International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 5 1111– 1115

Imapct of Network layer DoS Attacks on performance of AODV

Er. Nitin Aggarwal
Electronics & communication Department
ISTK, Kurukshetra University Kurukshetra
Haryana, INDIA
nitininworld@gmail.com

Ms. Kanta Dhankar
Computer Science Department
ISTK, Kurukshetra University Kurukshetra
Haryana, INDIA
kanta.dhankhar@gmail.com

Abstract— Mobile Adhoc networks (MANETs) are composed of mobile user equipments that are self-configuring connected through wireless links and without any fixed infrastructure. These networks are dynamic in nature and runs without any centralized authority to maintain all the connections. This characteristic of decentralization makes it susceptible to various attacks. Ad-hoc on Demand Distance Vector (AODV) protocol is mainly used for routing in MANETs. AODV has no inbuilt security mechanism against attacks. This paper evaluates the effect of DoS attacks on AODV protocol's performance. DoS attacks that are implemented for evaluation are Blackhole attack, Grayhole attack and Flooding attack. The evaluation provides us the performance parameters routing overhead and packet delivery fraction calculated over different scenarios.

Keywords- *MANETs, DoS Attacks, Blackhole, Grayhole, Flooding*

*****

1. INTRODUCTION

Wireless mobile networks and devices are becoming increasingly popular as they provide users access to information and communication anytime and anywhere. The term "ad hoc" implies that this network is a network established for a special, often extemporaneous service customized to applications. So, the typical ad hoc network is set up for a limited period of time [1]. Ad-hoc networks works with multihopping. In multihopping path from source to destination traverse many nodes. Basically every transmission relies on cooperation of nodes. Feature of mobility and scalability makes the network more applicable to military and battlefield areas and at the same time this makes it more difficult from security point of view.

Due to mobility of nodes the topology keeps on changing and nodes have to keep a track with newest routing paths. Scalability means that any node can enter or leave a network at any moment. As any node can be added to network, it's always possible that any unauthorized node becomes a part of network and may lead to disturbance or even may lead to destroy the whole communication process. These loopholes allow various types of attacks on network. In this paper, we evaluate the AODV performance in the presence of the three types of attacks mentioned earlier: The Blackhole attack, Grayhole attack and Flooding attack. The evaluation considers the cases for different number of nodes in absence of any attacker and under attack as well. The rest of the paper is organized as follows: in Section 2 the necessary background for this paper is presented. Section 3 discusses attacks. Section 4 deals with simulation environment. Section 5 presents simulation results and Section 6 summarizes the paper and discusses future scope.

2. BACKGROUND

IETF MANET working group was tasked with standardization of routing protocols in MANETs. In order to execute communication within the network, a routing protocol is needed to discover routes between nodes. The primary goal of such an ad-hoc network routing protocol is to find correct and efficient route between mobile nodes so that messages may be delivered in a timely manner. There are several routing protocols designed for wireless ad hoc networks. Routing protocols for ad hoc wireless networks can be classified into three types based on the nature of routing formation mechanism employed. The three types are: Reactive protocols, Proactive protocols, Hybrid protocols. Reactive protocols are also called Demand Driven protocols and Proactive protocols are known as Table Driven protocols. Hybrid routing protocols are combination of both reactive and proactive characteristics.

One of the most commonly used Reactive protocols is AODV. AODV is Adhoc on Demand Distance Vector Routing Protocol. AODV handles discovering, establishing, recovering, and maintaining routing paths. The basic message set consists of – HELLO messages, Route Request (RREQ), Route Reply (RREP) and Route Error (RERR) [2]. There are basically two main phases in AODV: Route Discovery Phase and Route Maintenance phase.

Route discovery by a node involves broadcast of RREQs to all neighbor nodes targeting the destination. RREQ message contains several fields like source and destination IP addresses, source and destination sequence number and unique ID for rejecting duplicate RREQs. RREQs keep getting rebroadcasted until their lifespan is up and waiting for a RREP. Single hop nodes who receive this RREQ rebroadcast the same RREQ to their neighbors. This process is iterated until the RREQ reaches the destination node. As the first RREQ arrives at the destination node, it sends a route reply (RREP) to the source node through the reverse path where the RREQ arrived. If a destination node receives multiple RREQs then the RREQ that arrives later will be ignored by the destination node. AODV also enables intermediate nodes that have sufficiently fresh routes (with destination sequence number equal or greater than the one in the RREQ) to generate and send an RREP to the source node [3].

