*International Journal of Research in Advent Technology, Vol.6, No.4, April 2018*
*E-ISSN: 2321-9637*
*Available online at www.ijrat.org*

# DAPS for detecting Wormhole Attacks in IEEE 802.11 networks using Ad hoc On-demand Distance Vector routing protocol

Parminder Kaur Saini[1], Dr. Pankaj Kumar Verma[2], Dr J.S. Sohal[3]
[1]*Research Scholar*
[2]*Associate Professor, Department of Computer Science & Engineering, NIILM University, Kaithal.*
[3] *Director, Ludhiana College of Engineering & Technology, Katani Kalan, Ludhiana.*
*Affiliated to IKG Punjab Technical University, Jalandhar*
***Corresponding author's e-mail address:*** *pparminderksaini@gmail.com*

**Abstract***: IEEE 802.11* [1] is a popular kind of network because its applications cover variety of areas. It is able to run without infrastructure. A number of issues arise due to its unpredictable topology changes [2]. Congestion, Routing and Security are the problems commonly faced in this type of network.Open standard and scattered arrangements are crucial features of IEEE 802.11 network which make it vulnerable to various kinds of attacks [3]. This paper proposes a new detection technique for Wormhole attacks. It is implemented by modifying routing structure of Ad hoc On-demand Distance Vector (AODV) routing protocol [4]. The proposed work is simulated using Network Simulator.

**Index Terms**: Routing Table, Malicious Nodes, Tunnel, NS2.

## 1. INTRODUCTION:

A group of Malicious Nodes [5] launch a Wormhole attack by occupying strong strategic locations in different segments of the Ad hoc network. These nodes occupy major stations in that network and cover entire network to indicate that these nodes are having shortest path for the Destination, even if it doesn't exist. These Malicious Nodes are linked to each other through a Tunnel. At one end of Wormhole Tunnel [6] one node overhears the data packets in its Local Area Network and forwards data to the other node which replays them to another network (i.e. its own Local Area Network, as shown in figure 1).

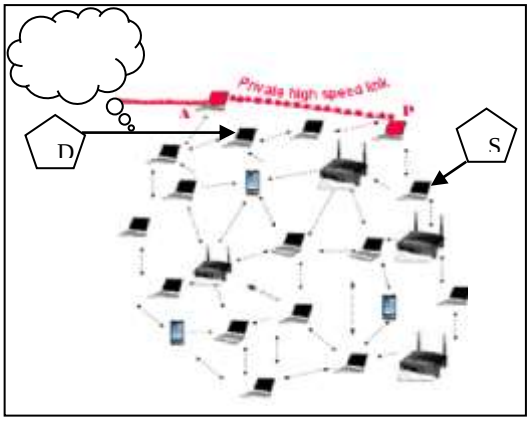


**Figure 1- Wormhole Tunnel.**

Malicious nodes drop the data packets or sometimes transfer those packets to some other network (personal network of those specific nodes) and also modify data packets during transmission. It throws light on the fact as to Mobile Ad hoc Network is prone to Wormhole Attacks. Wormhole attack is a big threat towards speed and security of the network. IEEE 802.11 network can be an important part of security services for secure communications. It is very important to understand the strategy of Malicious nodes to detect Wormhole attack. Thus, it is need of the hour to detect Wormhole attack and Tunnel between the Malicious nodes.

## 2. SIMULATION ENVIRONMENT:

In this work following *Simulation Environment* has been used:

| Parameters | Value of Parameter |
|---|---|
| **Antenna** | Antenna/Omni Antenna |
| **Channel** | Channel/Wireless |
| **Dimension of Topology** | 750*550 |
| **Interface Queue** | Queue/ Droptail/ Pri queue |
| **Link Layer Type** | Link Layer (LL) |
| **MAC** | Mac/802.11 |
| **Malicious Nodes** | 2 |
| **Network Interface** | Phy/Wireless Phy |
| **No. of Nodes** | 10 |
| **NS Version** | NS-allinone-2.35 |
| **Simulation Duration** | 1 to 20 Seconds |

## 3. RESEARCH ON ATTACKING POINTS:

### 3.1. *Route Discovery Process (RDP):*

When a node requests a route from Source node to a particular Destination node, Route Discovery Process [7] starts. Frequently route discovery broadcasts Route Request (RREQ) packets marking the Destination and waits for a Route Reply (RREP). An intermediate node receiving a Route Request packet first sets up a reverse path to the Source node using the previous hop of the Route Request as the next hop on the reverse path.

