International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 3 Issue: 10
ISSN: 2454-4248
222 – 229

Black hole Attack Prevention in VANET

Prof. Ajay N. Upadhyaya
Computer Engineering Department
Doctoral Research Scholar, Faculty of Technology,
RK University, Rajkot, India
Assistant Professor L.J. Institute of Engineering & Technology, GTU, Ahmedabad, India,
ajay8586g@gmail.com

Dr. J. S. Shah
Computer Engineering Department
Ex. Principal, Government Engineering college,
Patan, India
jssld@yahoo.com

Abstract— The past decade has witnessed the emergence of Vehicular Ad-hoc Networks (VANETs), from the well-known Mobile Ad Hoc Networks (MANETs) in wireless communications. VANETs are self-organizing networks established among vehicles equipped with communication facilities. In VANETs vehicles are equipped with On Board Unit (OBU) through which they are capable of organizing themselves, by discovering their neighbor vehicles and capable to communicate with Infrastructure nodes equipped with Road Side Unit (RSU) for finding optimal path, Service based Information as well as other sensible Information for safe Transportation over the wireless medium. Recently, VANETs have been getting greater attention as more applications are depending on them. Researchers have tried to propose various Protocols, Approaches and methodologies that will improve the Quality, Efficiency, Authenticity and Integrity of different services of VANETs. Many of the applications require a high level of security. Thus, the main challenge is to protect VANETs from different security attacks. VANETs use the open wireless medium to communicate which makes it easy for an attacker to impose his attacks by Manipulating, Sniffing, and blocking the different packets. In VANETs all the nodes can act as routers for the data packets and there is no clear line of defence where it is possible to place a firewall. The main concern is how to provide best security in VANET without any negotiating with performance & reliability.The objective of this work is to check feasibility of using infrastructure based vehicular communication for detecting and preventing Blackhole Attacks. In this paper we proposed three different approaches for Blackhole attack prevention. We analyze performance of the proposed approaches for different scenario by generating heterogeneous traffic environment. With the proposed approaches we get the reduction in Packet Loss of up to 79.6971%.

Keywords-*Blackhole Attack Detection, Blackhole Attack Prevention, AODV, Maximum Sequence Number, Neighbor Awareness Count, Trusted Path*

*****

I. INTRODUCTION

All Attacker's role is important in vehicular network due to launching different type of attacks. The objective of attackers is to create problems for other users of the network by manipulating, delaying or hiding the messages from the needy user. Here we will mainly discuss blackhole routing attack. Routing attacks are the attacks which exploits the vulnerability of network layer routing protocols. In this type of attack the attacker either drops the packet or disturbs the routing process of the network. The most common Routing attacks are: Blackhole attack, Wormhole Attack and Grayhole attack.

In blackhole attack, the malicious node firstly attracts the other nodes for transmit the packet through itself. This can be easily done by sending the Malicious Route Reply (MRR) with fresh route details and hop count having a very less value. After this process other node will attract to malicious node and send all their packets through that malicious node which will be silently drop by malicious node. This effect is known as a blackhole attack.A blackhole is an area which can be either created by a single node or by multiple nodes where the network traffic is redirected wrongly. Also malicious node rapidly sends advertises that it has a fresh route for the each upcoming route request.

Fig. 1 illustrates an example where the Car-A wants to send data packets to Car-F but it doesn't having any route details for Car-F. Therefore, Car-A initiates the route discovery process and RREQ is forwarded to Car-B, Car-C and Car-D. As a malicious node, Car-D will claim that it is having shortest route to reach at Car-F. Based on available reply Car-A will send

messages to Car-D and becomes the victim of blackhole attack. Malicious node may change its strategy for attack depending on the types of routing protocols like Ad hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR) or Optimized Link State Routing (OLSR).

