are not active all the time. Third, packet loss occurs because of an increase in mobility and interference between the nodes. Fourth, the dynamic topology and movability of nodes reduces the probability of detecting the misbehaving nodes, as they can disturb communication even before vacating the network. Fifth, decision-making power with respect to packet dropping is a complex process. Due to the restriction of mobility, power and dynamic topology of MANET, dropping of packets is not always because of the misbehaving node or occurrence of any type of attack. For example, packets can be considered as dropped due to a link break. Hence MANET is extra unguarded to many attacks including routing attacks, impersonation, and eavesdropping (Albandari et al., 2016). In DDoS attack the main effort is to assemble target system resources inaccessible to its authorized users. MANET is an example of distributed system that consists of migrant nodes that are wireless in nature can freely self organize themselves into a temporary ad-hoc network topology, allowing faultless interconnection without preceding communication framework and central manager. Due to its exclusive aspects, MANET is vulnerable to different security threats, and that particularly makes it responsive to the DDoS attack. The system that falls under the attack is called as “primary victim”, whereas the system that launches the attack is often known as “secondary victim”. Presently, MANETs are basically unguarded to various varieties of DDoS attacks:

i) Active DDoS attack- This attack occurs when a misbehaving node has to tolerate some energy cost to resulting in occurrence of the threat
ii) Passive DDoS attack- This attack occurs mostly because to the lack of collaboration with the ambition of saving energy selfishly (Afroze Ansari and Dr. Mohammed Abdul Waheed, 2017).

DoS attack is also called as Node Isolation Attack which is mainly caused by the attacker in the OLSR protocol (R. Bhuvaneswari and R. Ramachandran, 2017). DoS attack generally results in the dropping of the packets. Packet dropping attacks generally happen from a router end or at a node that results in DoS attack using some DDoS tools (P. Rathiga and Dr. S. Sathappan, 2016). This paper introduces a novel approach to detect and mitigate the DoS attack in MANET. Specifically, a choke packet method is used to detect the DoS attack and in order to mitigate such attack; a digital signature technique is used for verifying the malicious nodes. This paper is classified as- Section 2 explains the work related to detect and mitigate the DoS attack. Section 3, explains the proposed system used for DoS attack. Section 4, explains the results and analysis of applying the proposed approach to MANET. Finally, section 5 explains the conclusion.

- *Mariyam Fatima is currently pursuing masters degree program in Computer Science and Engineering in Integral University, India. E-mail: f.kulsum21@gmail.com*
- *Jameel Ahamd is currently associate professor in Computer Science and Engineering in Integral University, India. E-mail: jameel@iul.ac.in*
- *Shish Ahmad is currently associate professor in Computer Science and Engineering in Integral University, India. E-mail: shishl@iul.ac.in*

2 RELATED WORK

In this section, recent research methodologies developed for the detection and mitigation of DoS attack are discussed. Ashish Kumar Jain and Jyoti Patidar (2018) suggests a system which is based on various parameters like average throughput, packet drop for the entire simulation session for detecting worm-hole nodes. The threshold value of every parameter is compared every time to determine the percentage of loss for every node. Their proposed routing process contains the establishment of the connection between the sender end and the receiver end. These senders send the RREQ message and wait for the reply. Then the source gets the RREP message. Then after establishing the connection, the detection of attack is performed for this some threshold parameters are determined. Round trip time is used to count the number of hop in the communication. Packet drop is also calculated the total number of packet dropping signifies the rate of packet drop. Finally, trust is calculated using the threshold value and assign the trust value to each node. If there is a wormhole attack it shows that the last hop is a malicious node and will stop the communication between those nodes. Eljilani Hmouda and Wei Li (2018) suggests an improvement in EAACK protocol to address the remedy and mitigation of the damage caused by the packet drops, hybrid cryptography that is a mixture of DES and RSA is used for higher malicious detection behavior detection rates and to improve the performance. In their first step, receiver collision occurs; the next step is to limit the transmission power. And the final step consists of reporting the false misbehavior by using a digital signature. Muhammad Salem Khan and Saira Waaris (2018) suggests focusing on the main reasons behind the packet loss in the network. In their research, a study is done to analyze the reason behind packet dropping under various circumstances such as due to high data rate, mobility, number of nodes, network area size, varying queue size and due to different sources. For this OLSD is compared to DSR in ns2 simulator. The results show that the increase in traffic load is the main reason behind packet loss. Vijin Justin and Prof. Nilesh Marathe (2017) suggests a scheme which is a hybrid IDS with SVM classifier for getting the best results in less training time. Signature and anomaly-based method are also used to test the detection performance. Their proposed system consists of a support vector machine and SVM based algorithm. In SVM based algorithm there is a stage on for the training data and stage two for testing the data. The proposed system also contains a packet collection module to capture the data and also a signature based detection engine. Rohit Chourasia, Rajesh Kumar Boghey (2017 IEEE) suggests a scheme which identifies the attacker node in the network. The identification of an attacker is noticed by the dropping of the packets in very large quantity. Prevention is done by choosing the alternate route from the attacker. The designed IDS system also increases the performance of the network. In their proposed system firstly sender wishes to send the data but due to dynamic network, it is not necessary that the neighboring node wants to receive the data so the sender should find the destination source and establish a path between them. It floods RREQ so hop count is evaluated between the sender and the receiver. The malicious node gives a reply that it has the shortest path in order to send the data so the sender would initiate the sending of the data through that shortest path. X value is calculated which is the shortest hop count and also Y value is determined which stores the value of X value. In order to detect the malicious behavior of attacker, the designed system calculates the path length through Xn and Yn which contain the value of X value and Y value respectively. If the difference in the value of Xn and Yn is zero then there is no malicious node whereas if the difference in two values is not equal to zero this indicates the malicious node is present in the network.

