International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 11 | Nov -2016 www.irjet.net p-ISSN: 2395-0072

# Security Solution to Gray Hole Attack in MANET with AODV and DSDV Protocol

**Dr.T.Pandikumar[1], AlemDesalegn[2], Tesfaye Shiferaw[3]**

[1]*Ph.D. Department of Computer & IT, College of Engineering, Defence University, Ethiopia*
[2]*M.Tech. Department of Computer & IT, College of Engineering, Defence University, Ethiopia*
[3]*M.Tech. Department of Computer & IT, College of Engineering, Defence University, Ethiopia*

---

**Abstract -***A wireless mobile Ad-hoc network is infrastructure-less network. Since the nodes communicate with each other, they cooperate by forwarding data packets to the other nodes in the network. Thus the nodes find a path to the destination node using routing protocols.*
*Due to the infrastructure-less nature and decentralized networks, wireless Ad-hoc networks are unprotected and vulnerable to the attack. Gray-hole attack is one of the most common and harmful attack in MANET. So avoidance for gray-hole attack will implement with routing protocols namely AODV and DSDV. The performance of these protocols will compare without gray-hole attack, with gray-hole attack and after avoidance of gray-hole attack. Performance metrics are throughput and packet delivery ratio is use.NS2 is chosen as a simulation environment because it is one of the leading environments for network modeling and simulation.*

***Key Words***:MANET, Gray Hole attack, IDS, AODV, DSDV, NS2

## 1. INTRODUCTION

Mobile ad hoc network (MANET) is infrastructure-less network. It consists of a collection of wireless mobile nodes (like mobile or a laptop) that are capable of communicating with each other. Nodes communicate with each other with the help of intermediate nodes; they provide communication by forwarding packets between them. To support this communication, nodes use routing protocols namely AODV and DSDV. Ad-hoc On-Demand Distance Vector (AODV) and Destination-Sequenced Distance Vector (DSDV) Routing Protocols are used for finding a path to the destination in an ad-hoc network. Each node acts as a host and as a router to find a path and forward packets to the correct node in the network. In this way, ad-hoc networks have a dynamic topology there for nodes are free to move independently, nodes can join or leave the network whenever needed. MANET has some attractive features like dynamic topology, battery powered, and multi-hop communication. Mobile ad hoc network use for applications especially in military and rescue operations such as connecting soldiers in the battle or emergency services such as establishing a temporary network in place of one which collapsed after a disaster like an earthquake and uses vehicle to vehicle communication.

Although Mobile ad hoc network is a very flexible and popular technology, still it is more vulnerable to many attacks as compared to wired network or infrastructure based wireless network due to the lack of centralized management. Attacks can destroy or disturb the normal functionality of the network and security goals such as confidentiality, authentication, integrity, availability and non-repudiation. There are different types of attacks present in mobile ad-hoc network, active and passive attacks. In passive attack, it does not destroy or disturb network but uses the useful information. But in the case of active attack, it steal, destroy, manipulate the useful information and as well as disturb the operations of network.

### 1.1 Statement of the problem

Security is important concern in all kind of network. Mobile ad-hoc networks are highly vulnerable to security attacks as compared to other wired networks. This is due to the following characteristics: insecure operating environment, physical vulnerability, shared broadcast radio channel, lack of central authority. Malicious node act as an obstacle in the secure path As it will absorb the data and thus reduce packet delivery , degrade the performance, Decrease end to end delivery, decrease throughput. In our study, gray-hole attack is involved in MANET based on AODV and DSDV routing protocols. To secure a network avoiding this attack is very important task.

## 2. MOBILE AD HOC NETWORK

This type of network, infrastructure-less network, is known as Mobile Ad Network (MANET). Mobile ad hoc network is an autonomous system, where nodes/stations are connected with each other through wireless links. There is no restriction on the nodes to join or leave the network, therefore the nodes join or leave freely. Mobile ad hoc network topology is dynamic that can change rapidly because the nodes move freely and can organize

themselves randomly. This property of the nodes makes the mobile ad hoc networks unpredictable from the point of view of scalability and topology.

When a node wants to communicate with another node, the destination node must lies within the radio range of the source node that wants to initiate the communication. The intermediate nodes within the network aids in routing the packets for the source node to the destination node. These networks are fully self organized, having the capability to work anywhere without any infrastructure. Nodes are autonomous and play the role of router and host at the same time. MANET is self-governing, where there is no centralized control and the communication is carried out with blind mutual trust amongst the nodes on each other. The network can be set up anywhere without any geographical restrictions. The general properties of MANETs are listed below.

**Dynamic Topologies:** Since nodes are free to move arbitrarily, the network topology may change randomly and rapidly at unpredictable times.

**Bandwidth constrained, variable capacity links:** Wireless links have significantly lower capacity than their hardwired counterparts. Also, due to multiple access, fading, noise, and interference conditions etc. the wireless links have low throughput.