3. DoS ATTACKS

Denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users. In MANETs attacker node(s) forces victim node(s) not to perform their basic services that's why called Denial of service attacks. It can be launched at different layers. At the physical layer, through signal jamming attack normal communication is disturbed. At the link layer, malicious nodes can capture channel and prevent other nodes from channel access. At the

network layer, DoS attacks are mounted on routing protocols and disrupt the network performance through flooding various types of routing packets. At the transport and application layers, SYN flooding, session hijacking, and malicious programs can cause DoS attacks [4]. In this paper we are going to discuss DoS attacks on Network layer. Three different DoS attacks have been considered and they are explained as follows:-

I. Blackhole Attack

This attack is one of the severe DoS attacks on network layer. It targets the route discovery process in AODV protocol. A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors [5]. An example is shown in fig.1

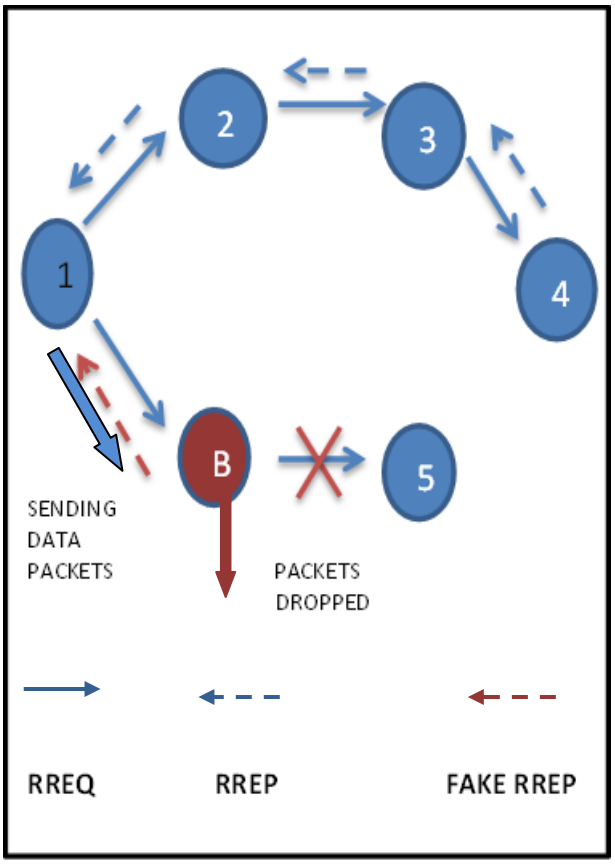

Figure 1.Example of blackhole attack

In this example node 1 is the source node and wants to send packets to node 5 which acts as destination node. Nodes 2, 3 and 5 are intermediate nodes and node B as attacker node. For route discovery node 1 floods the network with RREQ packets. As the RREQ packet reaches the attacker, it instantly responds to RREQ packet. Even though it has no valid route to destination but it sends a false RREP to victim node. In this false RREP packet it sets hopcount 1 and destination sequence number to a maximum value claiming itself the freshest and shortest route. This forged reply makes victim node believe that this is the best path for further transmission and it starts sending packets and then Blackhole node starts dropping those packets and makes that victim node unavailable to its intended users.

II. Grayhole Attack

This attack also targets a node's route discovery process. This attack is executed into two steps. First step is similar to blackhole attack, in which a false RREP is send to victim node claiming to be the node with shortest path to destination. In second step the node drops the intercepted packets with a certain probability. A gray hole may exhibit its malicious behavior in different ways. It may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of Grayhole node may behave maliciously for some time duration by dropping packets but may switch to normal behavior later. A Grayhole may also exhibit a behavior which is a combination of the above two, thereby making its detection even more difficult [6].

III. Hello Flooding Attack

It is a type of active attack in which source node sends large amount of data, Root request (RREQ) and Sync packet to destination node [7]. Flooding attacks are those DoS attacks that work on the plan of flooding a victim node with either data packets or control packets. Hello message is a RREP message with TTL = 1 [8]. Hello packet with following fields:

- Destination IP address
- Destination Sequence Number
- Hop Count
- Lifetime

Destination IP address is the node's IP address, destination Sequence Number is the node's latest sequence number and hop Count is set equal to zero. Lifetime depends on two parameters ALLOWED_HELLO_LOSS and HELLO_INTERVAL. When a node wishes to check connectivity to its neighbors it transmits hello packets. HELLO_INTERVAL is the time interval between hello message transmissions. An attacker node by changing this HELLO_INTERVAL keeps on sending hello packets to neighbor nodes which makes the buffer of victim node overflow and node comes to halt.