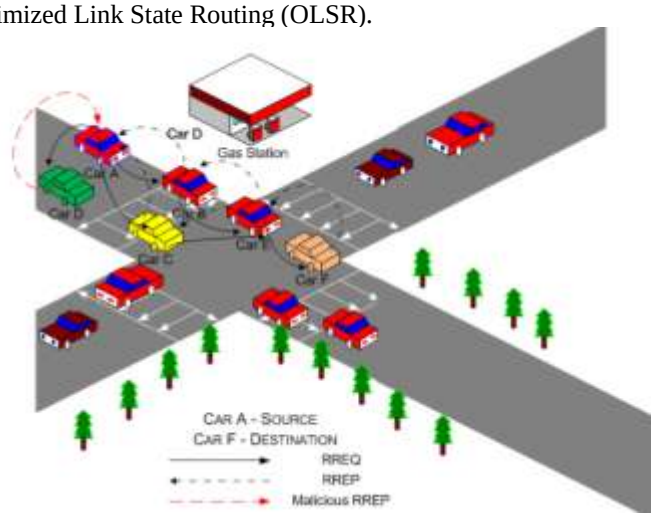

Figure 1. Blackhole Attack in VANET

 ISSN: 2454-4248
222 – 229

We can categories the blackhole attack in two categories: Single Node Blackhole Attack and Collaborative Blackhole Attack. Some researcher had proposed different methods for detecting such blackhole attacks. But it required more research in the domain of blackhole detection and prevention.

II. RELETED WORK

VANETs are particularly prone to malicious behaviour. Due to the lack of any centralized authority VANETs becomes very vulnerable to eavesdropping and infiltration. Security is often considered to be the major barrier in commercial application of VANETs. In the recent research work different researcher had proposed different solutions for the domain of blackhole attack.

In recent research work [1], the author proposed solution for AODV enhancement by managing the Coming Route Reply table (CRRT), sequence number, lifetime, and hop count of packet. In [2], [9], [11], [13] and [14] the different solutions are proposed by authors for establishing trust management in VANETs. In trust management trust level can be establishing by nodes on other car nodes by their OBU or by RSU-Infrastructure Nodes. Trust is a very difficult task to achieve in VANETs because it is decentralized in nature. The entry and exit time of any car nodes in the range of other car nodes as well as in the range of RSU is unpredictable. In this solution need to built trust table based on the trust values given by other vehicle which they collected from their neighboring vehicles. For the blackhole attack detection in [4] and [6], author proposed the usage of cryptographic methods. By using RSA key exchange neighbor node can be authenticated. As well as fingerprint and digital signature can be used for the checking the authenticity and integrity of routing messages. In [5],author analyze the effects of blackhole attack with routing protocols AODV and DOV(Hybrid protocol having benefits of AODV and DSR) in ad hoc network. In [8], author discussed about eliminating co-operative blackhole and grayhole attacks by managing the history of nodes and with the implementation of negative acknowledgement. In [10], author discussed about cooperative cross layer detection for blackhole attack by improving the watchdog detection by monitoring the number of RTS/CTS (request to send/clear to send) requests. In [12], author represented the approach about the Identity Based batch Verification (IBV) scheme for the authentication of node. The whole authentication process is done in three steps: System Initialization, Anonymous Identity Generation and Message signing & verification.

III. PROPOSED APPROACH

Here we will discuss about implementation of three different approaches. All the approaches are of blackhole preventive solution. We have taken AODV routing protocol so each approached name is given based on it. Here we will discuss about algorithm, Implementation, Result and conclusion of each approach AODV_MSN, AODV_NAC and ADDV_TP.

Approach- 1 is mainly based on the concept of Maximum Sequence Number. It is named as "AODV_MSN-Maximum Sequence Number" in which if source node will receive reply from any node with largest sequence number then it will be considered as a malicious node who want to imposed blackhole attack on network and that route toward that blackhole is discarded and based on it update the routing table and after that decision is taken based on the remaining entries.

Algorithm:

Here we will discuss blackhole prevention method using the route reply method. We had taken some of the notation like SN for Source Node, DN for Destination Node, N_ID for Node ID, MN_ID for Malicious Node ID, SN_SEQ for Source Sequence Number, DN_SEQ for Destination Sequence Number, RT for Routing Table, RREQ for Route Request, RREP for Route Reply.

Step 1: Initially source node, which is unaware about destination node broadcast Route Request Message (RREQ).

SN → «RREQ»

Step 2: Different node will receive RREQ broadcasted by Source Node and based on it different node will send Route Reply Message (RREP) to Source Node.

SN ← <RREP>

Step 3: Source Node will store all the upcoming RREP messages in Routing Table (RT) with the detailing of N_ID for Node ID and DN_SEQ for Destination Sequence Number.

SN(RT) ← {N_ID ,DN_SEQ}

Step 4: After getting reply from the different nodes, Source Node (SN) has to choose route for transmission from the available details of Routing Table (RT).But for avoiding Blackhole Attack, preventive measurement is taken as in Step 5 for identifying Malicious Node (MN).

Step 5: For Avoid Blackhole attack, Source Node will Check Routing Table (RT) for Malicious Node (MN) Entry. If Destination Node Sequence Number is very higher then Source sequence Number then it will be treated as Malicious node.