**Energy constrained operation:** Some or all of the nodes in a MANET may rely on batteries. In this scenario, the most important system design criteria for optimization may be energy conservation.

**Limited physical security:** Mobile networks are generally more prone to physical security threats than are fixed cable networks. There is increased possibility of eavesdropping, spoofing and denial-of-service attacks in these networks.

Irjet Template sample paragraph .Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

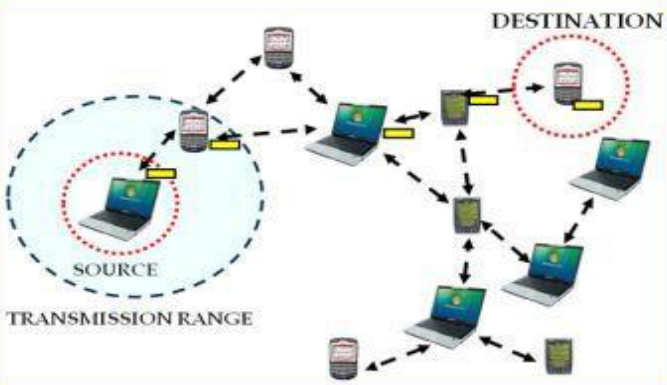


Figure 1: Mobile Ad hoc Network

### 2.1 Mobile Ad hoc Network routing protocols

Routing data through a wireless mobile ad hoc network (MANET) is more complex than routing data through a fixed infrastructure based network. The changing topology of MANET requires that the routing protocol be able to manage and adapt the routes in real time. The limited resources of the mobile nodes, both in terms of battery power and network bandwidth, require the routing protocol to be efficient. MANET routing protocols can be categorized into three types: proactive (table-driven), reactive (demand-driven) and hybrid.

### 2.2 Proactive Routing Protocols

In proactive protocol, every node in a network maintains one or more routing tables that are updated regularly. Every node sends a broadcast message to the entire network if there is a change in the network topology. But, it incurs additional overhead cost due to maintaining up to-date information and as a result, throughput of the network may be affected but it provides the actual information to the availability of the network. Destination-Sequence Distance-Vector (DSDV) and Optimized Link State Routing (OLSR) are proactive protocols.

### 2.3 Ad Hoc On-Demand Distance Vector (AODV)

The AODV routing protocol is designed for ad-hoc mobile networks and it can handle unicast routing and as well as multicast routing. This protocol has the advantageous features of both DSR and DSDV algorithms and this protocol is an example of On-demand routing protocol which means the routes will be created only when there is a demand and also it maintains the routes only as long as they are needed. Creating and maintaining the routes in the network only when they are needed/demand makes this AODV protocol very useful and also a good algorithm for mobile ad hoc networks (MANET).

### 2.4Working of AODV

All the nodes in the network have routing tables of their own and they also maintain sequence numbers in order to avoid looping problems. If a source node wants to send some data to a destination node and if it doesn't have a route to the destination at that time then the source node broadcasts a route request (RREQ) packet throughout the network. The structure of the RREQ contains as below.

1. Source address
2. Source Sequence number
3. Destination address
4. Destination sequence number
5. Hop count

The nodes will reply with a RREP if either the destination node or the intermediate node which is on the way to find the destination node and the structure of RREP format is as follows.

1. Destination address

2. Destination sequence number

3. Source address

4. Lifetime

In detail a node which receives the RREQ will send a reply (RREP) only if it is either the destination or if it is a path/route to the destination with a corresponding sequence number and only when that number is greater than or equal to the number which contains the RREQ. In cases like this the nodes will unicasts a RREP to the source, otherwise; the nodes will rebroadcast the RREQ. The nodes will discard the RREQ and do not forward them if they have been processed those already. And the RREP will set up forward pointers to the destination by propagating back to the source nodes. When the source node receives the RREP, it records the latest sequence number to the requested destination and this process is called as Forward Path setup.

The intermediate nodes that receives another RREP after they had propagated the previous RREP towards the source, it then checks and compares the new destination sequence number of the new RREP with the previous RREP. These intermediate nodes updates their routing information and propagates a new RREP only when,

1. The destination sequence number is greater or

2. The new sequence number is same but the hop count is small or

It will just skip the new RREP. This process ensures that this algorithm is not making any loops and only the most effective is chosen. If the data packets keep travelling from one node to another node along a certain path only then the route remains active otherwise the links will timeout and then be deleted from the routing tables of the intermediate nodes. In situations like where the links break while the route is being active then the node upstream of the link break generates a route error (RERR) to the source node to inform that it is not reachable to the destination(s). After the source node receives this (RERR) message, then even if the source node still needs the route then it will reinitiate the route discovery to that destination.