If a legitimate route to the Destination node is vacant, then the transitional node generates a Route Reply, otherwise the Route Request is broadcasted again. During the RDP copies of the Route Request packet received multiple times are discarded by nodes. When the Destination node receives a Route Request, it also generates a Route Reply and routes it back to the Source node through the reverse path. As the Request Reply proceeds towards the Source node, a Forward Path to the Destination node is established immediately.

A Destination node increments its own Sequence Number either 'before a node initiates a Route Discovery Process' or 'before a destination node initiates a Route Reply in response to a Route Request. The route is only updated in the Routing Table in three conditions i.e. 'if latest Sequence number is greater than the existing Sequence number of Destination node', 'if the fresh Sequence Number is equal but the Hop count is less than the existing Hop count in the Routing Table', or 'fresh Sequence number is unknown'.

During the entire process all the information is updated in a table called Routing Table.

### 3.2 *Routing Table Analysis:*

A Routing Table contains the essential information to forward a data packet to the Destination along the best path. All packets contain information about respective Source and Destination. When a packet is received, a network device scrutinizes the packet and matches it with the Index-ID in the Routing Table providing the best match for its Destination as the Routing Tables contains the updated information of the network for all known Destinations and carry the shortest distance among the nodes. Protocol also maintains fresh lists of Destinations and respective routes by periodically distributing Routing Tables throughout the network. So that when data packets are transferred, an already identified route is used instantly. Once the Routing *Tables* are setup, data is forwarded as fast as in the *Wired networks*. All Internet Protocol (IP) - enabled devices like *Routers* and *Switches* use Routing Tables. Routers and Switches are used to find out that where data packets are roaming over an Internet Protocol. Each node in the network carries a Routing Table. All Routing Tables have the information of all previous routes in the specified network. Routing *Table* of AODV routing protocol is given below:

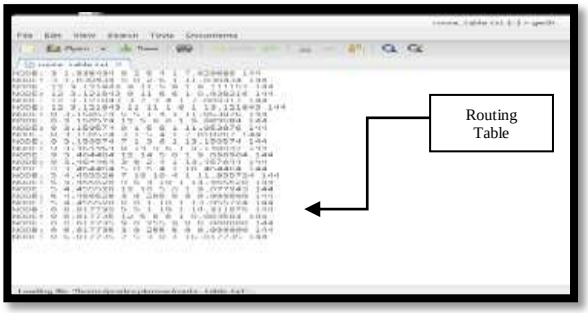


**Figure 2- Routing Table of AODV routing protocol.**

Following information is updated in Routing Table of AODV routing protocol:

- ✓ IP Address of Destination node, Subnet etc.
- ✓ Valid Destination Sequence Number flag,
- ✓ Sequence Number of Destination node.
- ✓ Hop Count Value, (specifying number of hops required to reach destination node),
- ✓ Value of Next Hop,
- ✓ List of Precursors
- ✓ Network Interface,
- ✓ Lifetime (deletion/ expiration time of the route)

All these entries are having further information like:

| Destination Address | Type of Route | Next Hop |
|---|---|---|
| ↓ | ↓ | ↓ |
| Address of Subnet in the network | Connected or Static or RIP or OSPF etc. | IP Address of next Hop in the route. |

A node can also amend the sequence number in the Routing Table entry in three circumstances i.e. 'when the node itself is a Destination node, and offers a new route to itself', 'when it receives an AODV message with new information about the Sequence number for a Destination node' or 'when the path towards the Destination node expires or breaks etc. All this is updated in the Routing Tables immediately. That is the reason a Routing Table plays major role in detecting attack points.

## 4. PROPOSED DETECTION TECHNIQUE:

Routing Table plays an important role in Wormhole Detection, since detail of all the Routing Tables of AODV protocol is stored in the *aodv_rtable.h* file. Thus, to detect Wormhole attack a new function has been designed and implemented. It is declared in the public area in *aodv_rtable.h* file as given below:

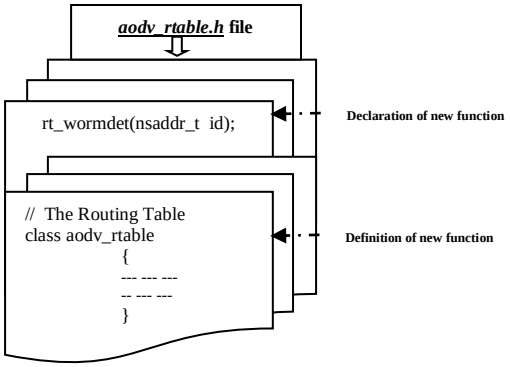


**Figure- 3 rt_wormdet function.**

## 5. RESEARCH DESIGN:

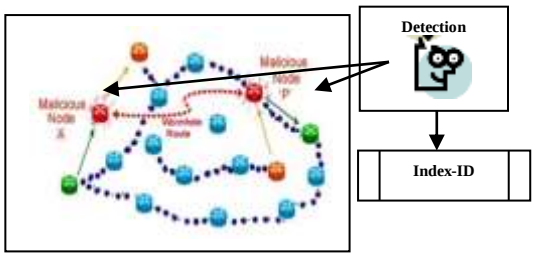


**Figure- 4 Detection of Malicious nodes.**

## 6. DAP ALGORITHM:

Step :1) Begin.

Step: 2) Take an integer variable and look for communication entry in Routing Table.

Step: 3) Assign the value to the variable.

Step: 4) Search for Malicious nodes/Tunnel by using the variable. Check, is Index-id between 'Zero' (for Source node) or 'One' (for Destination node')?

Step: 5) Check again if its 'zero' then display "Source node" otherwise display "Destination node found".

Step: 6) Recheck, if the value is neither 'zero' nor 'one' then display "It is a Malicious node".

Step: 7) On the behalf of 'assigned value' of the variable check all the nodes in the network one by one.

Step:8) End.

### *6.1 Malicious Nodes Detection:*

Following new functions are developed to detect the attacking points like Malicious nodes, Tunnel. **rt_wormdet (nsaddr_t id)** function is developed to detect the Tunnel between Malicious nodes as shown in figure-4.

```
rt_wormdet(nsaddr_t id);

class aodv_rtable
{
public:
.
.
//DAPS
void rt_wormdet(nsaddr_t id);
.
.
}
```

**aodv_rtable.cc** file is also modified and updated as given below:

```
//DAPS
void aodv_rtable::rt_wormdet(nsaddr_t id)
{
aodv_rt_entry *rt = rthead.lh_first;

for(; rt; rt = rt->rt_link.le_next)
{
if(id==0 || id ==1)
{       if(id==0)
        {
        printf("Source=node0 \n");
        }
        else
        {
        printf("Destination= node1 \n");
        }
continue;
}
printf( "Malicious_Node: %d \n", id);
break;
}
}
```

Following function called from file aodv.cc file:

```
//DAPS
        void AODV::rt_resolve(Packet *p)
         {
        if(rt == 0)
                {
                rt = rtable.rt_add(ih-
                >daddr());
                rtable.rt_wormdet(index);
                rtable.rt_wormdet(ih-
                >daddr());
                }
        }
```

Default data failure is handled by NS2 [8] using *callback*. It is carried out by using the following functions:

```
ch->xmit_failure_ = aodv_rt_failed_callback;
ch->xmit_failure_data_ = (void*) this;
```

But when the failure occurs beyond a specified limits then it is considered as an attack and need arises to detect it.

## 7. IMPLEMENTATION OF NEW TECHNIQUE (DETECTING ATTACK POINTS-DAP):

Following new functions are added in the protocol:

```
rtable.rt_wormdet(index);          //DAPS
rtable.rt_wormdet(ih->daddr()); //DAPS
```

These functions check Routing Table of each node to identify the Index-id of Malicious Nodes.

When a Malicious Nodes or attacks are detected, it broadcasts message to other Routing Tables and hence all the other nodes in the network update respective Routing Tables. By implementing this technique all the attacking points are detected successfully.

## 8. RESULTS:

In the following figures performance is captured as:

i. Before Attack (i.e. execution of AODV Base).
ii. After Attack (i.e. execution of DAPS).

