Reputation Approach to detect BLACKHOLE ATTACK in VANET

Ravi Patel[1], Khushbu Shah[2]
[1]*Department of computer engineering, LJ Institute of Technology, India*
[2]*Assistant Professor, Department of computer engineering, LJ Institute of Technology, India*
[1]*E-mail: ravicpatel@live.com*

***Abstract*– In this paper, we present our idea of detection and countering the effect of blackhole attack in Vehicular Ad-hoc Network (VANET). Recently, many attackers have been attracted towards VANET which is subclass of Mobile Ad-hoc Network (MANET). To save this life saving system from Blackhole Attack we have tried to implement Intrusion Detection System based on Reputation of Nodes, explained in this paper. On implementing Reputation Approach (RA), there are possibilities of innocent nodes getting affect. This technique helps us to study behavior of blackhole node and tries to counter accordingly. In addition, in this paper we have provided report based on simulated implementation.**

***Index Terms*- IDS, Reputation Based Approach, VANET, Blackhole Attack**

I. INTRODUCTION

In past few years, cyber-crime rate has increased its bound. They are now focusing on making VANET system vulnerable. Today major concern is to provide safety of users and safe their lives in road accidents. Safety and non-safety potential applications of VANET are to ensure the safety of human life on the road. Security is main concern because when data is compromised, the whole system suffers. Security measures must be taken to avoid malicious attacks on the system.

Now, Attackers try to compromise the system according to their need. The do various kind of attacks, some of them are explained in this paper. And research division has also tried to strengthen the system for intruders.[1]

1.1 VANET

In the recent years, the multi-path ad hoc networks have become an attractive topic. VANET, a subclass of MANETs potential application fields have emerged. Basically, in VANET architecture there is no fix network structure. It has highly dynamic network. In VANET basically, there are two types of communication possible, Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V). Each vehicle is installed with On Board Unit (OBU), which is helpful to communicate with other OBUs and Road Side Units (RSU), which are installed on Road Side to help in communication. [2]

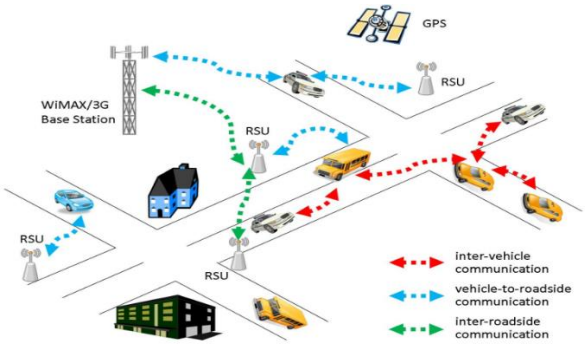

Figure 1.1: VANET working [12]

II. ATTACKS ON VANET

Here in this section we will go through some of the attacks carried by intruders on VANET.

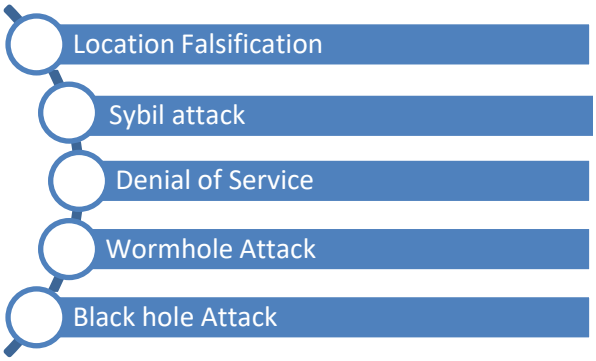

Figure 2.1: Various attacks on VANET.

Here we have basically two way of data forwarding

1. Predefined Route
2. Dynamic Route

Generally in Predefined Routing below attacks may happen [3]

1. Location Falsification [3]: Attackers passes faked position.
2. Black hole Attack [3]: Attackers lure data towards it and consumes it fully.
3. Sybil Attack [4]: Attackers creates illusion for the other nodes of network.

