Node level based DDoS attack Routing Approach in MANET

V. Rajanesh

Assistant Professor, Department of ECE, JNTUH College of Engineering Sultanpur, Telangana, India.

Abstract - Mobile ad hoc network (MANET) allows multiple hosts without a prefixed framework to organize a correspondence. The compact, specifically built device plays an important role in military applications as it is particularly intended to provide a network for physical networking on demand and in situations where it cannot be anticipated. Although it offers great flexibility, the fight against malicious assaults also involves additional difficulties for MANETs. In any case, new plans to define protection procedures are motivated by mobility and excess. This paper propose a procedure to alleviate DDoS attacks against MANETs. Expect a malicious attacker to target certain victims ordinarily. If after a certain length of time, the attacker fails to achieve the desired objectives, the attacker must surrender. This method have made by use of high excesses and choose a safety node in this assurance network. Once a DDoS attack has been identified, suspicious movements are retracted to the protective node. The victim is normally working and the attacker will be able to withstand insignificant efforts. Also this have checked the feasibility of obtained solution and measured the expense and overhead of the system with the aid of increased recreation tests using NS-2.

Keywords: Security, Jamming attack, IDS, Routing, MANET, NS-2, DDoS, PDDoS, PNB-DDoS.

I. INTRODUCTION

All nodes within a mobile ad hoc network are constantly moving to a limited area in a dynamic environment. The MANET was a network which was self-organizing, also nodes can communicate without a fixed infrastructure. Network management for the network operations does not have a centralized authority. The wired network has copper wire for communication, and radio waves are used for the transmission of signal through ad-hoc networks [1]. Two nodes are linked to and used in exceedingly complete form and time for price-efficient setting, as well as for a scenario in which the infrastructure is problematic to set up. Security in MANETs is difficult [2], owing to its features as designers, operational but not central arrangers, complex topology, unsafe organizational configurations and regular connection breaking, due to mobile nodes, battery times, system power and consistency. In MANETs communication was by single hop in protocols for link layers with multihop in protocols for network layers, support the presumption that every node in an extensive network cooperates in coordination, but unfortunately this is not true in an hostile environment. Malicious attacks [2] would actually interrupt the service of the network via violation of the protocol. Outcome and forwarding of the information packet are subject to harmful attacks in MANET network layer operations. Mobile ad hoc systems are less infrastructural and use a wireless network interface to make them unpleasantly vulnerable to ad hoc networks of an adversary. The risks to health and the basic truth of pernicious attacks are over-sized. Attackers in Ad-hoc networks are serious security vulnerabilities that can be exploited without difficulty by misusing flaws in on-demand management agreements such as AODV. In order to avoid attacks by single and multiple nodes, this attempts at using intrusion detection (ID) and hence to detect and repair malpractice under MANET. This solution we seek to achieve by minimizing control packages and efficiently limiting attacks on mobile ad hoc networks [1]. The solution improves network performance.

1.1 types of Attacks in MANET

Various types of attacks occur at intervals on the mobile ad hoc network. Almost all attacks can be classified into two types.

1.2 External attacks

Attackers aim to create congestion in external attack [5], spread redundant routing information or bother services nodes.

1.3 Internal attacks

At an internal attack[4] the person needs to access the network in general by means of any negative pantomime, or even by explicitly manipulating an existing node, or to use the existing node to carry out his malicious behaviour. In intermediate attacks, the person wants to access the device and to use it as a premise. The two groups mentioned above measure external attacks[5] such as common attacks on conventional wired networks in which the person is at intervals, although proximity at network intervals is not yet a reliable node, and therefore this type of attack can also be denied and recognized by security methods, such as membership authentication and firewalls.

1.4 Denial of Service (DOS)

Primary kind of attack was a service denial [6] aimed at reducing the availability of certain nodes or even of services across accidental networks. In order to degrade the processing capacity of the target and make service provided by the target unavailable, the attacks on DOS occur because of a large amount of network traffic flooding inside the

conventional wired network [7]. However, it is not wise to conduct standard DOS attacks [7] due to the quality and the continually dynamic topology of mobile phones.