3 PROPOSED SYSTEM

Our proposed system methodology has taken place in the given manner shown in figure 3.1. The basic steps that are involved are described using figure 3.1.

Step 1: As we know for the perfect behavior of the network, proper communication should be established between different nodes in MANET

Step 2: For proper communication establishment in MANET the sender sends packets to the receiver.

Step 3: The receiver receives the packet that is sent by the sender.

Step 4: Once the receiver collects the packet from the sender end, it sends the acknowledgment back to the sender of the received packet.

Step 5: Digital signature is generated of every nodes in the network for verification of their authenticity.

Step 6: Once the connection is established and sender starts sending the packet to the receiver, few nodes in the network start to send the packet with high speed which results in the congestion at the receiver end.

Step 7: When the receiver receives the data with such high speed, it checks its buffer memory. If the quantity of packets received at the receiver end is greater than its buffer size, the packet is dropped else it is admitted to the buffer.

Step 8: When there is a packet drop in the network, the receiver sends the choke packet to the sender in order to decrease the transmission speed.

Step 9: The sender receives the choke packet send by the receiver.

Step 10: After receiving the choke packet from the receiver end, if the sender reduces its transmission speed it is considered as non- malicious node or else is treated as a malicious node.

Step 11: That node is marked as a malicious node in the network and is asked for its digital signature to prove its authenticity.

Step 12: If the marked malicious node is able to provide its digital signature then it is considered as an authorized node, if not then it is considered as a malicious node and packets coming from that particular node are dropped in to avoid congestion.