And in Dynamic routing below attacks may happen [3]

1. Black hole Attack
2. Sybil Attack
3. Wormhole Attack: Attackers, creates a tunnel and works same as blackhole attack.
4. Denial of Service: Attackers, jam whole network, which provides inconvenience to other nodes.

III. ANALYSIS OF BLACKHOLE ATTACK [5]

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. When the route is established, now it's up to the node whether to drop all the packets or forward it to the unknown address.

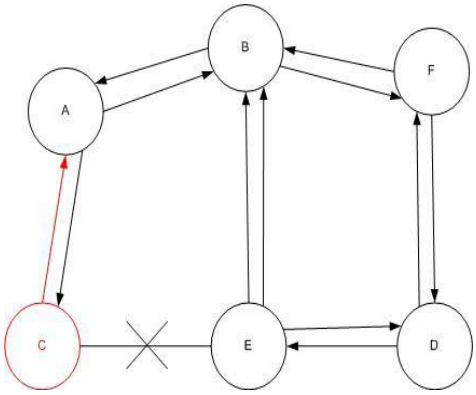

Figure 3.1: BLACKHOLE attack [5]

Fig. 3.1 [5] shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost. [5]

Blackhole Attack on AODV [5]-

Generally by two ways attack may happen in AODV as internal node which fits in between the routes of given source and destination and other one is external which is not in route.

Internal node can easily attack as it is in the routing path.

External node can attack by following way [5]:

1. Malicious node detects the active route and notes the destination address.
2. Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
3. Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
4. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
5. The new information received in the route reply will allow the source node to update its routing table.
6. New route selected by source node for selecting data.
7. The malicious node will drop now all the data to which it belong in the route.

IV. PROPOSED MODEL OF REPUTATION APPROACH (RA)

As per literature review done, proposed model will try to counter the effect by using Reputation and also the monitoring from IDS node which will help to reduce the memory consumption on IDS node and also tries to efficiently detect BLACKHOLE attack.