1.5 Impersonation

The attack by impersons may pose a serious threat to mobile accidental network security [9]. As we can see, the human being will grab certain nodes in the network and make them appear like benign nodes because there is not an effective authentication mechanism between them. Thus, the affected nodes can form a part of the network as normal Nodes and cause malicious conduct, for example spreading fake routing information and gaining inappropriate preference for access.

II. LITERATURE SURVEY

Let's look at several previous researches carried out by different security scientists in this section against jamming attacks and other attacks.

Soneram Verma and Maya Yadav [10] also developed trust-based routes to transmit knowledge in addition to the jamming attack on MANET. In the areas of packet deliveries, end-to - end time, normalized routing loads (NRLs), waste energy and efficiency, the proposed Protocols should be effective.

The aim of this paper is the implementation of secure on-demand routing (TAODV) for data transmission in the field of MANET, based on the motivation of new security measures incorporated in popular AODV routing protocols. The anticipated methods used to alleviate and thwart jamming attacks in the medium-access control layer (MAC) using a number of coordination techniques have been adopted by Pawani Popli and Paru Raj [11]. PCF functions are assimilated to coordinate network behavior of the MAC layer and RTS / CTS (clear-to-send) mechanisms, which are a handshaking tool that dominates wireless network collisions.

Simulation tool is used for simulating the entire network output and technology in this OPNET. Intrusion-Detection System (IDS) is projected by Ashwini Magardey, and Dr Tripti Arjariya[12], which recognizes the attacker by routing information on additional routing nodes. The attacker dumped the entire network output. If the attack occurs on an existing route, the AOMDV multipath routing protocol has provided a multipath.

Attack contagion with performance metrics such as throughput, routing load are assessed also secure anticipated protection technique was restrained to avoid Jamming Attacker routing misconductions and ensure that safe AOMDV routing performance is available as well as usual AOMDV. Krunz et al.[13] suggested a distributed random network that allows nodes with frequency hopping to set up a new control channel. Their approach differs from classic hopping frequencies in which there is no hopping sequence between two nodes to minimizes the effect of node compromise.

In addition, a compromise node can be identified by its hop sequence, which results in it isolation from any future information on the control channel's frequency position. Dorus et al. [14] proposed to use constructive and reactive protocols to avoid jammy attacks on wireless networks to determine the effectiveness of jamming attacks and overhead contact on the wireless networks. For data packet integrity information, RSA algorithm is used during wireless transmission. The implemented mechanism of prevention and integrity protection by simulation and performance review offers a higher packet transmission ratio in the proactive OLSR (proactive routing protocol) than the AODV.

III. PROPOSED SYSTEM

3.1 Protection node selection:

Propelled through conspiracy SAODV, have embrace numerous layout-structures in which nodes have their significance divided into different levels. Lower nodes are used to provide abnormal nodes of state. Each node will in particular be appointed as the safety node at the lower level, named as the Local Protection Node (LPN). They ensure that DoS attacks are carried out. A neighbor with the same level is chosen for the reduced level nodes as his security node.

The malevolent node at the source of the DDoS attack movement can then be tracked with a node.

In our system, the node that is the primary bounce from the source node is also dispersed as a security node when an assault route is made. This type of insurance node is called an Attack source node Remote Protection Node (RPN). The RPN will drop packets from that node, if the source nodes are distinguished as a malicious source node. The RPN will also be deleted from the malicious node from the latest RREQ. It therefore avoids establishing another route for the DoS assault expert.

Every higher node selects its LPN when joining MANETs in our system. The LPN of a secured node should be intermittently updated due to the dynamical system topology. When the LPN node is selected, it is inserted into the route which aims at the assured node. The LPN fills in before the destination node as the last hop, and all packets are sent to the destination node via the LPN. LPN shows the movement whose destination is the security node along these lines.