### 2.5 Destination-Sequenced Distance Vector (DSDV) Protocol

This is a proactive routing protocol which is based on Bellman-Ford routing algorithm. A routing table is maintained at each node in the network and with the help of this routing table, transmission of packets is done from one node to another node in the network. The improvement that has been made to Bellman-Ford routing algorithm is that in this, sequence numbers are used in this instead of loops in routing tables and this sequence number is originated by the destination node.

The consistency is maintained by and when each node transmits and updates its routing table periodically. If the packets are broadcasted between nodes then it indicates that those nodes are accessible and how many hops are required to reach that particular node. These packets may be transmitted and containing the layer 2 or layer 3 address. All the nodes advertise its own route tables to all of its neighbors in the network and this is the requirement of the DSDV routing protocol. As the entries of the routing tables change frequently, the advertisement should also be frequently updated so that all the nodes in the network have the information about all of their neighbors in the network. The purpose of doing this is to make sure that the paths to reach a destination will have the number of hops for the routes, so that through this way even there is no direct connection from one node to another they can still communicate and exchange data.

As we have said earlier that each node transmits data and that data consists of new sequence number and the following information for each new route:

1. Destination address

2. Number of hops required to reach the destination and

3. The new sequence number originally stamped by the destination

The routing tables that are transmitted contain the information about the hardware address, network address of the host. The latest sequence number is preferred as the basis for making the forwarding decision of the data in the network between the hosts. In the cases like if the sequence numbers are the same then the one with better metrics is preferred. Even the sequence numbers are updated to all hosts in the network so that the nodes will decide on maintaining the routing entry for that originating mobile node. As soon as the route information is received, the receiving node increments the metric and transmits the information by broadcasting and this incrementing process is done only after the transmission because, even the incoming packet has to travel one more hop to reach its destination.

The mobile node(s) can cause broken links as they are mobile and these will be detected at the layer 2 protocols, which can be described as infinity. Whenever there is a broken route in the network, then that metric is assigned an infinity metric there by confirming that there is no hop and the sequence number are also updated. The sequence numbers are defined to be even numbers and the infinity metrics are defined as odd numbers.

In DSDV protocol, the broadcasting of information can be done in two types namely: full dump and incremental dump. Full dump broadcasting carries all the routing information while incremental dump carry the information which has changed since the last full dump. Broadcasting is done in Network protocol data units (NPDU). A full dump requires multiple NPDU's while the incremental dump requires only one NPDU to fit in all the required information. Whenever a node enters into the network, then it will announce itself and the other nodes in the network update their routing information about that node as a new entry in their routing tables. Each mobile node advertises about reachability, information about layer 3 protocols at that destination.

## 3. METHODOLOGY AND IMPLEMENTATION

In this chapter, we present and explain the implementation and the methodology which we followed in this research. We organize this chapter into four main sections. The selected network simulator is listed in Section 3.1, section 3.2 contains the implementation of new AODV and DSDV routing protocols in the network simulator.

### 3.1 Simulation Tool

All simulations have been carried out using the NS simulator program version 2.35 under Ubuntu operating system. NS2 is a discrete-event driven object-oriented network simulator and it is open source simulator software used by a lot of institutes and researchers. The main goal of the NS2 simulator is to provide support to education and research in networking. NS2 has been written in two languages, Object oriented variant of Tool Command Language (OTCL) and object oriented language C++. While the C++ defined the internal mechanism (backend) of the simulation objects, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events (frontend). NS2 creates two main analysis reports simultaneously. One is NAM (Network Animator) object that shows the visual animation of the simulation. The other is the trace object that consists of the behavior of all objects in the simulation. Former is .nam file used by NAM software that comes along with NS. Latter is a ".tr" file that includes all simulation traces in the text format. In this paper we analyze the two most common MANET protocols AODV and DSDV under normal operation, with gray-hole attack and under security solutions by varying speed of nodes.

### 3.2 Gray-hole Attack

In a Mobile Ad-hoc Network that uses AODV and DSDV protocols one attacker node can drop some selected packets according to some criteria or randomly. This is called gray-hole attack or selective drop attack. This type of attack is very difficult to detect, especially in the wireless scenario, because packets can be dropped because of line congestion, channel capacity, etc. In the simulation we used random dropping of packets using the random function. While the packets are sending to destination, packets are dropped randomly by the malicious node. Simulation of gray hole-attack is done on ns-2.35. In order to simulate gray-hole attack on ns2 we have to modify and implement the existing AODV and DSDV protocol.