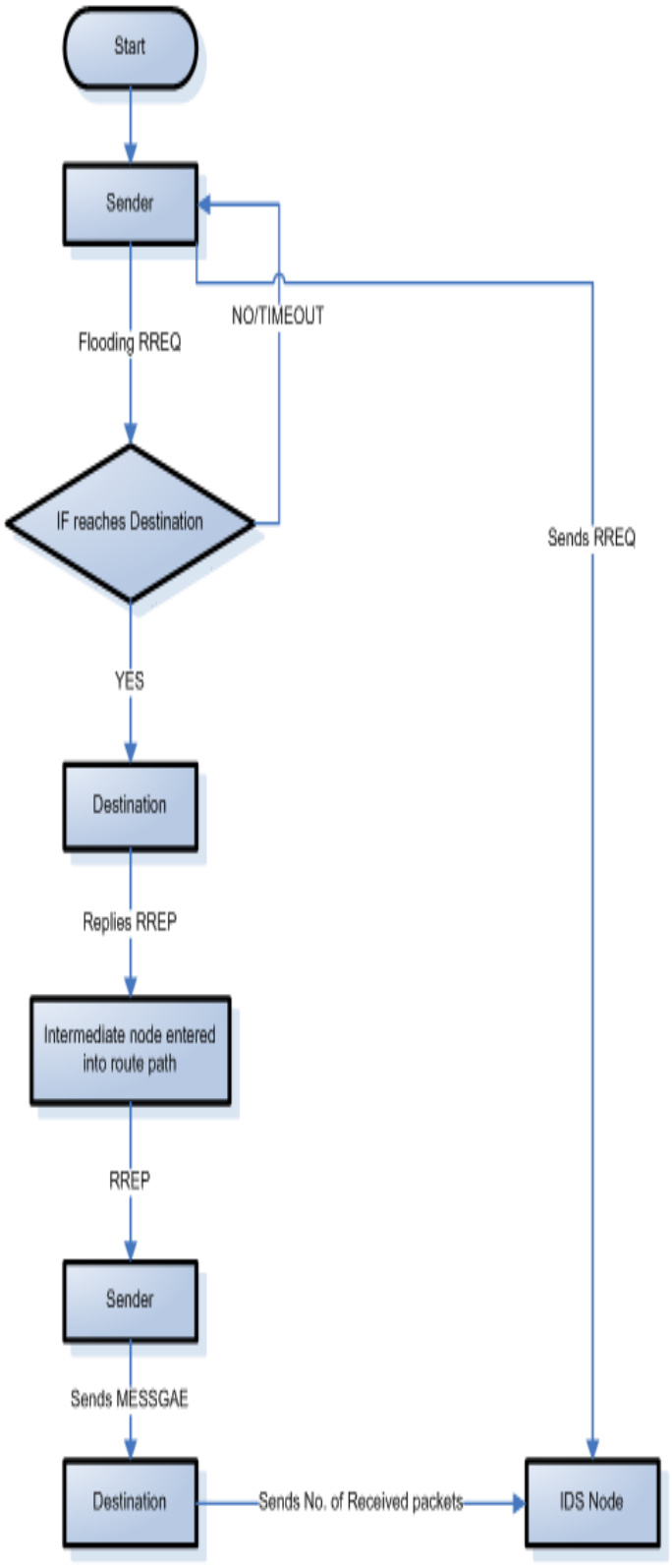

Figure 4.1: Proposed Flow diagram for Routing Strategy

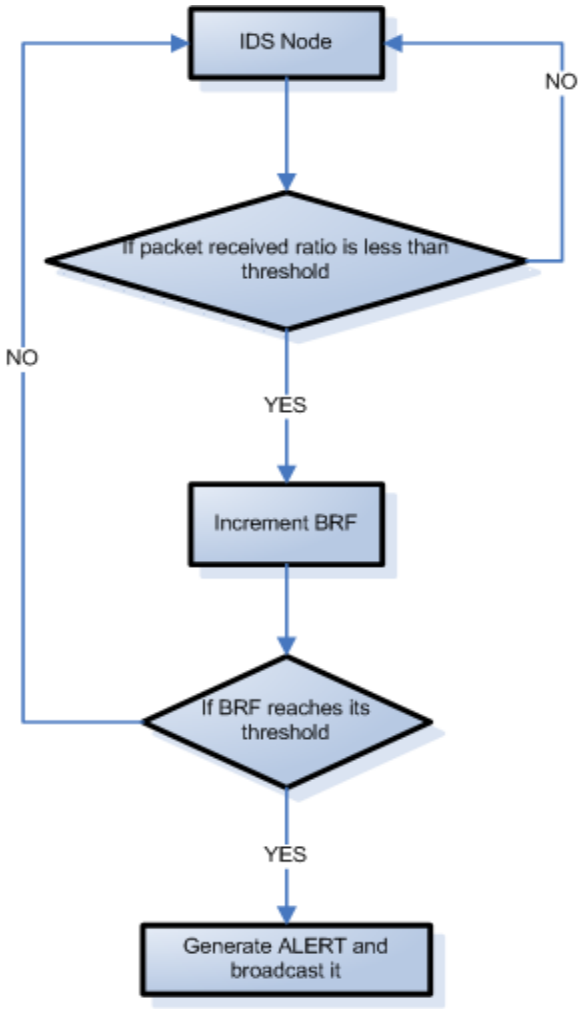

Figure 4.2: Proposed Flow diagram of IDS node for detecting black hole node

- As from Figure 3.1, when sender wants to send message to destination then it floods RREQ and sends a copy to IDS node to.
- RREQ will be containing the total number of packets sender wants to send in its one of the field.
- After that on RREQ, Destination will reply RREP and intermediate path will be embedded in it.
- When Sender gets an RREP from destination, sender will send message with the intermediate node if no maliciously marked node exist in it.
- After receiving packets from sender destination, destination will send number of packets received to IDS node.
- Now, further IDS node will handle as shown in Figure 3.2

- IDS node will find Nd/Ns (packet delivery ratio); where Nd is number of packets received and Ns is the number of packet sent.
- According to threshold value of Packet Delivery Ratio (PDR) it will detect a blackhole node, if any in the communication.
- Then IDS node will mark node as blackhole node and broadcast to other nodes in network.
- This will help other node to avoid communication from blackhole node.