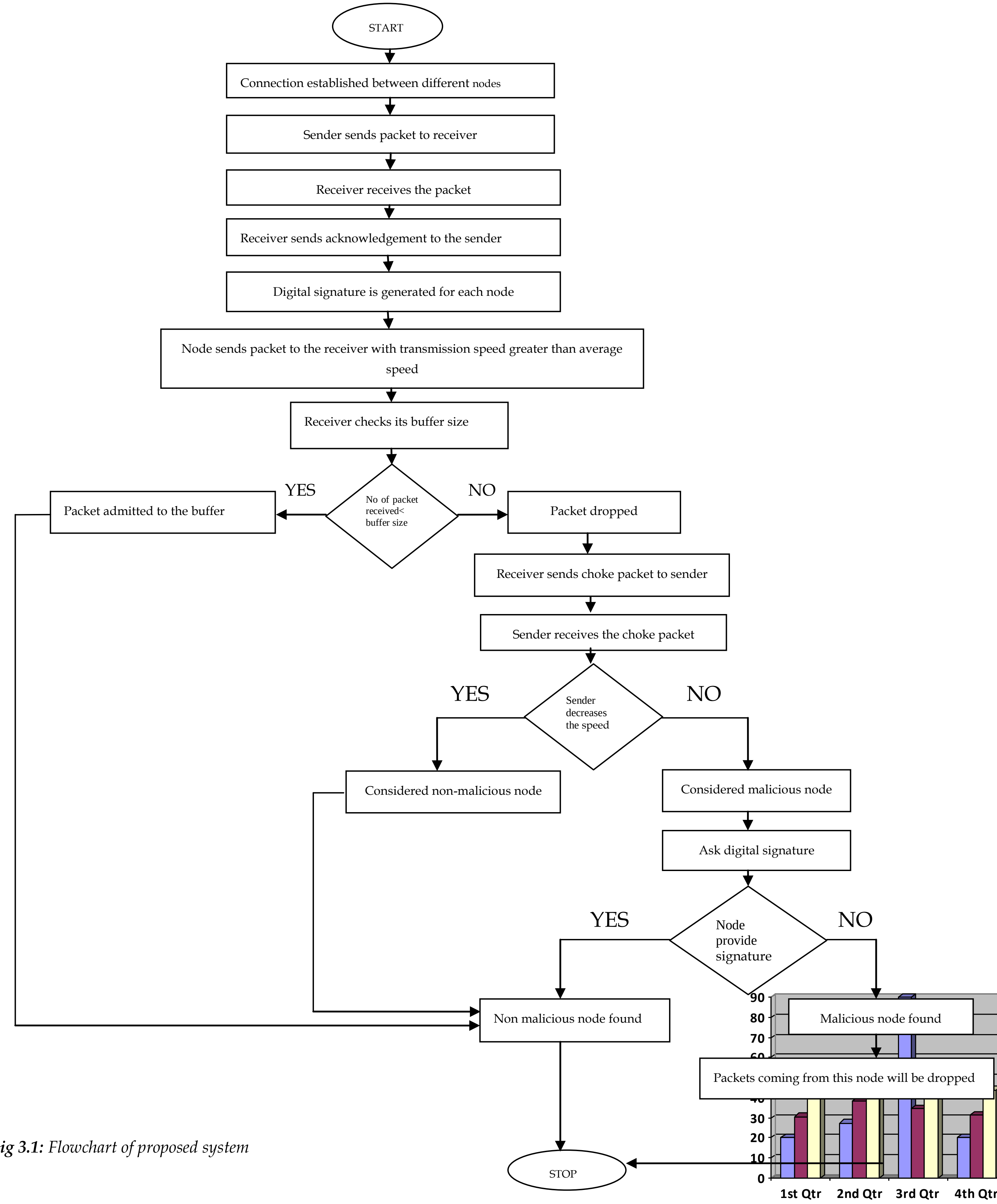

START
Connection established between different nodes
Sender sends packet to receiver
Receiver receives the packet
Receiver sends acknowledgement to the sender
Digital signature is generated for each node
Node sends packet to the receiver with transmission speed greater than average speed
Receiver checks its buffer size
No of packet received< buffer size
YES
NO
Packet admitted to the buffer
Packet dropped
Receiver sends choke packet to sender
Sender receives the choke packet
Sender decreases the speed
YES
NO
Considered non-malicious node
Considered malicious node
Ask digital signature
Node provide signature
YES
NO
Non malicious node found
Malicious node found
Packets coming from this node will be dropped
STOP
90
80
70
60
40
30
20
10
0
1st Qtr
2nd Qtr
3rd Qtr
4th Qtr

Fig 3.1: Flowchart of proposed system

4 RESULTS AND ANALYSIS

The proposed work is simulated on NS-2. NS-2 provides considerable simulation support for the routing, TCP and in multicast protocols. In this operation like traffic analysis, data loss and data signature are modularized.

4.1 Simulation Parameters

Table 4.1 Simulation Parameters

Simulation Parameters	Values
Area of monitoring field	500*50 m2
Routing Protocol	DSR
Simulation time	55 sec
No of nodes	5,50,100,150,200
Maximum Bandwidth	32 bytes
Pause time	5 sec
Maximum speed	32byte/sec