IF (DN_SEQ>>>=SN_SEQ)
{
Identify Node as a Malicious Node for
Node →→ MN
$DN_{(N\_ID)} := MN_{(MN\_ID)}$
Drop Malicious Node Entry from Routing Table
$SN\_RT_{\{Drop(MN\_ID)\}}$
}
ELSE
{
Node →→ Normal Node
}

Approach-2 is based on detection of malicious node by using Neighbor Awareness Count named it as "AODV_NAC". In this method responsibility will be given to Neighbor node for finding malicious node. Neighbor node will maintains two counters fwd_count and rcv_count used for counting number of forwarded packets and number of received packets respectively. First of all neighbor node will identify malicious node but neighbor node cannot directly take decision for it, so include that node into suspected node list and now onwards observe activities of that suspected nodes. fwd_count will be incremented by Neighbor node when it will transmits a packet to a particular suspected node. If suspected node forwards the packet, it will be overheard by

 ISSN: 2454-4248
222 – 229

Neighbor node and it increments rcv_count. Finally, neighbor node will forward packets to suspected node until fwd_count reaches a threshold (Thf); thereafter if rcv_count is 0 or difference between fwd_count and rcv_count will reaches to threshold (Thd), then neighbor node will identify that node as malicious node.

Algorithm:

Here we will discuss Blackhole Prevention method based on Neighbor awareness. We had taken some of the notation like SN for Source Node, DN for Destination Node, IN for Intermediate Node, RT for Routing Table, MN for Malicious node, NN for Neighbor of malicious node, PM for Promiscuous mode and MAL_NOT:- Malicious Notification, MN_ID for Malicious Node ID, RREQ for Route Request and RREP for Route Reply, fwd_count for counting number of forwarded packets, rcv_count for counting number of received packets, Thf for forwarding Threshold and Thd for Difference Threshold.

Step 1: Initially source node, which is unawares about destination node broadcast Route Request Message (RREQ).

SN → «RREQ»

Step 2: Different node will receive RREQ broadcasted by Source Node and based on it different node will send Route Reply Message (RREP) to Source Node.

SN ← <RREP>

Step 3: In this method total responsibility for malicious node detection is given to neighbor. So first neighbor node will put particular node into the list of Promiscuous mode and based on the activities of node neighbor node will take the decision that suspected node is malicious node or not.

Step 4: If any node receive the Route Reply (RREP) from any neighbor who is Originator of message then temporarily takes the judgment that the particular node for malicious node and then observe the activities of suspected node by putting it into Promiscuous mode. fwd_count and rcv_count will be calculated of Suspected Node. fwd_count will be incremented when it will transmits a packet to a particular suspected node and also manage rcv_count If suspected node forwards the packet.

While(*fwd_count* <Th_f && (fwd_count - rcv_count) < Th_d)
{
IF (Current node is NN)
{
Increment *fwd_count*;
IF (In PM received Packet from MN)
Increment *rcv_count*;
}
}
IF(*rcv_count*= 0)
{
Broadcast suspected node as a malicious node.
NN → «MAL_NOT»
End If;

Step 5: Remove the Malicious node entry from Routing Table.

Node →→ MN
SN_RT $_{\{Drop(MN\_ID)\}}$

Approach-3 is mainly based on the concept of trusted path named it as an "AODV_TP-Trusted Path". In the said approach node will build the trust level and based on it will take the decision for send data through particular node. Source node unaware about destination node will broadcast RREQ. All intermediate node is receiving route request and response accordingly RREQ. Source node will receive RREP response from many nodes. Source node will check each RREP message. Source node will get RREP message with the value of current time and arrival time of each reply which received during specific time limit. After that check repeated entries in Collect Route Reply Table (CRRT).If any repeated next hop node is present in the reply paths it assumes the paths are correct or the chance of malicious paths is limited. Now based on trusted list source node can select any route randomly.

Algorithm:

Here we will discuss preventing blackhole method using trusted path. We had taken some of the notation like SN for Source Node, DN for Destination Node, CRRT for Collect Route Reply Table, RT for Routing Table, RREQ for Route Request, RREP for Route Reply, IN for Intermediate Node, NH for Next Hop, Current_Time for the current time of packet and Arrival_time for arrival time of packet, Spec_Time_Limit for the specific time limit for receiving packet.

Step 1: Initially source node, which is unawares about destination node broadcast Route Request Message (RREQ).

SN → «RREQ»

Step 2: Different node will receive RREQ broadcasted by Source Node and based on it different node will send Route Reply Message (RREP) to Source Node.