## 4. IMPLEMENTING NEW AODV PROTOCOL

To implement the new AODV routing protocol, we start by duplicating the AODV protocols in this directory and named the directory as "grayholeaodv" (all the header files and classes of AODV directory are modified). All the files in the AODV directory are modified with grayholeaodv such as *grayholeaodv.cc*, *grayholeaodv.h*, *grayholeaodvrqueue.cc*,*grayholeaodvrqueue.h*etc except for *"aodvpacket.h*. The new protocol will use the same AODV packets and thus it's possible for the new grayholeaodv protocol to send the same AODV packets. So we have changed all the names of classes, structures, functions in all the files except for the struct names that belong to the AODV *packet.h*code. By creating all this we have designed aodv and grayholeaodv protocols to send packets with each other. To integrate the grayholeaodv protocol to the NS2, two common files has to be modified. Since we are using the same packets used in AODV, we don't have to modify the common files related to packet. Thus had to modify two files.

The first modified file is the *ns-lib.tcl*. It's in this file the protocol agents are coded in a procedure. So here we had to add the protocol agent for the newly created grayholeaodv protocol. When a node is using grayholeaodv protocol this agent is scheduled at the beginning of the simulation and is assigned to the nodes which use the protocol.

```
grayholeaodv {
setragent [$self create-grayholeaodv-agent $node]
}
#grayholeaodv patch
Simulator instproc create-grayholeaodv-agent { node } {
setragent [new Agent/grayholeAODV [$node node-addr]]
$self at 0.0 "$ragent start"                ; # start
BEACON/HELLO Messages
$node set ragent_ $ragent
return $ragent
}
```

Figure 2: *ns-lib.tcl*grayholeaodvmodifiation

The next file to be modified is the *ns-agent.tcl*. In this we have to set the port numbers for the new routing protocol. *sport*is the source port and *dport*is the destination port.

```
#grayholeaodv patch
Agent/grayholeAODVinstprocinitargs {
        $self next $args
}
Agent/grayholeAODV set sport_   0
Agent/grayholeAODV set dport_   0
```

Figure 3: *ns-agent.tcl*grayholeaodv modification

The third file modified is the *makefile.in* in the root directory of ns-2.35. This file is modified for creating the object files for the c++ coded files. After all the implementations are ready, we have to recompile NS-2 again to create the object files.

```
grayholeaodv/grayholeaodv_logs.ograyholeaodv/grayholeaodv.o \
grayholeaodv/grayholeaodv_rtable.ograyholeaodv/grayholeaodv_rqueue.o \
```

Figure 4: *makefile.in* grayholeaodv modification

### 4.1 Implementing new DSDV protocol

Implementation of new DSDV protocol is similar to that of a new AODV protocol implementation and the library changes are similar and we used the name grayholedsdv instead of grayholeaodv. To integrate new grayholedsdv protocol to the simulator we similarly modified the two files as follows.

```
grayholedsdv {
setragent [$self create-grayholedsdv-agent $node]
}
simulatorinstproc create-grayholedsdv-agent {node} {
setragent [new Agent/grayholeDSDV]
setaddrs [$node node-addr]
$ragentaddr $addr
$ragent node $node
If [simulator set mobile_ip_] {
$ragent port-dmux [$node demux]
}
$node addr $addr
$node set ragent_ $ragent
$self at 0.0 “$ragent start-grayholedsdv”  ; # start updates
Return $ragent
}
```

Figure 5: *ns-lib.tcl*grayholedsdv modification

```
grayholedsdv/grayholedsdv.ograyholedsdv/grayholertable.o queue/rtqueue.o\
```

Figure 6: *makefile.in* grayholedsdv modification

### 4.2 Attack implemented on AODV and DSDV protocol

In general, AODV and DSDV are efficient and scalable in terms of network performance, but it allows attackers to easily advertise falsified route information to redirect routes and to launch various kinds of attacks. In each AODV and DSDV routing packet, some critical fields such as hop count, sequence numbers of source and destination, IP headers as well as IP addresses of AODV and DSDV source and destination, and RREQ ID, are essential to the correct protocol execution. Any misuse of these fields can cause AODV and DSDV to malfunction. Table 5 denotes several vulnerable fields in AODV routing messages and how possibly they are tampered.

| Field | Modification |
|---|---|
| RREQ ID | Increase to create a new RREQ request |
| Hop Count | If sequence number is the same, decrease it to update other nodes’ forwarding table, or increase it to invalidate the update |
| IP headers as well as AODV source and destination IP address | Replace it with another or invalid IP address |
| Sequence number of source and destination | Increase it to update other nodes’ forwarding route tables, or decrease it to suppress its update |

Table 1: Vulnerable Fields in AODV and DSDV Packets

Based on these Vulnerable Fields, implementation of the gray-hole attack is done in AODV and DSDV protocol and simulated in NS-2.35. To show the gray-hole behavior, one node is selected as attack node and it will drop packets randomly. The new protocols which show gray-hole attack should be able to participate in AODV and DSDV messaging.