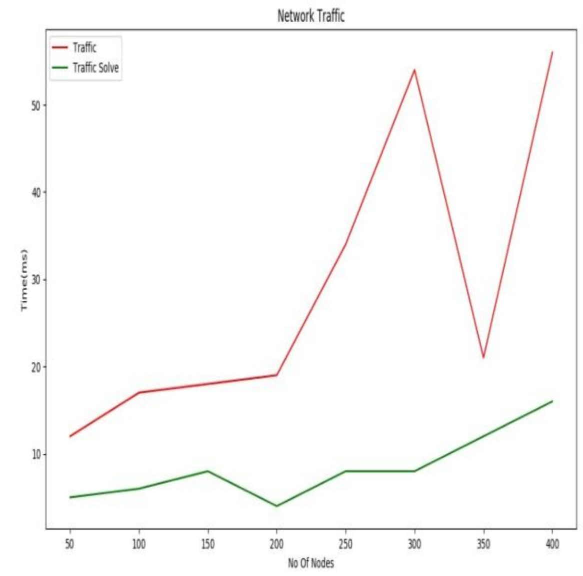
4.2 Traffic Analysis

Traffic analysis is an imperative constraint for recording and analyzing networks for the performance purpose. Figure 4.2 shows the traffic analysis when the sender sends the data to the receiver. The analysis is performed on various numbers of nodes. The above line graph shows the value of the traffic when the sender introduces flooding in the network. The bottom line graph shows the reduction in the traffic after the choke packet technique is applied in the network. The graph is plotted between different number of nodes and the time taken in milliseconds.

Table 4.2 Traffic Analysis

Number of nodes	Traffic nodes	Traffic resolved
50	12	5
100	17	6
150	18	8
200	19	4
250	34	8
300	54	8
350	21	12
400	56	16

Figure 4.2 Traffic Analysis

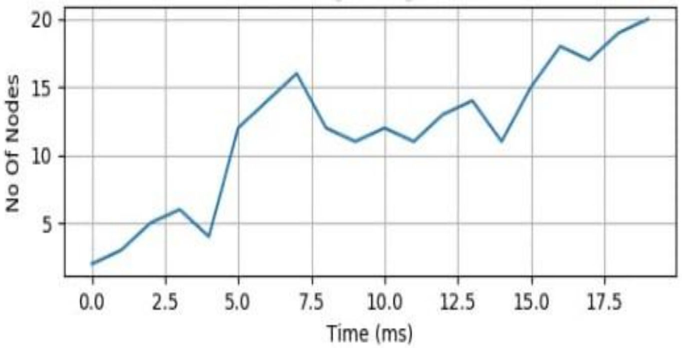


4.3 Digital Signature

Digital signature is a methodology to verify the originality of the sender.

Figure 4.3 shows the reducing in the data when digital signature is applied. The X- axis signifies the time taken by malicious nodes for its verification in milliseconds while Y-axis signifies the number of nodes. The graph shows the verification time taken by the malicious node to demonstrate its authenticity.

Figure 4.3 Digital Signature



4.4 Data Loss

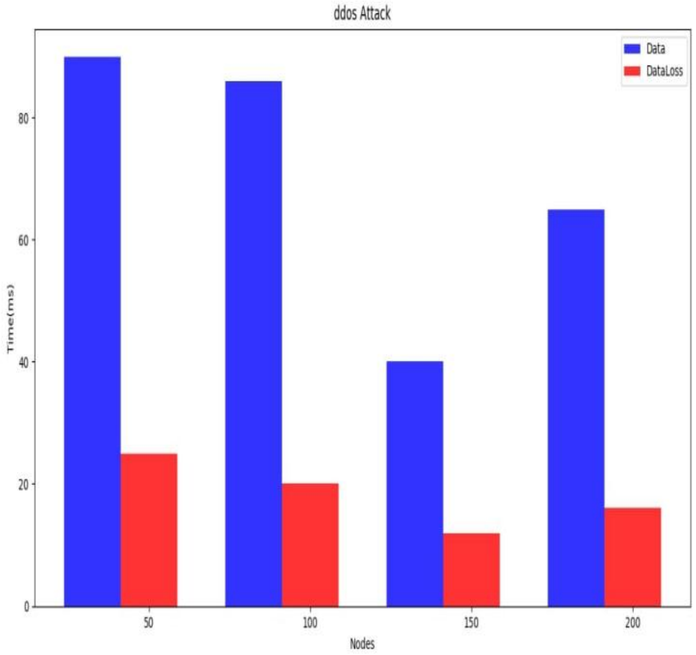
Data loss is a process which results in corruption, deleting of data also making it unavailable to the user.

Fig 4.4 shows the graph resulting in the data loss. An analysis is performed on various numbers of nodes ranging from 50 to 200. The first bar graph shows the numbers of data send by the sender while the second bar graph demonstrates the number of data loss while receiving the data.