3.2 DDoS attack Mitigation:

The LPN defense scenario for the DDoS victim node is shown in the figure. 2. The LPN node filters all attacking packets with a traffic destination. The LPN also recognizes the malicious traffic IP addresses and sends the Victim Node with an Attack Notification Message (ANM). ANM includes the IP root of the affected malicious agents. The victim node will then broadcast an AIM packet (Remote Protection Node (RPN). All malicious packets on the source side are filtered by the RPN nodes with AIM information. This implies that the destination node service is retrieved and every other node

from the malicious node is dropped by the RREQ. The malicious nodes can't submit or create a route afterwards.

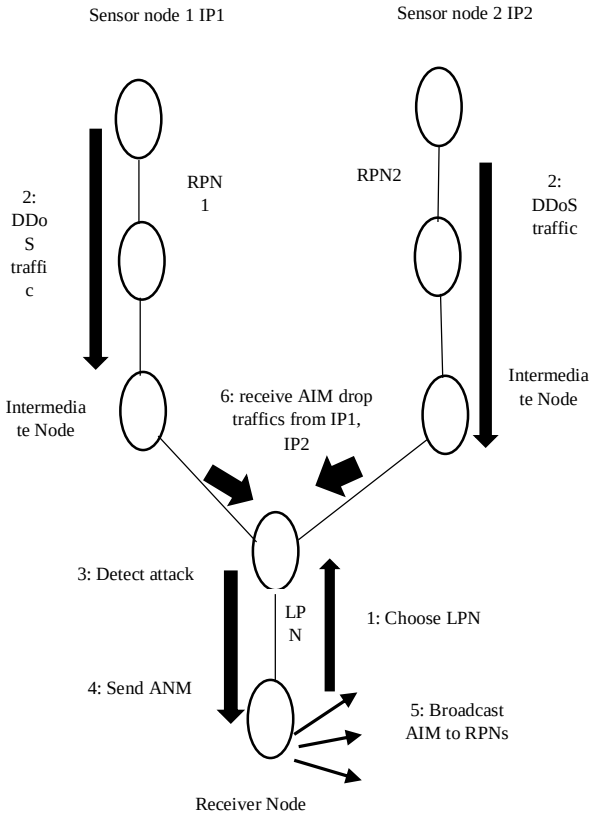

Figure 1. Process of defending DDoS attack

3.3 Local protection node (LPN) selection:

To detect the LPN for a larger quantity node, an advanced three-hand shock approach is adopted. The next lower node in the first step is transmitted with the higher node of the LPN query packet (LPNREQ). Neighboring nodes will unset their new labels, once the demand has been received. At this point, LPNREQ node packets are not recognized.

The recipients send back a verified packet (LPNACK) to the sender in the second step. This LPNACK contact fulfils two requirements: 1) that the sender is told that it will complete the LPN; and 2) that the sender is able to organize the LPNACK messages for a choice. LPNACK packet generator is chosen to produce the principal.

In the fourth stage, an LPN assertion (LPNCFM) message will be sent to the secured node. Besides notifying the LPN node, the LPNCFM message provides other unselected nodes an opportunity to reset their fresh tag, which allows them to be selected with specific nodes. Node-LPN match can be configured after three steps.

Figure 3 shows how a newly selected LPN is inserted to the route when the last hop node is entered. A source node sends RREQs for determining the path and the RREQ label estimate is only set if an RREQ is received by the LPN. INROUTE label is first verified at the point where the safe node receives the RREQ and the RREQ is finally recognized with the given tag. The LPN must not be on its way unless the label esteem is valid. In cases where an intermediate node accepts an RREQ nevertheless the route toward destination node is fresh enough, novel route is always constructed with the old route. Because the LPN is included in the route at the first time, this can ensure that the LPN is included in the route, if the above situation occurs.