### 4.3Implementing Gray-hole behavior on AODV protocol

To add gray-hole behavior in to the new AODV routing protocol we have to make some changes in the *grayholeaodv.cc* C++ file. By explaining the working mechanism of aodv and grayholeaodv protocol we will describe the changes made to the *grayholeaodv.cc*. In

*aodv.cc* code when a packet is received it is received by a function called the *recv*and the received packets are processed based on the type of the packet. In this code the different control packets in AODV like RREQ, RREP and RERR packets are processed by different functions. The *recv*function checks whether the received packet belongs to any of these control packets. If it so then it will call the *recvAODV*function. If the received packet is a data packet, usually the AODV protocol will forward the packet to the destination address. But in grayholeaodv protocol the code is modified such that it will drop random packets without forwarding it.

```
// if destination address is itself
if ((u_int32_t) ih->saddr ( ) == index)
forward ((grayholeaodv_rt_entry*) 0, p, NO_DELAY);
else if ((rand ( ) %6) ==3 | | (rand ( ) %6) ==4 | | (rand ( ) %6) ==1)
// for gray-hole attack in mobile ad-hoc network, after giving a true route to demanding node, gray-hole node drops some packets according to the random function.
drop (p, DROP_RTR_ROUTE_LOOP);
```

Figure 7: *grayholeaodv.cc* grayholeaodv modification

This attack is implemented in the *recv*function of grayholeaodv. First the conditions checks whether the packet is destined to itself if it so it will accept the packet, otherwise a condition is checked which is made of random numbers and if the condition becomes true the packet is dropped otherwise it will forward the packet.

### 4.4 Implementing Gray-hole behavior on DSDV protocol

To implement the gray-hole behavior in to the new DSDV routing protocol, the *recv*function of grayholedsdv protocol is used to forward the packet if the packet is a data packet otherwise the packet is dropped randomly.

```
else if ((rand()%6)==3 || (rand()%6)==4 || (rand()%6)==1) {
drop (p, DROP_RTR_ROUTE_LOOP);
        }
else
      {
        forwardPacket(p);
      }
```

Figure 8: *grayholedsdv.cc* grayholedsdv modification

## 5. Experiments and Evaluation

In this chapter, we evaluate the impact of gray-hole attack and IDS security solution to secure AODV and DSDV routing protocols in MANET. To evaluate these models, packet delivery ratio, throughput and packet lost is used. And we provide a detailed analysis that obtained from the simulation results.

### 5.1 Modeling of Network

The experiments are simulated using NS-2. The size of the network is specified by selecting the X distance and Y distance in given units. We selected 700 x 700 meters as our network size. More technologies are specified which are used in the simulation. We selected Mobile Ad hoc Network model in the technologies. After selecting the network size, nodes are properly configured manually.

### 5.2 Simulation Parameters

In our simulation we used the UDP connection instead of using a TCP connection. The reason behind using UDP over TCP is that, in TCP the protocol will close the connection if it won't get a reply ACK from the destination for the packets send. So if the grayholeAODV and grayholeDSDV protocols are implemented then the TCP will close the connection when the node drops the packet. Thus UDP protocol is used in the simulation in which no acknowledgement is received by the source node for the packets send. We are able to count the number of packets sent and received in the simulation because of using the UDP protocol. If the TCP protocol is used the source node will stop the connection if the TCP ACK packets are not received.

We simulated a network with a field size of 800m x 800m that has 20 nodes and create a UDP connection between two nodes and attach CBR (Constant Bit Rate) application that generates constant packets through the UDP connection. UDP agents are attached to the sending nodes and NULL agents are attached to receiving nodes. CBR packet size is chosen to be 512 bytes long and the packets are generated at an interval of .05s. The MAC layer used is *MAC* 802*:*11 with a data rate of 1Mbyte. The nodes will move within the network space according to the random waypoint mobility model. In random waypoint mobility model, each node will moves to a random location within the specified network area. A brief summary of the simulation parameters are listed in Table 6.

Table 2: simulation environment

| Parameter | Value |
|---|---|
| Simulator | NS-2(version 2.35) |
| Network area | 800 x 800 (m) |
| Connection type | UDP |
| Traffic type | Constant bit rate (CBR) |
| Routing protocol | Modified AODV and DSDV |
| Number of node | 20 |
| Packet size | 512 bytes |
| Node speed | 5,10,15,20,25,30 |
| Number of attack | 1 |
| Node placement | Random |

### 5.3 Performance Metrics

The performance of any routing protocol is measured by certain quantitative metrics. The performance metrics chosen for the evaluation of gray-hole attack are packet delivery ratio, throughput and packet loss.

**Packet Delivery Ratio:** Total number of delivered data packets divided by total number of data packets transmitted by all nodes. This performance metric will give us an idea of how well the protocol is performing in terms of packet delivery at different speeds using different traffic models. The more packet delivery data to the destination means better execution of the protocol.