SN ← <RREP>

If (Intermediate node have address as per SN $_{(RREQ)}$) Then
SN ← IN $_{(RREP)}$

Step 3: Source Node will store RREP Message with specific details in routing table. Source Node get RREP message Withcurrent time value and also store the timing for each arrival whose response received during specific time limit.

If (Arrival_Time<Spec_Time_Limit) Then
SN (RT)← IN $_{(RREP\{Current\_Time\ \})}$

Step 4: First preference will be given to the trusted node which can be selected based on repeated entry found in routing table. Source node will Check Repeated entry in CRRT for the particular Selecting Root.

Repeat_Entry←CRRT
If found (Repeated_Entry) then

 ISSN: 2454-4248
222 – 229

Select_Random_Route ← CRRT (Select the route randomly from the available route entry from CRRT)

Else

Select_Random_Route ← RT (Select Random route from RT)

End If;

IV. SIMULATION

A. *Simulation Parameters*

TABLE I. SIMULATION PARAMETERS

Parameters	Approach-1	Approach-2	Approach-3
Area	18000 × 12000 meter	5000 × 5000 meter	18000 × 12000 meter
Description	Real City Road map	Real City Road map	Real City Road map
No. Of Vehicle	300	100	1800
Simulation Time	4500 Sec	500 Sec	4500 Sec
Type of Vehicle	Car	Car	Car
Traffic Light Support	Yes	Yes	Yes
Type of Packet Send	UDP	UDP	UDP
Max. Speed of Vehicle	10/20/30 m/s	10/20/30 m/s	10/20/30 m/s
Length of Vehicle	3 meter	3 meter	3 meter
Safe Distance	Front and Rear -2 m	Front and Rear -2 m	Front and Rear -2 m
Allow Overtaking	Yes	Yes	Yes
No. of LAN of Road	2	2	2
Width of LAN	6m	6m	6m
Transmission of OBU	100 m	100 m	100 m
Transmission of RSU	250m	250m	250m
Routing Protocol	AODV	AODV	AODV
Simulator	SUMO 0.15.0, MOVE, NS2-2.34	SUMO 0.15.0, MOVE, NS2-2.34	SUMO 0.15.0, MOVE, NS2-2.34
Traffic model	CBR	CBR	CBR
Mobility Model	Random Waypoint Model	Random Waypoint Model	Random Waypoint Model

B. *Approaches with different scenario*

Here we have represented three approaches for blackhole prevention.

TABLE II. RESULT FOR APPROACH-1

Scenario	Loss (%)	Blackhole Loss (%)	Blackhole Loss under Preventive Mode (%)
Scenario-1	3.2774	41.4382	27.8515
Scenario-2	3.1846	40.8325	26.4134
Scenario-3	3.3704	39.0728	27.4412
Scenario-4	3.3613	40.4247	27.2420
Scenario-5	3.4448	41.8384	28.1664
Final Average	3.3277	40.7213	27.4229

In Approach-1, we taken the 300 vehicles and we run the simulation by considering the different parameters as given in Table-I. We run the system in three different ways. Firstly we run the simulation in simple way without presence of any malicious node and in it we have calculated loss of packets. After that we imposed blackhole attack in the same examples without any other modification by adding malicious nodes. To check the effect of malicious nodes we further calculated packet loss. In the result we found drastic change in packet loss due to blackhole attack in network. After that to check the effectiveness of Approach-1 "AODV_MSN-Maximum Sequence Number" under blackhole attack we run the same example with the implementation of Approach-1 and we found reduction in blackhole attack effect. We implemented the Approach-1 with the different scenario for checking the accuracy of result and we found it as per Table-II.

Result Analysis of Approach-1

We first run the simulation as simple case by using AODV protocol and we got the average packet loss 3.3277%. After that we run same scenario under Blackhole Attack and received Packet Loss 40.7213% and then we run the same scenario under Preventive Mode of Blackhole Attack and received packet Loss of 27.4229%. So from the above result we found that by adopting approach-1 we can reduce effect of blackhole attack by 13.2984%. Fig.2 is displaying the result of each scenario with different Packet Losses.