TYPE	FLAGS	No. of PACKETS	HOP COUNT
RREQ (BROADCAST) ID			
DESTINATION IP ADDRESS			
DESTINATION SEQUENCE NUMBER			
SOURCE IP ADDRESS			
SOURCE SEQUENCE NUMBER			

(a) RREQ

TYPE	ROUTING PATH	RESERVED	HOP COUNT
DESTINATION IP ADDRESS			
DESTINATION SEQUENCE NUMBER			
SOURCE IP ADDRESS			
SOURCE SEQUENCE NUMBER			

(b) RREP

Figure 4.3: Proposed Packet Structure RREQ and RREP

Suspicious Node Table

Node ID	Bad Reputation Factor (BRF)	Malicious Node Marked/Unmarked
3	6	0
7	1	0
8	17	1

Table 4.1: Proposed Suspicious Node Table

Block Node Table

IDS Node	Malicious Node	Time

Table 4.2: Proposed Block Node Table

V. IMPLEMENTATION OF REPUTATION APPROACH (RA)

5.1 Implementation Setup

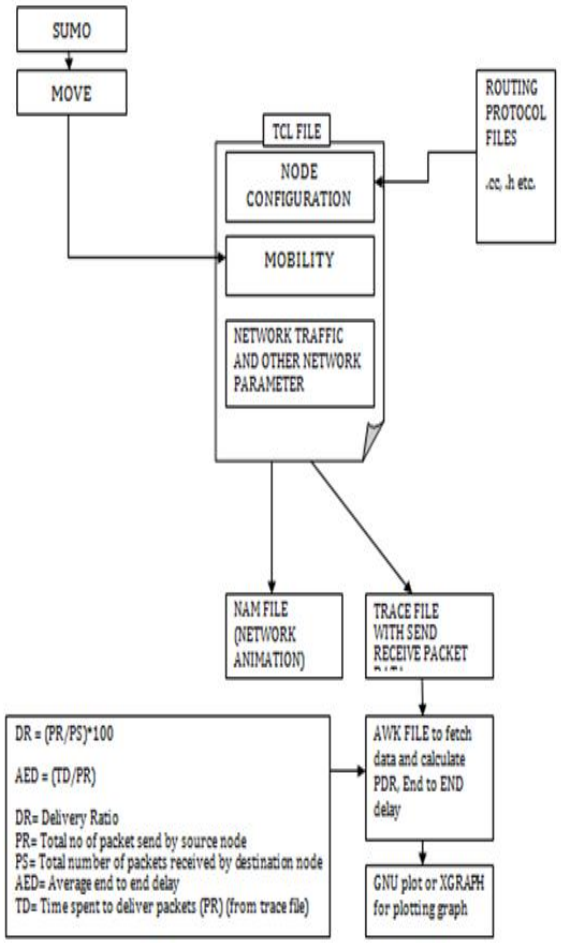

Figure 5.1.1: Flow of Code for Implementation

5.2 Implementing Blackhole Attack in ns-allinone-2.34

Step 1: Modifying "Makefile" so that new protocol's file can be compiled and linked