PDR (%) = (total number of packets received /total number of packets send) x100.

**Packet Lost:** It is defined as total number of packets dropped during simulation for the better performance of a network this ratio should be minimum.

Lost packet = Number of send packet - Number of Received packet.

**Average throughput:** it is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet.

Average throughput = (number of bytes received x 8 /simulation time x 1000) Kbps

### 5.4 Simulation Scenario

We are mainly focusing on three simulation scenarios, the normal operation of routing protocols, gray-hole attack behavior and provide security solution for routing protocols in MANET.

#### 5.4.1 First Scenario

In these experiments, no gray-hole nodes are considered. The network size is 20 nodes and is randomly distributed in 800m×800m area. UDP connections are established between the sending and receiving nodes. In all the scenarios, we have a total of 6 connections between 12 nodes and every node is placed in different coordinates and shows different movements.

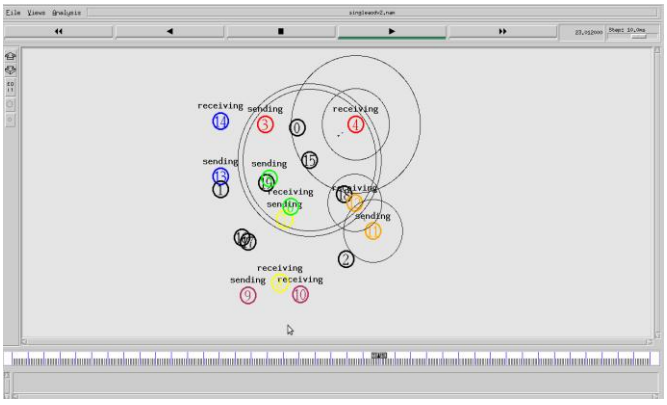


Figure 9: Simple MANET Scenario

## 6 Results and Discussion

This focuses on result and its analysis based on the simulation performed in NS-2. Our simulated results are provided in the Figures below gives the variation in network mobility while under normal operation, under gray-hole attack and after defending gray-hole attack. To evaluate the simulation result, we considered the performance metrics of packet delivery ratio, throughput and packet lost.

### 6.1 Packet Delivery Ratio

This represents the level of delivered data to the destination. The more packet delivery data to the destination means better execution of the protocol. Figure 10 shows the effect of the network mobility on packet Delivery Ratio and performance comparison of normal AODV, AODV with gray-hole attack and Proposed or idsAODV under varying network speed between 5 to maximum speed as 30 m/sec. we can clearly observed that for normal implementation of AODV, the packet delivery ratio is 99.76 % in 10 ms but after the gray hole attack is added on the AODV, the packet delivery ratio becomes 87.28 % means there is a loss of packets & the loss of packet is due to the gray hole attack problem. And the second observation is that idsAODV protocol has a high packet delivery ratio as compared to gray-hole Attack AODV. So it is more secure and attack free route for data delivery.

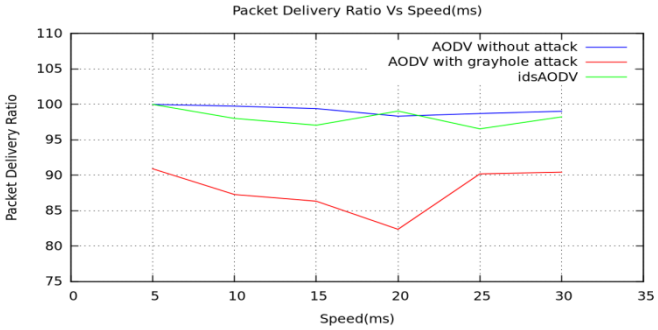


Figure 10: Packet Delivery Ratio vs. mobility for AODV

Figure 11 shows, for normal implementation of DSDV with 10 ms, the packet delivery ratio is 85.52 % but after the gray-hole attack is added on the DSDV, the packet delivery ratio with same speed value becomes 68.73 %. When we used the solution for the attack, the packet delivery ratio increased to 84.92 %.

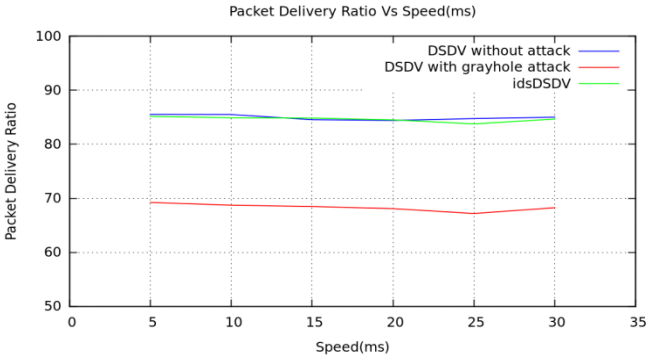


Figure 11: Packet Delivery Ratio vs. mobility for DSDV

## 6.2 Throughput

The Figure 11 shows the effect of the network mobility on throughput for normal AODV, AODV with gray-hole attack and idsAODV solution. The first observation from the Figure 11 is that in the case of AODV without attack, its throughput is higher than in the case with under attack because of the packets dropped by the malicious node. The second observation is that our protocol idsAODV gives higher and enhanced throughput than AODV with attack and it's near to the performance of normal AODV (without attacking) protocol. The idsAODV strongly prevents gray-hole attack based on the proposed solution. On the other hand from the Figure 12, we also observed that the throughput of normal DSDV and idsDSDV are better than compared to gray-hole DSDV.