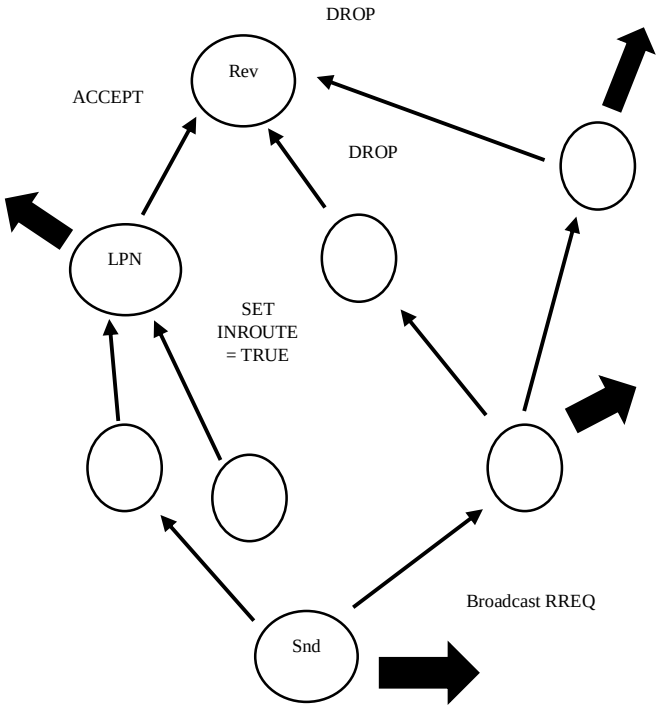

Figure 2: Process of adding LPN to route

This mitigation approach to DDoS attacks was primarily a compensation for redundancy in order to improve system availability. Their approach is based on protection nodes. The false positive alert impacts legitimate traffic throughput while effectively blocking malicious traffic.

IV. EXPERIMENTAL STUDY

The NS-2 simulator is used to perform our experiments. Two steps are required for the experiments. The first step is to test the feasibility of our proposal and then a more in-depth analysis was shown to further assess the cost.

In first step, 25 mobile nodes are located on the network and four nodes simultaneously send traffic to the same destination node. No single traffic rate exceeds a certain threshold, but their total is valid. Another malicious node can send traffic after 600 m seconds to similar destination to check whether protocol is soft to its initial state. It can then react properly to new attacks.

Mobile nodes provide UDP connections, and CBR (Constant Bit Rate) traffic is sent to all channels of communication. Therefore, two nodes that move traffic to the same destination node will not trigger a warner but will trigger three nodes. CBR rate of communication was 512Kb / s and agents threshold was1.5M / s. The field is 1000 m x 500 m in size. Tail drop is the tail drop mechanism. The routing protocol here use is a revised AODV routing protocol which incorporates LPN RPN. The LPN re-select interval is 200 m of seconds.

In step two, let us measure implementation in a different network scale of our new DDoS Attack Mitigation Scheme. The network size arrangements are shown in Table 1. The node traffic applies to our network.

PARAMETER	VALUE
Application Traffic	CBR
Transmission rate	100 packets/sec
Radio range	250m
Packet size	512 bytes
Maximum speed	25m/s
Simulation time	8000ms
Number of nodes	25
Area	1000x500
DDOS nodes	4
Maximum number of packets	10000
Protection node	1
Routing protocol	AODV
Routing Methods	PDO-AODV, BIAS-PDDOS, PNB-DDOS

Table1. Network scale configurations

The study compares our DDoS-based attack mitigation approach to protection nodes to the Bia variance mechanism with original DDoS-based P-AODV protocol. The main aim is to verify the extent of the overhead to alleviate the DDoS attacks. The following are five metrics:

- **Packet propagation delay:** Average time to propagate a packet from the source node to the destination node.
- **Packet drop rate:** In the entire simulation, the packet drop rate.