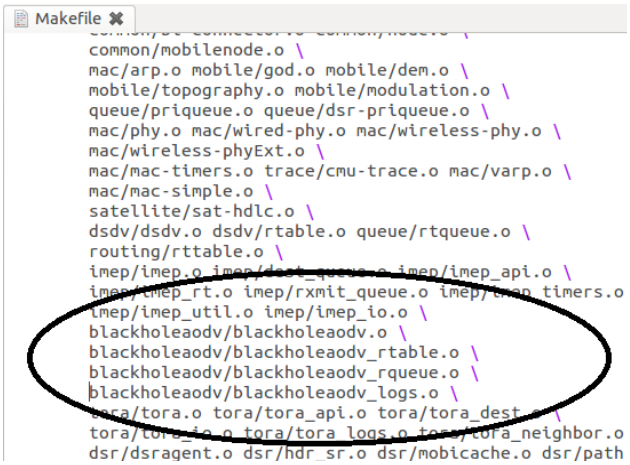

Figure 5.2.1: MakeFile

Step 2: Patching new Packet

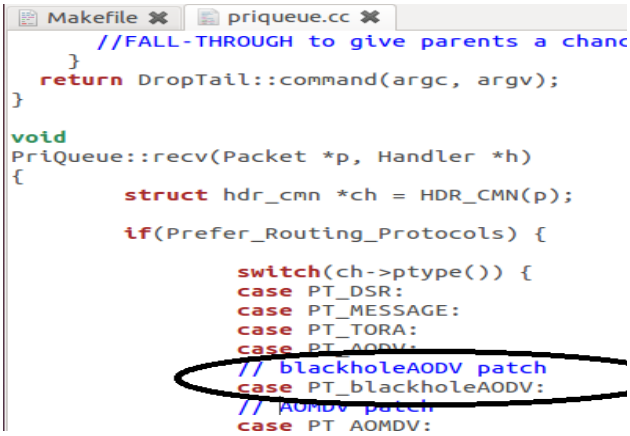

Figure 5.2.2: priqueue.cc for patching

Step 3: To define new routing protocol packet type we have to modify ~/ns-allinone-2.34/ns-2.34/common/packet.h file.

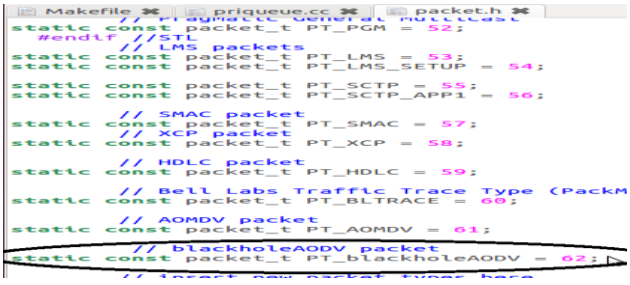

Figure 5.2.3: packet.h for adding new packet

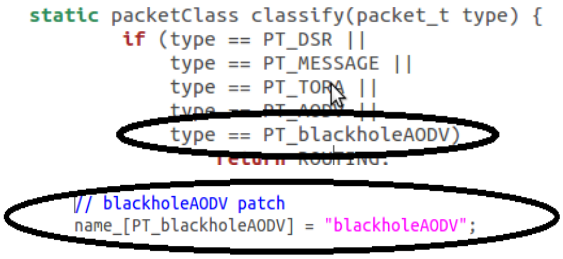

Figure 5.2.4: packet.h for prioritizing new packet

Step 4: Now we will modify tcl files to create routing agent.

Figure 5.2.5: ns-lib.tcl for creating routing agent

Step 5: Now we will set port numbers of routing agent. sport is source port, dport is destination port.

Step 6: Now in ~/ns-allinone-2.34/ns-2.34/tcl/lib/ns-mobilenode.tcl

```
# Special processing for blackholeAODV
set blackholeaodvonly [string first "blackholeAODV"
[$agent info class]]
if {$blackholeaodvonly != -1 } {
$agent if-queue [$self set ifq_(0)] ;# ifq between LL
and MAC
}
```

Step 7: After this changes to compile again and link the files run command

root@ubuntu ~/ns.34#make clean
root@ubuntu ~/ns.34#make

5.3 Implementing IDS based on Reputation Approach (RA) in ns-allinone-2.34

```
*aodv_packet.h
};

struct hdr_aodv_request {
        u_int8_t        rq_type;        // Packet Type
        //u_int8_t        reserved[2];
        u_int8_t        rq_no_packet;   //no. of packets
        u_int8_t        rq_hop_count;   // Hop Count
        u_int32_t       rq_bcast_id;    // Broadcast ID

        nsaddr_t        rq_dst;         // Destination IP Address
        u_int32_t       rq_dst_seqno;   // Destination Sequence Number
        nsaddr_t        rq_src;         // Source IP Address
        u_int32_t       rq_src_seqno;   // Source Sequence Number

        double          rq_timestamp;   // when REQUEST sent;
                                        // used to compute route discovery late
```