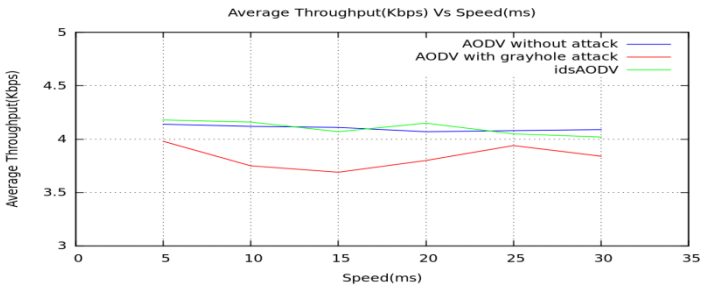


Figure 11: Average Throughput vs. mobility for AODV

### 6.3 Packet Lost

Figure 14 shows the effect of the network mobility on packet Delivery Ratio and performance comparison of AODV, AODV with gray-hole attack and Proposed or idsAODV under varying network speed between 5 to maximum speed as 30 m/sec.

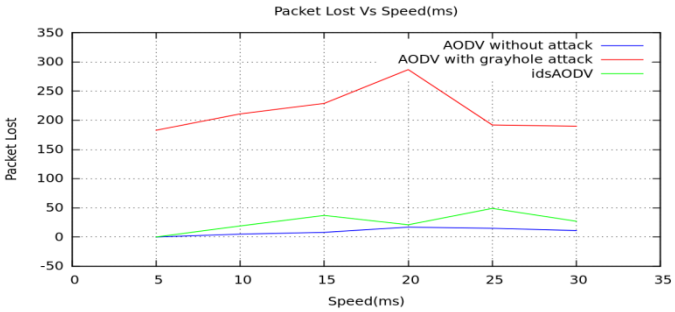


Figure 12: Average Throughput vs. mobility for DSDV

Having simulated the gray-hole Attack, we saw that the packet loss is increased in the ad-hoc network. The simulation result shows the difference between the number of packets lost in the network with and without a gray-hole attack. This also shows that gray-hole attack affects the overall network connectivity and the data loss could show the existence of the gray-hole Attack in the network. If the network mobility is increased then the data loss would also be expected to increase. Another observation is that idsAODV gives lower packet dropped than AODV with gray-hole attack.

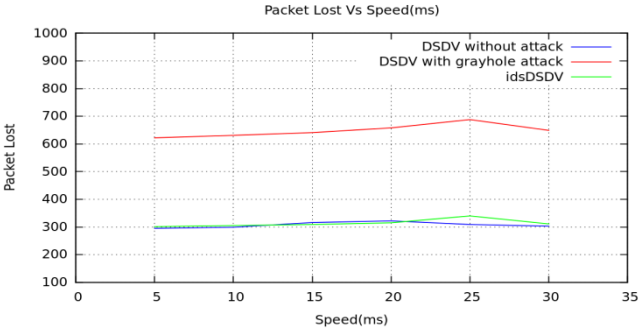


Figure 14: Packet Lost vs. mobility for AODV

Figure 15 shows that the packet loss is more when network is under attack by malicious node. When idsDSDV is introduced, packet loss is reduced more.

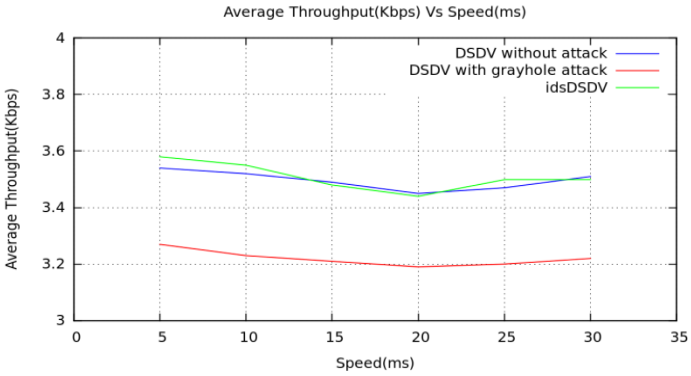


Figure 15: Packet Lost vs. mobility for DSDV

## 7 RESULTS SUMMERY

Based on the simulation result, performance of AODV is better than DSDV in normal operation (without the gray-hole attack), with gray-hole attack and after introducing intrusion detection system into MANET. We also observed that AODV has more PDF than DSDV because of high mobility, instability, and low density and the proactive nature of DSDV protocol. But in the presence of gray-hole attack AODV has more delay than DSDV this is because its route searches and reactive nature.