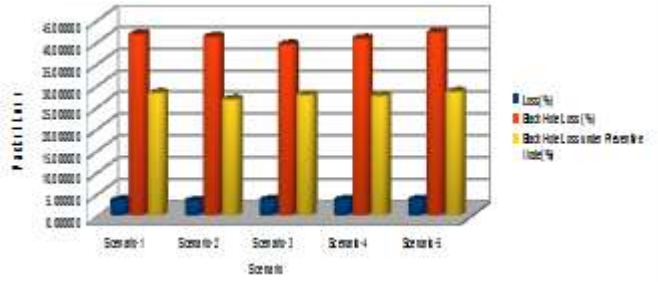

Figure 2. Result Analysis for Approach-1 for different Scenario

In Approach-2, we have taken 100 vehicles and we run the simulation by considering the different parameters as given in Table-I. We run the system in as the same ways as we run for Approach-1. Firstly we run the simulation in simple way without presence of any malicious node and in it we have calculated loss of packets as per Table-III. After that we imposed blackhole attack in the same examples without any other modification by adding malicious nodes for checking the effect of malicious nodes and we found Packet Loss as per Table-IV. After that to check the effectiveness of Approach-2"AODV_NAC"under blackhole attack we run the same example with the implementation of Approach-2and we found reduction in blackhole attack effect as per Table-V.

TABLE III. RESULT FOR APPROACH-2 WITHOUT BLACKHOLE ATTACK

Time	Sent Pkt	Recv. Pkt	Pkt Loss	Pkt Loss (%)	Total Packet Loss
0	0	0	0	0.0000	0
50	1572	1502	70	4.4529	70
100	1559	1493	66	4.2335	136
150	1507	1445	62	4.1141	198
200	1607	1539	68	4.2315	266

ISSN: 2454-4248
222 – 229

250	1632	1568	64	3.9216	330
300	1460	1408	52	3.5616	382
350	1431	1371	60	4.1929	442
400	1515	1449	66	4.3564	508
450	1607	1536	71	4.4182	579
500	1537	1484	53	3.4483	632
Total	15427	14795	632	3.7210	-

TABLE IV. RESULT FOR APPROACH-2 WITH BLACKHOLE ATTACK

Time	Sent Pkt	Recv. Pkt	Pkt Loss	Total Blackhole Packet Loss Pkt Loss (%)	Total Blackhole Packet Loss
0	0	0	0	0.0000	0
50	1530	133	1397	91.3072	1397
100	1523	118	1405	92.2521	2802
150	1481	115	1366	92.2350	4168
200	1573	143	1430	90.9091	5598
250	1583	111	1472	92.9880	7070
300	1432	107	1325	92.5279	8395
350	1391	136	1255	90.2229	9650
400	1469	141	1328	90.4016	10978
450	1576	89	1487	94.3528	12465
500	1577	94	1483	94.0393	13948
Total	15135	1187	13948	92.1573	-

TABLE V. RESULT FOR APPROACH-2 WITH BLACKHOLE PREVENTIVE MODE

Time	Sent Pkt	Recv. Pkt	Pkt Loss	Total Blackhole Packet Loss in Preventive Mode Pkt Loss (%)	Total Blackhole Packet Loss in Preventive Mode
0	0	0	0	0.0000	0
50	1593	125	1468	92.1532	1468
100	1583	138	1445	91.2824	2913
150	1525	875	650	42.6230	3563
200	1616	1536	80	4.9505	3643
250	1646	1578	68	4.1312	3711
300	1472	1398	74	5.0272	3785
350	1450	1387	63	4.3448	3848
400	1525	1436	89	5.8361	3937
450	1625	1544	81	4.9846	4018
500	1639	1577	62	3.7828	4080
Total	**15674**	**11594**	4080	26.0304	-

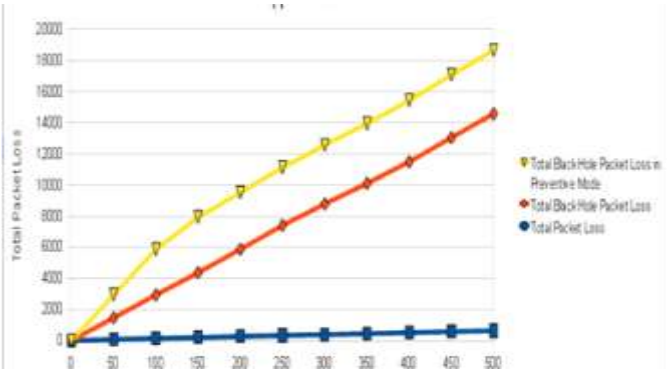

Figure 3. Analysis for Approach-2 under each case

We analyzed the Packet loss based on time for each case like Simple scenario without any Blackhole attack, With Blackhole attack and Blackhole Preventive mode as per Table-VI.