### *i) Before Attack (i.e. Execution of AODV Base):*

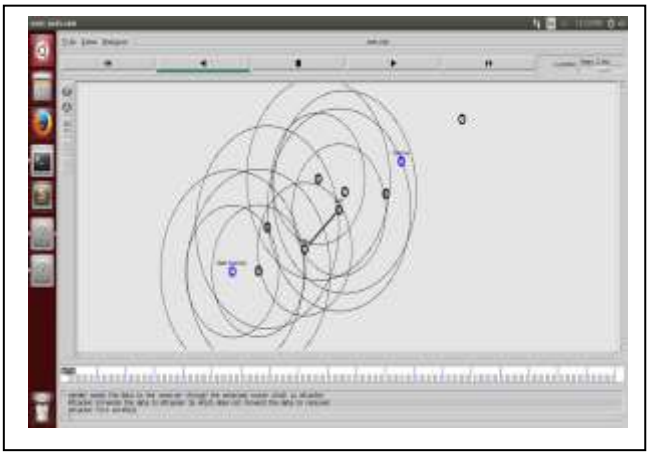

**Figure- 5** Execution of **AODV Base**, Simulation time 20 seconds, 10 nodes scenario.

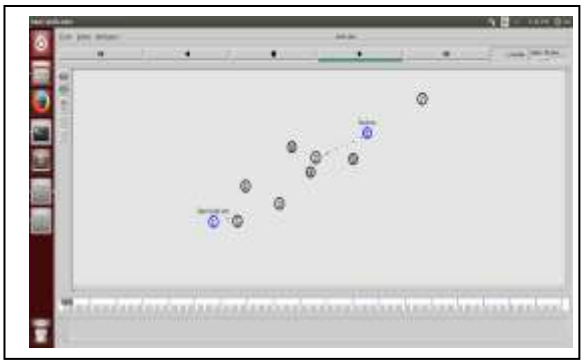

**Figure- 6** Packets forwarded from Source node to Destination node.

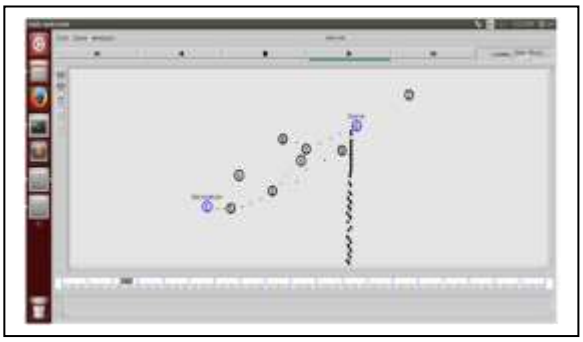

**Figure- 7** During the packet transmission process, some packets have been dropped by default, yet several packets have been forwarded successfully from Source node to Destination node.

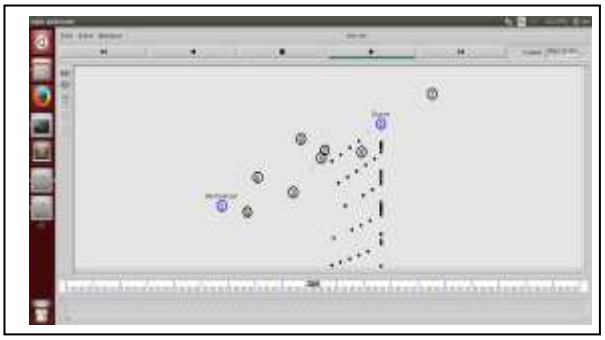

**Figure- 8** In normal scenario, Source node continuously sends data packets to the destination node. By default a few packets are dropped till the last second, yet several packets have been forwarded to destination successfully.

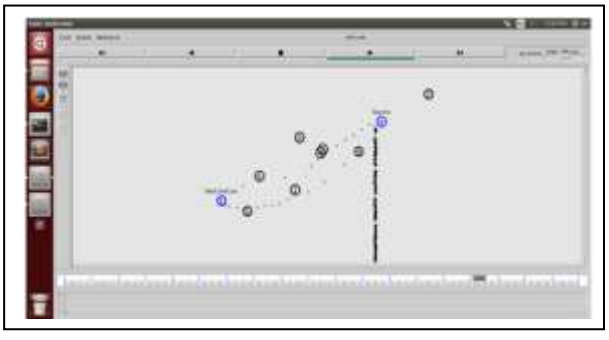

**Figure- 9** It has been continuously observed the packet transmission to the destination is almost the same after 10 seconds, as it was in figure 7.