Another way of hello flooding is to flood the entire network with hello packets whether a node is neighbor or not. As attacker node not participating in communication, it must have high battery and bandwidth resources. This high power availability makes it easy to send hello messages even to multihop nodes. When these packets reach victim nodes they start sending packets treating it as genuine neighbor but due to power used for transmission can only be used to reach real one hop neighbors, therefore, the packets get lost and never reach this fake malicious node.

4. SIMULATION ENVIRONMENT

This section presents the topology and different parameters used in the simulation process. Simulations were done using NS-2 [9]. NS is a discrete event simulator targeted at networking research. Ns provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks. This simulation process considered a wireless network of twenty four static

nodes which are placed within a 700m x700m area. CBR (constant bit rate) traffic is generated among the nodes. The simulation runs for 100 Seconds. The simulation parameters are shown in Table I

TABLE I. SIMULATION PARAMETERS

Parameter	**Value**
Simulation time	100 Sec
Simulation area	700m x 700m
Antenna	Omni antenna
No. of nodes	24
Packet size	512 Bytes
Max queue length	50
Node movement model	Random waypoint
Traffic	CBR (Constant bit rate)
Routing protocol	AODV
Transport Layer	UDP
Pause time	2 sec
Data Rate	0.75
Bandwidth	2Mbps

The following metrics were used to evaluate the AODV protocol's performance under different scenarios:

Packet delivery fraction (PDF)

PDF can be measured as the ratio of the data packets delivered to the destinations to those generated by the CBR sources. The greater value of packet delivery ratio means the better performance of the protocol. This metric characterizes the packet loss rate, which limits the throughput of the network. It is given by

$$\text{PDF}(\%) = \frac{\sum \textit{Number of packet received}}{\sum \textit{Number of packet sent}} \times 100$$

Routing Overhead

It is defined as the total number of routing packets transmitted over the network, expressed in bits per second or packets per second. Due to scalability, the number of nodes increases in the network. Most routing protocols rely on their neighbors to route traffic and the increase in the number of neighbors causes even more traffic in the network due to multiplication of broadcast traffic. Routing overhead is thus used as a measure how effective a routing protocol is in dealing with these challenges under the constraints of network congestion and low bandwidth.

5. SIMULATION RESULTS AND ANALYSIS

In this section, we will present simulation results in the absence and in the presence of attacks according to the scenarios in Table II

TABLE II SIMULATION SCENARIOS

CASES ⇨ / PARAMETERS ⇩	NORMAL AODV	UNDER BLACKHOLE ATTACK	UNDER GRAYHOLE ATTACK	UNDER HELLO FLOODING
NO. OF ATTACKERS	NIL	1,2,5	1,2,5	1,2,5
SPEED OF NODES(m/s)	5,10 ,20 & 30	5,10,20 & 30	5,10,20 & 30	5,10, 20 & 30

Packet delivery fraction and routing overhead were calculated for AODV and AODV under different DoS attacks for different scenarios. The results are discussed as follows:

Packet Delivery Fraction

PDF decreases in the case of AODV that is subject to an attack. This is due to the fact that the number of correctly received packet is very less than the number of transmitted packets. It is clear from Fig 2-4 that PDF of routing protocol, AODV, is heavily affected by the malicious nodes in presence of blackhole and Grayhole attack as speed of mobile node increases from 5 m/s to 30 m/s. Greyhole node selectively drops data packets so PDF is slightly more than blackhole. In Hello flooding attack, there is slight decrease in PDF due to congestion in the network as attacker does not drop any data packets intentionally.