TABLE VI. TIMEWISE RESULT FOR APPROACH-2

Time	Avg. Pkt Loss (%)	Avg. Blackhole Packet Loss (%)	Avg. Blackhole Packet Loss in Preventive Mode (%)
0	0.00000	0.00000	0.00000
50	4.17243	92.01297	91.83765
100	4.03609	92.41606	91.34235
150	4.17375	92.31419	46.77246
200	4.35446	90.72638	5.08313
250	4.24037	92.72950	3.63826
300	4.06156	92.31598	4.59051
350	4.30123	90.59314	4.45296
400	4.25147	90.84654	4.82209
450	3.98035	94.01861	4.62314
500	3.67509	94.02553	4.12076
Average	**4.12468**	**92.19989**	**26.12833**

Result Analysis of Approach-2

We first run the simulation as simple case by using AODV protocol and we got the average packet loss 4.12468%. After that we run same scenario under Blackhole Attack and received Packet Loss 92.19989% and then we run the same scenario under Preventive Mode of Blackhole Attack and received packet Loss of 26.12833%. So from the above result we found that by adopting approach-2 we can reduce effect of blackhole attack by 66.07156%. Fig. 4 is displaying the result of each scenario with different Packet Losses.

 ISSN: 2454-4248
222 – 229

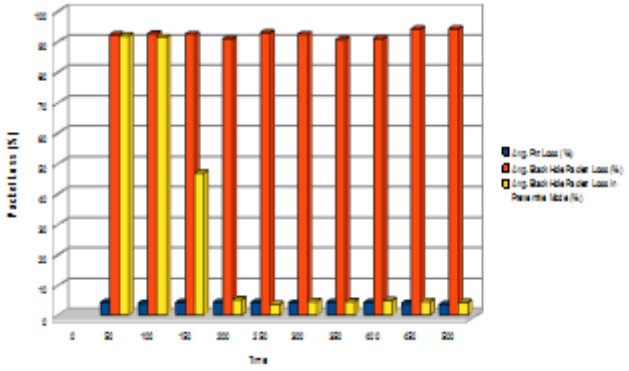

Figure 4. Result Analysis for Approach-2 for different Scenario

In Approach-3, we have taken 1800 vehicles and we run the simulation by considering the different parameters as given in Table-I. We run the system in as the same ways as we run for Approach-1. Firstly we run the simulation in simple way without presence of any malicious node and in it we calculated loss of packets as per Table-VII. After that we imposed blackhole attack in the same examples without any other modification by adding malicious nodes for checking the effect of malicious nodes and we found Packet Loss as per Table-VIII. After that to check the effectiveness of Approach-3"AODV_TP" under blackhole attack we run the same example with the implementation of Approach-3 and we found reduction in blackhole attack effect as per Table-IX.

TABLE VII. RESULT FOR APPROACH-3 WITHOUT BLACKHOLE ATTACK

Time	Sent Pkt	Recv. Pkt	Pkt Loss	Pkt Loss (%)	Total Packet Loss
0	0	0	0	0.0000	0
500	131040	121512	9528	7.2711	9528
1000	129885	122889	6996	5.3863	16524
1500	127580	119607	7973	6.2494	24497
2000	129790	121729	8061	6.2108	32558
2500	127995	120115	7880	6.1565	40438
3000	126695	117664	9031	7.1281	49469
3500	123280	113825	9455	7.6695	58924
4000	136210	126258	9952	7.3064	68876
4500	72875	67437	5438	7.4621	74314
Total	**1105350**	**1031036**	74314	6.7231	

TABLE VIII. RESULT FOR APPROACH-3WITH BLACKHOLE ATTACK

Time	Sent Pkt	Recv. Pkt	Pkt Loss	Pkt Loss (%)	Total Blackhole Packet Loss
0	0	0	0	0	0
500	131276	4668	126608	96.4441	126608
1000	129621	4149	125472	96.7991	252080
1500	128938	4027	124911	96.8768	376991
2000	128806	5705	123101	95.5709	500092
2500	125153	3905	121248	96.8798	621340
3000	127164	3752	123412	97.0495	744752
3500	129825	4759	125066	96.3343	869818
4000	138432	4942	133490	96.4300	1003308
4500	70156	2628	67528	96.2541	1070836
Total	**1109371**	**38535**	1070836	96.5264	