***ii) After Attack (i.e. Execution of DAPS):***

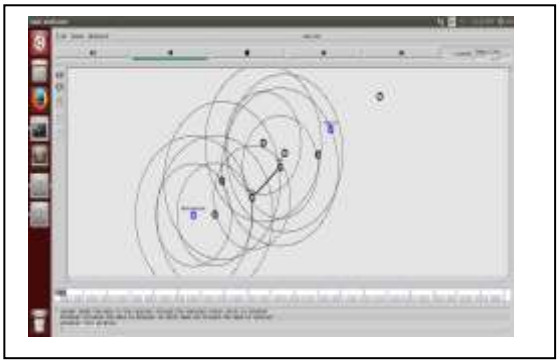

**Figure- 10** Execution of **DAPS**, Simulation time 20 seconds, 10 nodes scenario.

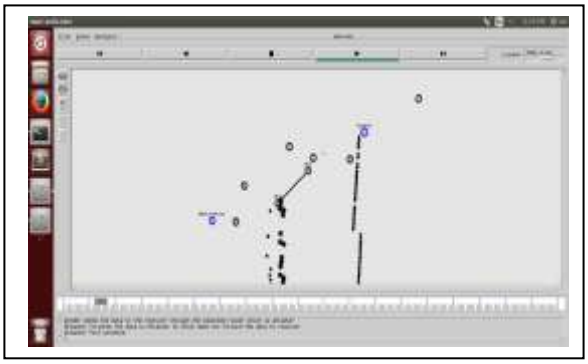

**Figure- 13** Malicious nodes continuously dropping data packets. Various packets dropped through Tunnel and several packets by default.

**Figure- 11** Packets forwarded from Source node to Destination node after implementing DAP.

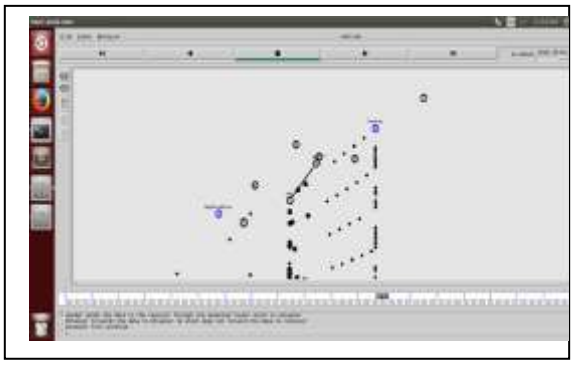

**Figure- 14** This figure shows almost 90% packets have been dropped.

**Figure- 12** Two attacking points i.e. *Node 3* and *Node 4 detected*. A Tunnel has also been created between these attacking points.

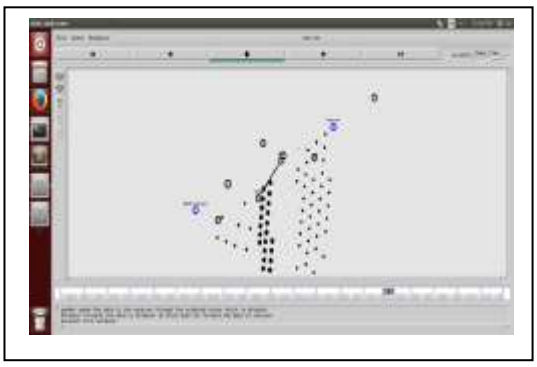

**Figure- 15** It is continuously observed that packets have been dropped after 15 seconds in the same way, as it is captured in figure-14.

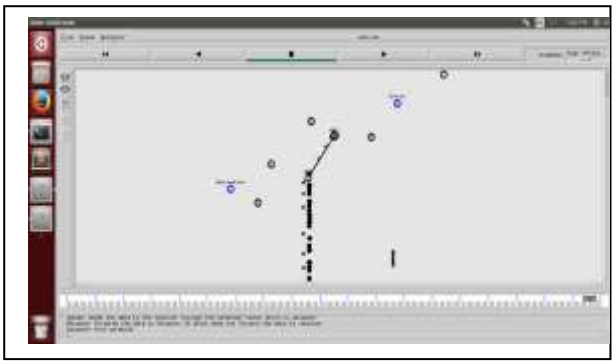

**Figure- 16** Default data dropping may decrease with the time but Malicious nodes are dropping data packets continuously in high speed by making a Tunnel. ***Hardly any packet has been forwarded to the destination***.