## 8.CONCLUSION AND FUTURE WORK

In this thesis, we analyzed the effect of gray-hole attack in an AODV and DSDV Networks. Gray-hole attacks in MANET meaningfully lower network performance and threat to network security. Gray-hole attacks are severe attacks that can easily destroy or disturb the normal functionality of the network and security goals such as confidentiality, authentication, integrity, availability and non-repudiation. By using the NS-2 network simulation environment, the intrusion detection system is implemented on the AODV and DSDV. The implemented solution reduced the impact of gray-hole attack in NS-2.

When we simulated the gray-hole Attack, we saw that the packet loss is increased in the ad-hoc network. In the simulation results show the difference of packets lost in the network without gray-hole attack, with gray-hole Attack and after prevented gray-hole attack in both protocols. This shows that gray-hole attack affects the overall network connectivity and the data loss shows the presence of gray-hole attack in the network.

We observed from AODV network has normally 0.24 % data loss and if a gray-hole node is added in this network data loss is increased to 12.72 %. Gray-hole node increases this data loss by 12.48 %. When we added idsAODV protocol in the network, MANETs Performance is increasing. The PDR, Throughput is increasing and the data loss decreased to 10.74 %. This result shows that our solution reduces the gray-hole impact by 10, 74 %.

Again we observed from DSDV network has normally 14.46 % data loss and if a gray-hole node is added in this network data loss is increased to 32.27 %. Gray-hole node increases this data loss by 16.79 %. When we added idsAODV protocol in the network, MANETs Performance is increasing. The PDR, Throughput is increasing and the data loss decreased to 16.19 %.

### 8.1 Future Work

In our thesis, we simulated the effect of gray-hole attack in MANET using AODV and DSDV protocols and we try to prevent the gray-hole attack in the network using Intrusion Detection Systems (IDS). In the future, the same work can be done for more than one gray-hole node that means for multiple gray-hole nodes and for different protocol like DSR.

## 9. REFERENCES

[1] OnkarV.Chandure,V.T.Gaikwad, "Detection Prevention of Gray Hole Attack in Mobile Ad-

Hoc Network using AODV Routing Protocol", March 2012.

[2] Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala "Improving Route discovery for AODV to prevent Black hole and Gray-hole Attack in MANTEs", INFOCOM, March 2012.

[3] A. Kanthe, D. Simunic, R. Prasad , " A Mechanism for Gray Hole Attack Detection in Mobile Ad–hoc Networks", International Journal of Computer Application, September 2012.

[4] Rashmi Ahlawat, Dr. Setu K Chaturvedi, "Performance Evaluation of AODV under Black Hole Attack Using Anomaly Based IDS", International Journal of Computer Science Research & Technology, August 2013.

[5] BhimsinghBohara,VarunSharma,"Analysis and Prevention of effects of gray hole attacks On Routing Protocol in Mobile Ad-hoc Networks", International Journal of Advanced Research in Computer and Communication Engineering, June 2013.

[6] NishaPuri, SimranjitKaur, Sandeep Kumar Arora, "Performance Analysis of Mobile Ad Hoc Network in the Presence of Sink Hole attack", International Journal of Scientific Engineering and Research (IJSER), November 2013.

[7] Jagdish J. Rathod , Amit M. Lathigara , " Enhanced AODV Routing for Secure MANET Using Preventing Gray hole Attack", International Journal of Science and Research (IJSR) 2013.

[8] Deepali A. Lokare,A.MKanthe,DinaSimunic, "Cooperative Gray Hole Attack Discovery and Elimination using Credit based Technique in MANET",International Journal of Computer applications, February 2014.

[9] https://www.crcpress.com/Security-of-Self-Organizing-Networks-MANET-WSN-WMN-

VANET/Pathan/9781439819197.

[10] RatnaSireeshaSingamsetty, "Detection of Malicious Nodes in Mobile Adhoc Networks", Master's Thesis, December 2011.

[11] Onkar V. Chandure, Aditya P. Bakshi, Saudamini P. Tidke, Priyanka M. Lokhande, "SIMULATION OF SECURE AODV IN GRAY HOLE ATTACK FOR MOBILE AD-HOC NETWORK", International Journal of Advances in Engineering & Technology, Nov. 2012.

[12] http://installwithme.blogspot.com/2014/05/how-to-install-ns-2.35-in-ubuntu-12.04.html

[13] https://sourceforge.net/projects/nsnam/