TABLE IX. RESULT FOR APPROACH-3 WITH BLACKHOLE PREVENTIVE MODE

Time	Sent Pkt	Recv. Pkt	Pkt Loss	Pkt Loss (%)	Total Blackhole Packet Loss in Preventive Mode
0	0	0	0	0	0
500	131926	111197	20729	15.7126	20729
1000	133359	111122	22237	16.6745	42966
1500	131193	108489	22704	17.3058	65670
2000	131675	110834	20841	15.8276	86511
2500	130259	110709	19550	15.0086	106061
3000	127745	106072	21673	16.9658	127734
3500	125745	102756	22989	18.2822	150723
4000	138003	113142	24861	18.0148	175584
4500	70156	57879	12277	17.4996	187861
Total	**1120061**	**932200**	187861	16.7724	

We analyzed the Packet loss based on time for each case like Simple scenario without any Blackhole attack, With Blackhole attack and Blackhole Preventive mode as per Table-X.

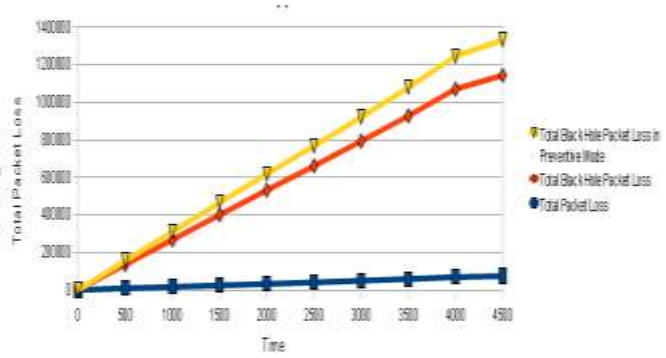

Figure 5. Result Analysis for approach- 3

TABLE X. TIMEWISE RESULT FOR APPROACH-3

Time	Avg. Pkt Loss (%)	Avg. Blackhole Packet Loss (%)	Avg. Blackhole Packet Loss in Preventive Mode (%)
0	0	0	0
500	6.836	96.4189	16.6866
1000	6.1169	96.7049	16.7327
1500	6.3862	96.7616	16.8955
2000	6.3366	95.4815	16.2033
2500	6.1296	96.8802	16.6356
3000	6.5429	96.7787	16.7261
3500	7.3108	96.0355	16.665
4000	7.3414	96.1609	16.6628
4500	7.3358	96.4186	17.1591
Average	6.704	96.4045	16.7074

 ISSN: 2454-4248
222 – 229

Result Analysis of Approach-3

We first run the simulation as simple case by using AODV protocol and we got the average packet loss 6.7040%. After that we run same scenario under Blackhole Attack and received Packet Loss 96.4045% and then we run the same scenario under Preventive Mode of Blackhole Attack and received packet Loss of 16.7074%. So from the above result we found that by adopting approach-3 we can reduce effect of black hole attack by 79.6971%. Fig. 6is displaying the result of each scenario with different Packet Losses.

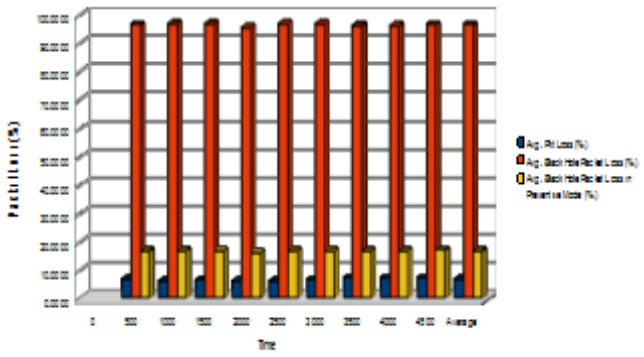

Figure 6. Result analysis for Approach-3 for different Scenario

V. CONCLUSIONS

After In this paper we propose an effect of black hole attack and its preventive solutions in VANETs. We have implemented different preventive solutions and simulated the scenarios using simulation. From the results we can conclude that by adopting different preventive solution suggested here, we can reduce the effect of black hole attack. Table XI is representing comparative analysis of each approach. By adopting approach-1 which is based on Maximum Sequence Number, we get the reduction effect in black hole attack is 13.2984%, by approach-2 which is based on Neighbor Awareness Count, we get it 66.0716% and by adopting approach-3 which is based on Trusted Path, we get the reduction of 79.6971%. So based on that we can say that approach-3 AODV_TP –Trusted Path is providing more secure solution compare to other implemented approaches.In this paper we have considered homogeneous vehicles and assumed that all the vehicles are VANET enabled. In future, we plan to analyze overhead on each vehicle for each approach and reduce that overhead by transferring some responsibilities to RSU.