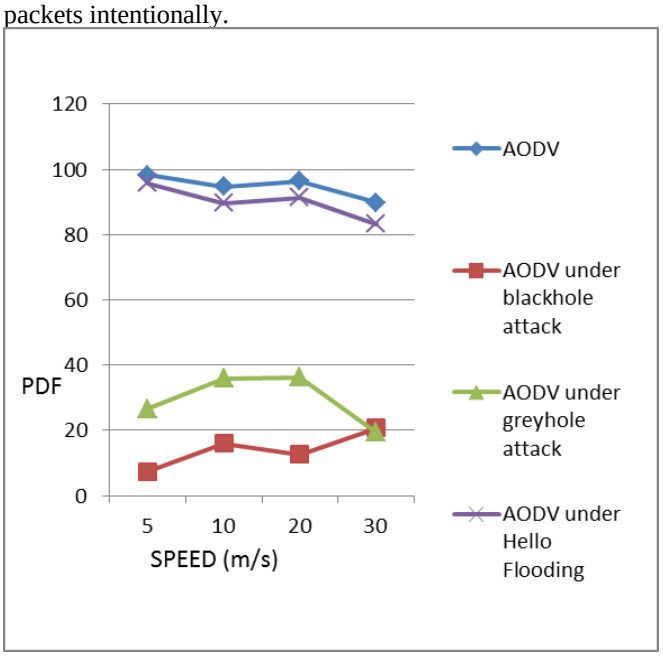

Fig.2 PDF vs. Speed for single attacker

ISSN: 2321-8169
1111– 1115

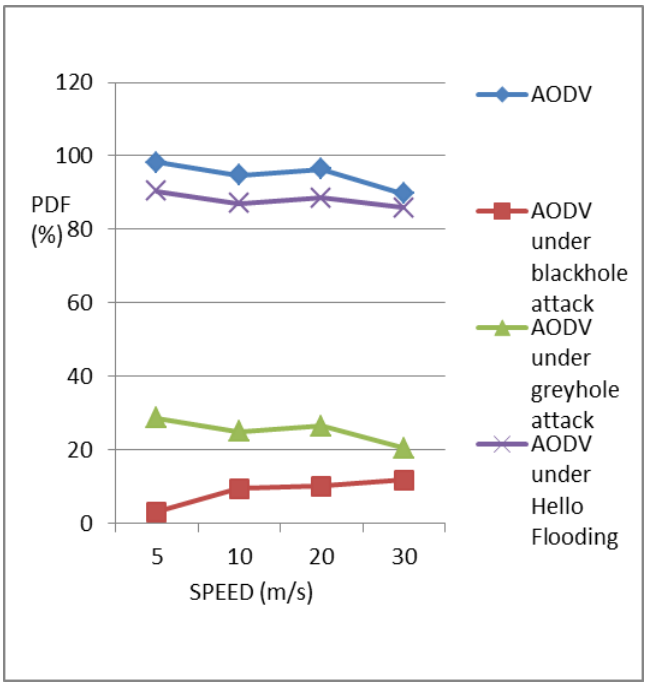

Fig.3 PDF vs. Speed for 2 attackers

With one attacker node, PDF drops from 98.3% of normal AODV to 7.36% in case of blackhole attack, 26.69% in Grayhole attack and 88.56% in presence of flooding node. As malicious node increases to two, PDF drops to 3.07% in presence of blackhole node and 24.69% in presence of Grayhole node. Indeed, with the increase of the attacker nodes, the probability of intrusion increases, and the malicious node absorbs more data packets passing through it. With 20% malicious nodes PDF further drops to 1-2% for packet dropping attacks and 74% for Hello flooding attack.