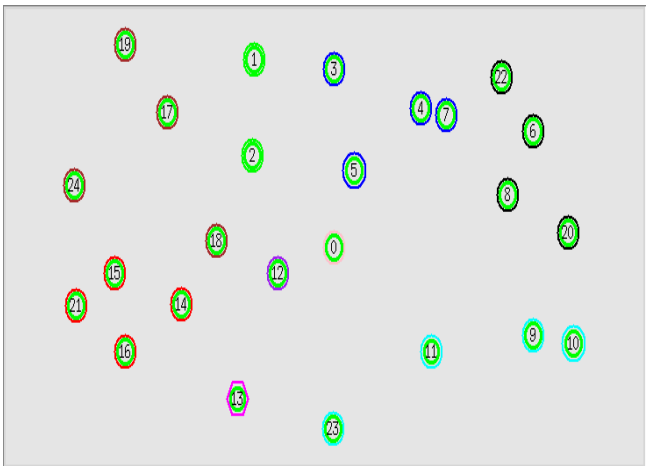

Figure 3: The Topology of Network

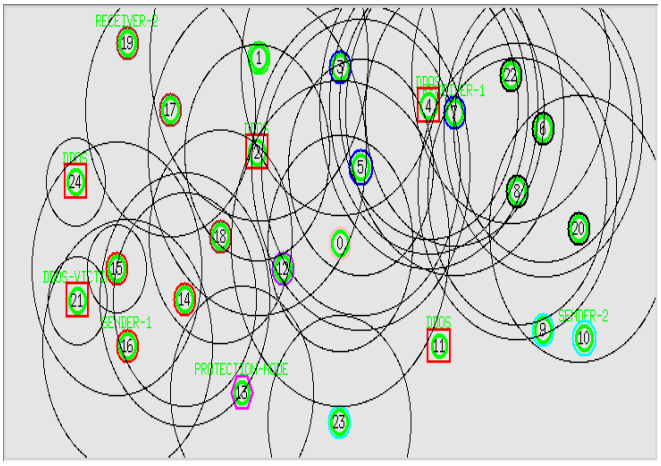

Figure 4: The protective node broadcasts the AIM packet

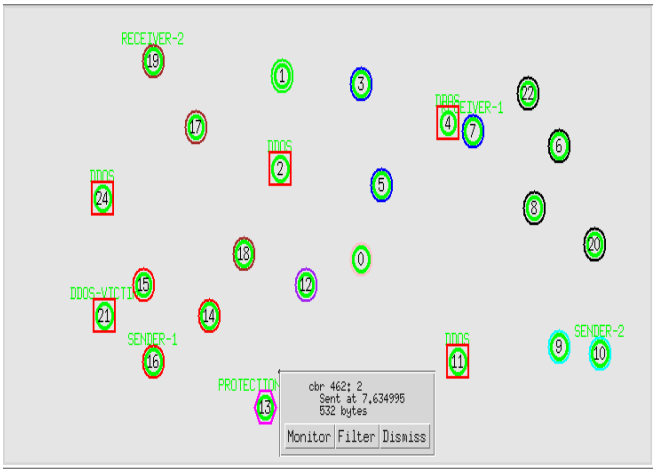

Figure 5: The packets are transferred to the node of protection

- **Energy levels of node:** The power level of nodes per second is used.

- **Network routing load:** Number of additional control packets sent for transmission to a data packet.
- **Network performance:** amount of Megabits measured per sec of transmitted packets

4.1 Result analysis:

Verification of effectiveness:

The first experiment produced 25 nodes randomly and the topology is shown in figure 4. Node 2, node 4, node 11 and node 24 are four traffic attacking nodes marked with a red mark. They all send-off traffic almost simultaneously. The destination of every traffic is Node 21, a high-level node identified as the DDoS victim in the network.

ANM packets are sent by LPN to the victim node that sends Target packets to the entire network as shown in Figure 5. The RPN node filters off the attacking traffic in the vicinity of malicious nodes. All the other nodes register the Malicious ID and delete all nodes sent through the packets. The results of the simulation have shown that our security nodes can mitigate DDoS attacks also allow victim node to usually operate. Figure 6 shows how to work with the simulation as a protection node.