Table 4.4 Data Loss

No of nodes	Data send	Data loss
50	90	25
100	86	20
150	40	12
200	65	16

Figure 4.5 Data Loss



5 Conclusion

As the demand and adaptability in MANET are increasing day by day, the chances of threats are also increasing rapidly. This is due to the less secured environment in MANET as compared to the other traditional network. In this paper, DoS attack is focused on the examination and research. In DoS attack, the attacker floods the targeted system by sending messages with high speed. Therefore, we proposed a secure method to detect this attack. From the high rate of transmission of data from the sender and then not reducing it after receiving the choke packet will make a decision for the malicious attacker behaviour. Therefore, the final check by the digital signature which is used for the verification of the authenticity of the malicious node will show the availability of denial of service attack. The simulation is carried out on NS-2.

References

[1] Afroze Ansari, Dr.Mohammed Abdul Waheed, "Flooding Attack Detection and Prevention in MANET Based on Cross-layer Link Quality Assessment", International Conference on Intelligent Computing and Control Systems, 10.1109/ICCONS.2017.8250535, 2017.

[2] Albandari Alsumyt, John Haggerty, "Detect DoS attack using MrDR method in merging two MANETs", 30th International Conference on Advanced Information Networking and Applications Workshop (WAINA), 10.1109/WAINA.2016.113, 2016

[3] Ashish Kumar Jain, Jyoti Patidar. "Detecting Packet Dropping Misbehaving Nodes in MANET Using RTT", Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI), 2018.

[4] Atifa Parveen, Shish Ahmad, "A solution for Detecting Black Hole Attack Using Improved DRI in MANET". SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 10.18090/samriddhi.v6i1.1555, 2015.

[5] Eljilani Hmouda, Wei Li, "Detection and Prevention of Attacks in MANETs by Improving the EAACK Protocol", 10.1109/SECON.2018.8478999, 2018.

[6] Muhammad Salem Khan, Saira Waaris, Idrees Ahmed, Majid Iqbal Khan, "A Comprehensive Analysis of Packet Loss in MANETs", 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering, 10.1109/TrustCom/BigDataSE.201 8.00028, 2018.

[7] Neha Sharma, Anand Singh Bisen, " Detection As Well As Removal Of Black hole And Gray hole Attack In MANET", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 10.1109/ICEEOT.2016.7755409, 2016.

[8] P.Rathiga, Dr.S.Sathappan, "Hybrid Detection of Black hole and Gray hole attacks in MANET", International Conference on Computational Systems and Information Systems for Sustainable Solutions (CSITSS), 10.1109/CSITSS.2016.7779411, 2016.

[9] Pai B. H Karthik, Nagesh H. R., Niranjan N. Chiplunkar.. "Mitigation and performance evaluation Mechanism for Selfish Node Attack in MANETs", International Conference on Computing, Communication, Control and Automation (ICCUBEA), 10.1109/ICCUBEA.2017.8463847, 2017.

[10] Parveen Kakkar, Krishan Saluja, "Performance Investigations of Reactive Routing Protocols under Flooding Attack in MANET", 3rd International Conference on Computing for Sustainable Global Development (INDIACom).

[11] R.Bhuvaneswari, R. Ramachandran, "Prevention of Denial of Service (DoS) Attack in OLSR Protocol Using Fictitious Nodes and ECC Algorithm", 2017 International Conference on Algorithms, Methodology, Models and

Applications in Emerging Technologies(ICAMMAET),10.1109/ICAMMAET.2017.8186625, 2017.

[12] Rohit Chourasia, Rajesh Kumar Boghey, “Novel IDS Security against Attacker Routing Misbehavior of Packet Dropping in MANET”, 2017 7th International Conference on Cloud Computing, Data Science & Engineering Confluence, 10.1109/CONFLUENCE.2017.794 3194, 2017.

[13] Sandeep Dhende, Sandeep Musale, Suresh Shirbahadurkar , Anand Najan, “SAODV: Black Hole and Gray Hole Attack Detection Protocol in MANETs”, International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 10.1109/WiSPNET.2017.8300188, 2017.

[14] Vrince Vimal, Madhav J. Nigam, “Plummeting Flood Based Distributed-DoS Attack to Upsurge Networks Performance in Ad-Hoc networks Using Neighborhood Table Technique”, Proc. of the 2017 IEEE Region 10 Conference (TENCON), Malaysia,10.1109/TENCON.2017.8227851, 2017.

[15] Vijin Justin, Pof. Nilesh Marathe , Nilima Dongre, “Hybrid IDS using SVM classifier for Detecting DoS attack in MANET Application”, International conference on ISMAC, 10.1109/I-SMAC.2017.8058284, 2017.