Figure 5.3.1: aodv_packet.h for using reserved 8 bit in IDS

5.4 Simulation of Blackhole Attack and IDS based on Reputation Approach (RA)

- Performance Parameter

Parameter	Value
Simulator	ns-2.34
Protocol	AODV
Number of nodes	12,20
Max. Simulation time	150,500
Simulation Area	500 * 400,750 *750
Pause Time	0,10,20,30,40

Table 5.4.1: Performance Parameters

- Simulating Blackhole Attack

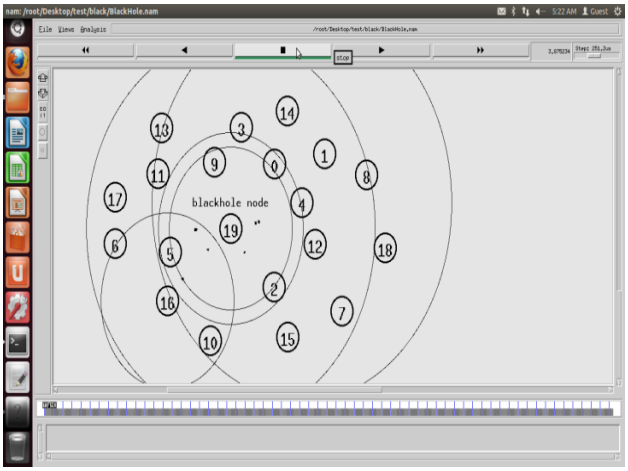

Figure 5.4.1: network simulation of BlackHole.nam

- Simulating IDS

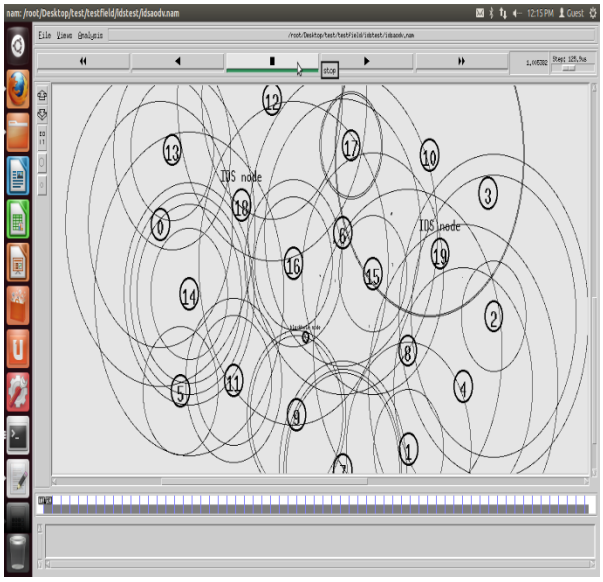

Figure 5.4.2: network simulation of idsaodv.nam

VI. RESULTS ANALYSIS

Packet Delivery Ratio = (No of Received Packets/No of Send Packets)*100

- Result obtained from trace for AODV

Pause Time	PDR(Packet Delivery Ratio)
0	98.96
10	99.05
20	99.12
30	98.79
40	99.73