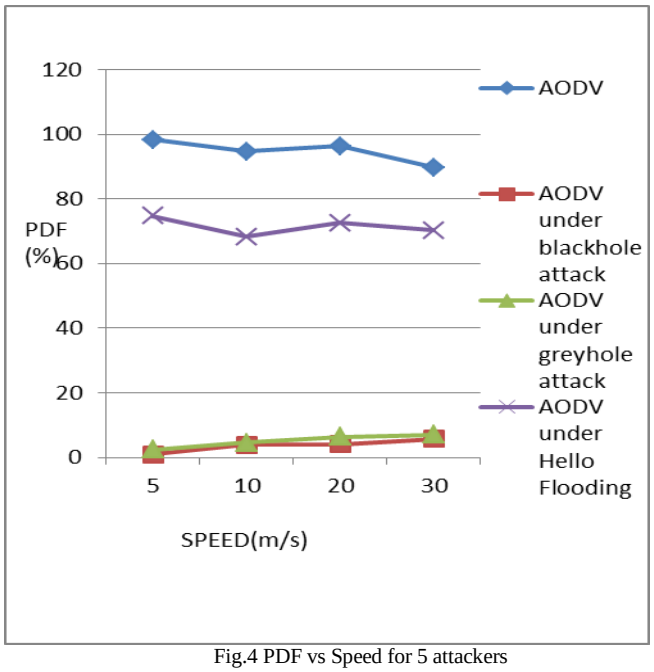

Fig.4 PDF vs Speed for 5 attackers

Routing Overhead

As speed of node increases, routing overhead for AODV increases due to more retransmissions as routing table entries become stale. Whenever node changes its direction or speed, route maintenance occurs. Blackhole and Grayhole attack does not cause much routing overhead as shown in figure 5-7 because attacker nodes immediately sends fake RREP so less route discovery messages are forwarded. In Hello flood attack routing overhead is very high and it increases multifold with increase in number of attacker nodes.