TABLE XI. CONCLUSION TABLE

	Average packet loss (%)	**Black Hole Packet Loss (%)**	**Black Hole Packet Loss under Preventive Mode (%)**	**Reduction in Black hole Effect (%)**
Approach-1 (AODV_MSN)	3.3277%	40.7213%	27.4229%	13.2984%
Approach-2 (AODV_NAC-Neighbor Awareness Count)	4.1247%	92.1999%	26.1283%.	66.0716%
Approach-3 (AODV_TP-Trusted Path)	6.7040%	96.4045%	16.7074%.	79.6971%.

REFERENCES

[1] Vimal Kumar , Rakesh Kumar., *"An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network,"* in Procedia Computer Science 48 (2015) 472 – 479,International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014) , ScienceDirect- Published by ELSEVIER 1877-0509 2015

[2] Irshad Ahmed Sumra, HalabiHasbullah, Iftikhar Ahmad, Jamalul-lail bin Ab Manan "*Forming Vehicular Web of Trust in VANET*" in 978-1-4577-0069-9/11/2011 IEEE

[3] Saurabh Gupta, SubratKar , S Dharmaraja "*BAAP: Blackhole Attack Avoidance Protocol for Wireless Network* " in International Conference on Computer & Communication Technology (ICCCT)-2011, 978-1-4577-1386-611, 2011 IEEE

[4] SisilySibichen, SreelaSreedhar, "An Efficient AODV Protocol and Encryption Mechanism for Security Issues in Adhoc Networks" in International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013) 978-1-4673-5149-2/13/$31.00 ©2013 IEEE

[5] P. R. Jasmine Jeni , A. V imala Juliet , R.Parthasarath, A.Messiah Bose, "*Performance Analysis of DOA and AODV Routing Protocols with Black Hole Attack in MANET*" in 2013 International Conference on Smart Structures & Systems (JCSSS-20 13), March 28 - 29, 2013, Chennai, INDIA, 978-1-4673-6240-5/32 $ 31.00 ©2013 IEEE

[6] Satria Mandala, Abdul Hanan Abdullah, Abdul Samad Ismail, HabibollahHaron, Md. AsriNgadi, YahayaCoulibaly, "*A Review of Blackhole Attack in Mobile Adhoc Network* " in 2013 3rd International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME) 339Bandung, November 7-8, 2013, 978-1-4799-1650-4/13/$31.00/©2013 IEEE

[7] Ms Monika Y. Dangore , Mr Santosh S. Sambare "*Detecting And Overcoming Blackhole Attack In Aodv Protocol*" in 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, 978-0-4799-2235-2/13 $26.00 © 2013 IEEE

[8] Vani A. Hiremani ,Manisha MadhukarJadhao "*Eliminating Co-operative Blackhole and Grayhole Attacks Using Modified EDRI Table in MANET*", 978-1-4673-6126-2/13/$31.00©2013 IEEE

[9] HichemSedjelmaci and Sidi Mohammed Senouci, "*A New Intrusion Detection Framework for Vehicular Networks*", IEEE ICC 2014 - Ad-hoc and Sensor Networking Symposium, 978-1-4799-2003-7/14/$31.00 ©2014 IEEE

[10] Raghad Baiad, HadiOtrok, Sami Muhaidat, Jamal Bentahar "*Cooperative Cross Layer Detection for Blackhole Attack in VANET-OLSR*" , 978-1-4799-0959-9/14/$31.00 ©2014 IEEE

[11] Yu-Chih Wei & Yi-Ming Chen "*Adaptive Decision Making for Improving Trust Establishment in VANET*", IEICE - Asia-

 ISSN: 2454-4248
222 – 229

Pacific Network Operation andManagement Symposium (APNOMS) 2014

[12] Shiang-Feng Tzeng, Shi-Jinn Horng, Tianrui Li, Xian Wang, Po-Hsian Huang, and MuhmmadKhurram Khan "*Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET*", VT-2014-00658, 10.1109/TVT.2015.2406877, IEEE Transactions on Vehicular Technology 0018-9545 (c) 2015 IEEE.

[13] Prathima P, Kishore Rajendiran, Shri Ranjani G, Preethi Kurian, Swarupa S "*Simple and Flexible Authentication Framework for Vehicular Ad hoc Networks*", IEEE ICCSP 2015 conference, 978-1-4799-8081-9/15/$31.00 © 2015 IEEE

[14] Wenjia Li, and Houbing Song, "*ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks*", IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 17, NO. 4, APRIL 2016, 1524-9050 © 2015 IEEE.