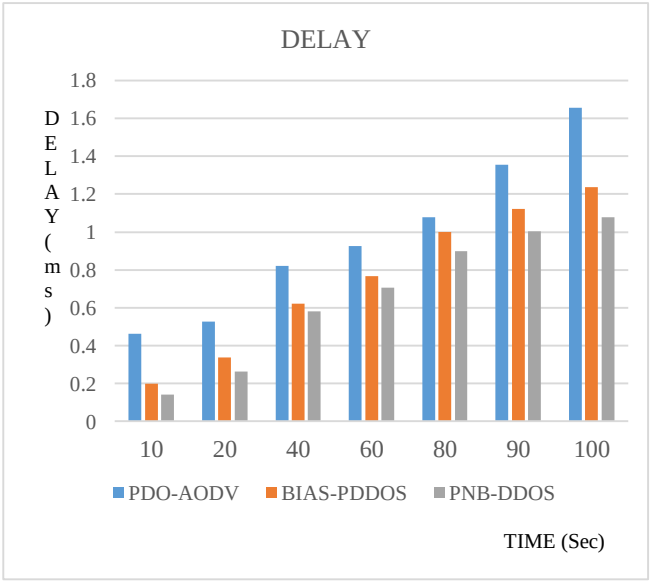

Figure 6: End-to-End Delay

Delay of the network was illustrated in figure 6. The delay in our proposed PDO-AODV system should be low compared to existing BIAS-PDDOS, PNB-DDOS methods in order to achieve a higher network efficiency.

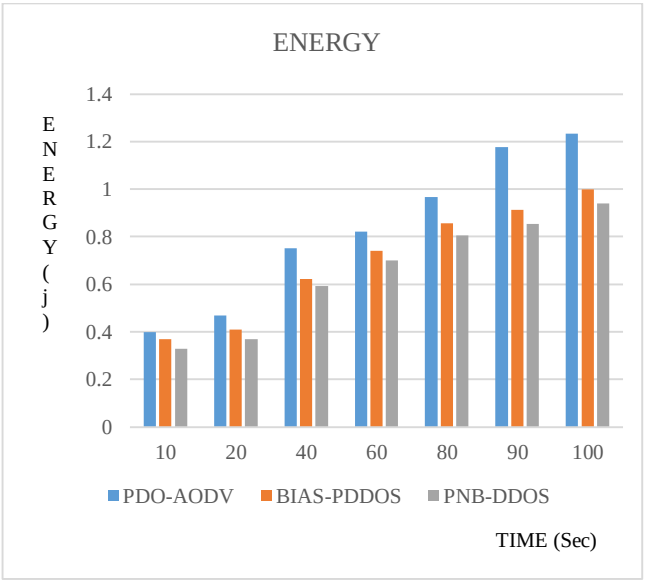

Figure 7: Energy Consumption

The figure 7 indicates the network's energy consumption. The energy consumption in our proposed PDO-AODV system in comparison with existing BIAS-PDDOS, PNB-DDOS, methods should be low for improving the performance of the network.