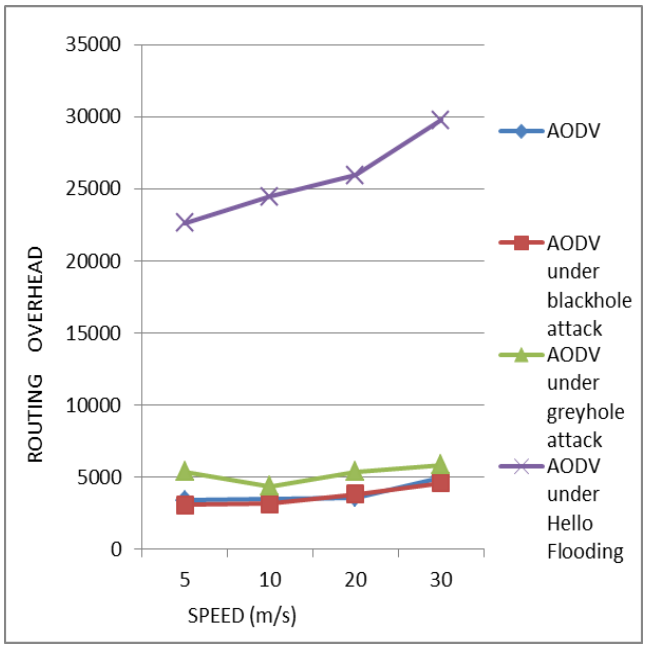

Fig.5. Routing overhead vs. Speed for single attacker

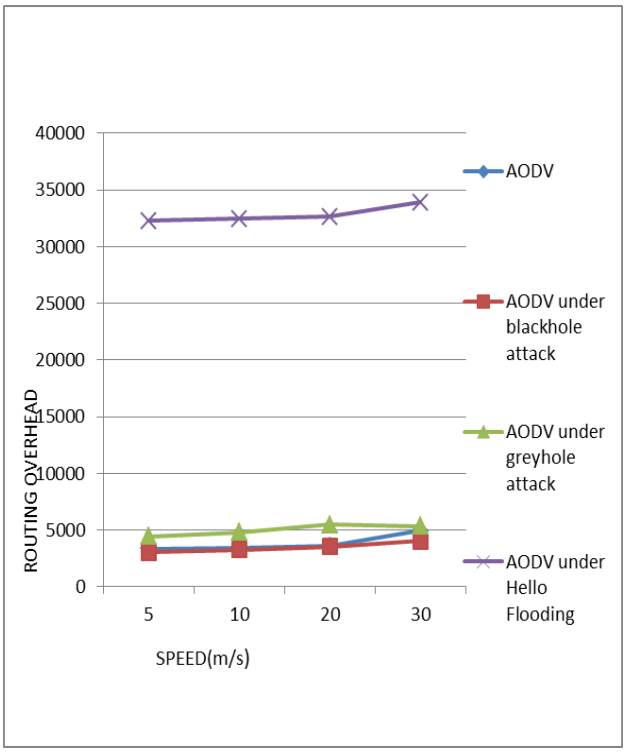

Fig.6. Routing Overhead vs Speed for 2 attackers

ISSN: 2321-8169
1111– 1115

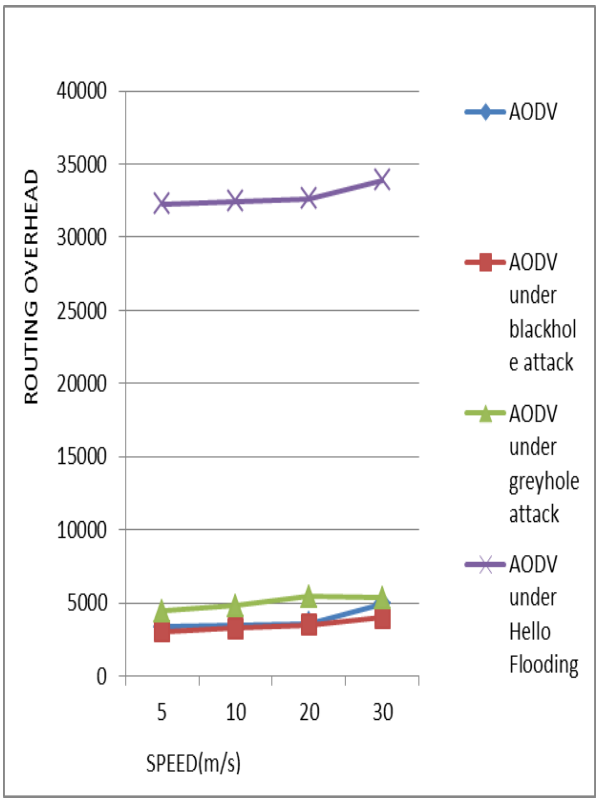

Fig.7. Routing Overhead vs Speed for 5 attackers

6. CONCLUSIONS AND FUTURE WORK

In this paper, network layer DoS attacks were discussed and then performance of AODV was evaluated under these attacks. Blackhole, Grayhole and Hello Flooding attacks were implemented. Performance was explored on Packet delivery fraction and Routing Overhead which were calculated in different scenarios by varying number of malicious nodes and speed of nodes. The simulation results show that presence of malicious nodes will have an adverse effect on the AODV performance. PDF drops to $1/13^{th}$ of its normal non-malicious node value in case of Blackhole attack and $1/3^{rd}$ in Grayhole attack. With increase in speed of nodes and number of attacker nodes, performance decreases sharply. PDF drops to $1/32^{th}$ of its normal non-malicious node value in case of two Blackhole nodes. As hello flood attack affects control packets, routing overhead in case of hello flooding is 5 times more than in normal AODV operation for single malicious node and 8 times for two malicious nodes. For future work, further analysis using other DoS attacks and different metrics can be carried out. Also, techniques for attacks mitigation and detection will be proposed and tested.

REFERENCES

[1] Prasant Mohapatra and Srikanth V. Krishnamurthy, Ad Hoc Networks: Technologies and Protocols, Springer International Edition, 2005.

[2] Tarunpreet Bhatia, Verma,"Performance Evaluation of AODV under Blackhole Attack", International Journal of Computer Network and Information Security" Vol. 12, pp. 35-44,2013

[3] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato, "A Survey Of Routing Attacks In Mobile Ad Hoc Networks," IEEE Wireless Communications, vol. 14, issue 5, pp. 85-91, October 2007.

[4] Nitin Aggarwal, Kanta Dhankhar,"Attacks on Mobile Adhoc Networks: A Survey", International Journal of Research in Advent Technology, Vol.2, No.5,pp 307-316 , 2014.

[5] F.Tseng, L. Chou and H.Chao, "A Survey of Black Hole Attacks in Wireless Mobile Ad Hoc Networks", Journal on Human-Centric Computing and Information Sciences, Springer, Vol.1, No.4, pp. 1-16, 2011.

[6] Sen, Jaydip, M. Girish Chandra, S. G. Harihara, Harish Reddy, and P. Balamuralidhar. "A mechanism for detection of gray hole attack in mobile Ad Hoc networks." In Information, Communications & Signal Processing, 2007 6th International Conference on, pp. 1-5. IEEE, 2007.

[7] Nitin Mohil, Kanta Dhankhar, "Survey of Detection and Prevention Mechanism for Flooding Attacks in MANETs",International Journal of Research in Advent Technology, Vol.2, No.5, May2014.

[8] Lotfy, P. A., and M. A. Azer. "Performance evaluation of AODV under dos attacks." In Wireless and Mobile Networking Conference (WMNC), 2013 6th Joint IFIP, pp. 1-4. IEEE, 2013.

[9] http://www.isi.edu/nsnam/ns/