Table 6.1: Result of PDR of AODV on different Pause time

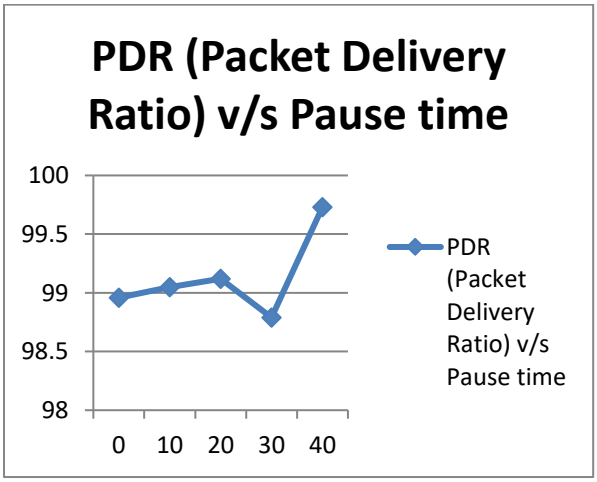

Figure 6.1: Graph of PDR v/s Pause time of AODV

➢ Result obtained from trace for blackholeAODV

Pause Time	PDR
0	72.57
10	73.19
20	71.6
30	71.77
40	72.35

Table 6.2: Result of PDR of blackholeAODV on different Pause time

➢ Result obtained from trace for idsAODV

Pause Time	PDR
0	75.97
10	76.54
20	75.59
30	75.99
40	77.74

Table 6.3: Result of PDR of idsAODV on different Pause time

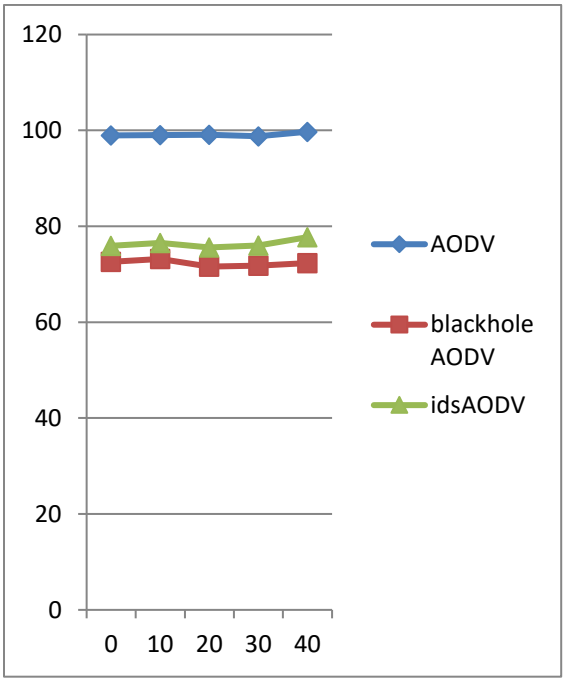

Figure 6.2: Graph of PDR v/s Pause time of AODV, blackholeAODV & idsAODV

VII. CONCLUSION

As per the Result analysis, it is cleared we are able to achieve 5% of more accuracy and precision on detecting blackhole attack and countering the effect of it. Our threshold was set on 95 as from Fig 6.1 it was clear that on normal network communication from 100 packets 95 packets were able to reach destination without attack. But when blackhole attack took place PDR reduces to (70-73). And after applying IDS based on Reputation Approach (RA) it increases to (75-78). Many times innocent neighboring node to the attackers has to suffer due to bad reputation.

So at last research is concluded as, Intruders have been attracted towards VANET. Various kinds of attacks take place over VANET. In BLACKHOLE Attack, packets are lost and do not reaches its destination. Proposed model enhance the security in the current IDS technique by building reputation of nodes. Reputation is built by number of packet sent and received in communication. And an IDS node is placed in every group to monitor the malicious activity of the node, and triggers alarm if BLACKHOLE Attack is detected.

REFERENCES

[1] Ravi Patel, Khushbu Shah. *"GLANCE over VANET, ATTACKS over VANET and their IDS approaches."*, International Journal of Innovative Research in Technology (2014).

[2] Yousefi, Saleh, Mahmoud Siadat Mousavi, and Mahmood Fathy. *"Vehicular ad hoc networks (VANETs): challenges and perspectives."* ITS Telecommunications Proceedings, 2006 6th International Conference on. IEEE, 2006.

[3] Xu, Yufei, X. Wu, and D. Teng. *"Secure Routing in WSNs and VANETs: Security Improved Geographic Routing and Implicit Geographic Routing."*

[4] Sumra, Irshad Ahmed, et al. *"Classes of Attacks in VANET."* Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International. IEEE, 2011.

[5] Ullah, Irshad, and Shoaib Ur Rehman. *"Analysis of Black Hole attack on MANETs Using different MANET routing protocols."*School of Computing Blekinge Institute of Technology, Sweden (2010).