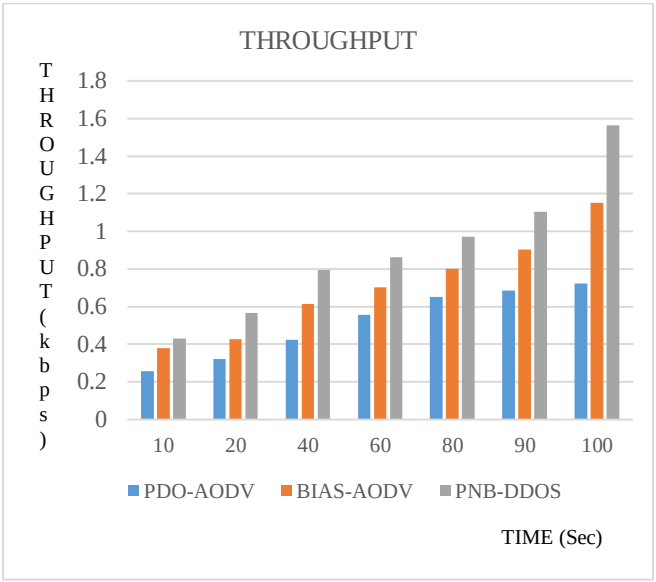

Figure 8: Throughput

It shows the network 's Throughput in figure 8. In comparison of existing BIAS-PDDOS, PNB-DDOS methods, the network performance must be high in our proposed system PDO-AODV.

V. CONCLUSION

This paper presents a new approach to protecting critical nodes against MANET DDoS attacks. Given the various roles that some nodes play on a MANET, some important nodes

are presumed to be higher priority secured. This paper has shown that all features function well and that attacks from the DDoS can be reduced efficiently by means of intensive simulation tests using NS-2. There are small overheads for implementing the DDoS mitigation scheme in addition to the well - known AODV protocol.

VI. REFERENCES

[1] S. Madhavi, "An Intrusion Detection System In Mobile Ad hoc Network", International Journal of Security and Applications, Vol. 2, No. 3, pp. 1-16, July 2008.

[2] V. P. and R. P. Goyal, "MANET: Vulnerabilities Challenges Attacks Application", IJCEM International journal of process Engineering & Management, Vol. 11, pp. 32-37, January 2011.

[3] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "Analyzing the Energy utilization of Security Protocols," Departure on of International conference of Low Power Electronics and Design (ISLPED '03), 2003.

[4] Ouyang, Chengsheng, Antonio Nanni, and Wen F. Chang. "Internal and external sources of sulfate ions in Portland cement mortar: two types of chemical attack." *Cement and Concrete Research* 18, no. 5 (1988): 699-709.

[5] Rozière, Emmanuel, Ahmed Loukili, R. El Hachem, and Frédéric Grondin. "Durability of concrete exposed to leaching and external sulphate attacks." *Cement and Concrete Research* 39, no. 12 (2009): 1188-1198.

[6] Wood, Anthony D., and John A. Stankovic. "Denial of service in sensor networks." *computer* 35, no. 10 (2002): 54-62.

[7] Santhoff, John. "Ultra-wideband communication through a wired network." U.S. Patent 6,782,048, issued August 24, 2004.

[8] Wang, Haining, Danlu Zhang, and Kang G. Shin. "Change-point monitoring for the detection of DoS attacks." *IEEE Transactions on dependable and secure computing* 1, no. 4 (2004): 193-208.

[9] Hussein Mustafa, Xin Zhang, Zhenhua Liu, Wenyuan Xu, Member, IEEE, and Adrian Perrig, "Jamming-Resilient Multipath Routing", IEEE Transactions on Dependable And Secure Computing, Vol. 9, No. 6, pp. 852-863, November/December 2012.

[10] Soneram verma1, Prof. Maya Yadav 2016 "Detection and Prevention for Jamming Attack in MANET using TAODV Protocol", International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 05.

[11] Pawani Popli1, Paru Raj 2016. Mitigation of Jamming Attack in Mobile Ad Hoc Networks", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 6.

[12] Ashwini Magardey, Dr. Tripti Arjariya 2013. Secure Detection and Prevention Scheme for Jamming Attack in MANET, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.

[13] Loukas Lazos, Sisi Liu, and Marwan Krunz "Mitigating Control-Channel Jamming Attacks in Multi-channel Ad Hoc Networks", WiSec'09, March 16–18, 2009, Zurich, Switzerland 2009 ACM 978-1-60558-460.

[14] R. Dorus, P. Vinoth "Mitigation of jamming attacks in wireless network ",Emerging Trends in Computing, Communication and Nanotechnology (ICE-CCN), 2013 International Conference on Date of Conference: 25-26 March 2013.