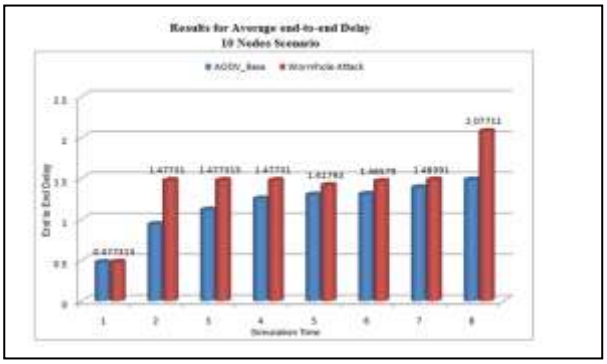


**Figure- 19** Representing comparison between AODV Base and DAP for **End to End Delay.**


**Figure- 17** Representing comparison between *AODV Base* and *DAP* for **Packet Delivery Ratio (PDR).**

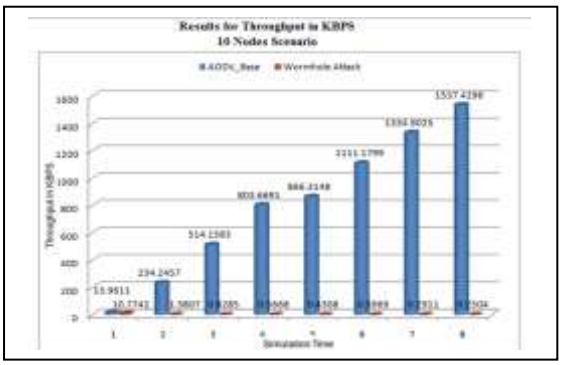


**Figure- 18** Representing comparison between AODV Base and DAP for **Throughput**.

## 9. DISCUSSION:

It is crucial to identify Tunnel between malicious nodes for Wormhole detection. In the new proposed technique, a Tunnel is identified successfully using Routing Table information. To identify Malicious Nodes it first checks the 'Index-ID' in 'Routing Table' to enquire the entry of all available nodes, because as per the genuine procedures, each node in the network carries out its own Routing Table and this rule is also implemented on Malicious Nodes. Malicious Nodes may also have false Routing Tables without having fresh Index-ID of other normal nodes. The Routing Table missing entry is an indication of attack (Malicious node). All the other nodes are checked in the particular network through the respective Index-ID of each node.

When the subsequent nodes cannot find original Index-ID in the Routing Table then it broadcasts message to the Source node indicating that Malicious Node is found in the network and then Source node immediately stops sending data packets through that specific route.

In this work, attacking points (Malicious Nodes) are detected one by one in the network and Tunnel is also detected between the Malicious Nodes by successfully implementing new designed technique *Detecting Attack Points Solution (DAPS).*

## 10. CONCLUSION AND FUTURE SCOPE:

DAP is a very powerful solution for detecting attack points in the IEEE802.11 networks. In this work Wormhole attacks are detected successfully by implementing DAP Solution.

Future scope of this work is to design new techniques for preventing Wormhole attacks in IEEE802.11 networks. Access of important data by Malicious nodes can only be prevented after detecting the faulty nodes which are responsible for Wormhole attacks. New methods can be developed for prevention by utilizing the proposed detection technique i.e. DAP. This technique may also be helpful to develop new security techniques.

## REFERENCES:

[1] IEEE Standards Department. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, IEEE standard 802.11–1997.
[2] Sandeep Sachan et. al., "Wireless Communications Principles and Practice (English) 2nd Edition (Paperback)", Product Id: 90109459.
[3] Parminder Kaur et. al, "A review of Wormhole Attacks for IEEE 802.11 networks", International Journal of Research in Advent Technology, Vol.5, No.8, August 2017, E-ISSN: 2321-9637.
[4] Ning P, et. al., "How to misuse AODV: a case study of insider attacks against Mobile ad-hoc routing protocols", in "Proceedings of the IEEE systems, Man & Cybernetics Society Information Assurance Workshop (IAW)", West Point, New York, USA, 2003. p. 60–7.
[5] Gagandeep et. al., "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", IJEAT, Volume-1, Issue-5, and ISSN: 2249 – 8958, June 2012.
[6] Aashima et. al, "Detection and Prevention of Wormhole Attack in MANET using DSR Protocol", *IOSR* Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. VIII (Nov – Dec. 2014), PP 44-47.
[7] C. Perkins et. al., "Ad hoc On-Demand Distance Vector (AODV) Routing", University of Cincinnati, July 2003, RFC 3561.
[8] Teerawat et. al., Introduction to Network Simulator NS2.