IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-11 E-ISSN: 2347-2693

Blackhole Attack and its effect on VANET

Ajay N. Upadhyaya[1*], J.S. Shah [2]

[1*] Dept. of Computer Engineering, Faculty of Technology, RK University, Rajkot, India
[1]L.J. Institute of Engineering & Technology, GTU, Ahmedabad, India
[2]Dept. of Computer Engineering, Ex. Principal, Government Engineering College, Patan, India

[*]*Corresponding Author: ajay8586g@gmail.com, Tel.: +91-9909715620*

Available online at: www.ijcseonline.org

Received: 13/Oct/2017, Revised: 25/Oct/2017, Accepted: 14/Nov/2017, Published: 30/Nov/2017

***Abstract*—** VANET is one type of adhoc networks which established among vehicles equipped with communication facilities. In VANETs vehicles are equipped with device known as on Board Unit (OBU) through which it can communicate with other vehicles as well as with infrastructure which is known as Road Side Unit (RSU). VANET can be used for different applications like Life-Critical Safety Applications, Safety warning Applications, Electronic Toll Collections, Internet Access in vehicles, Vehicle Group Communications, Roadside Services Finder and many more. Various researchers are proposing different solutions in VANET for Protocols, Effective Service Parameters, Smart Network challenges and lot more by seeing the usefulness of VANETs in various applications but security is a main issue for adopting VANET as a life critical solution. Security is the major concern for various VANET applications where a wrong, replicated or delayed messages may directly or indirectly affect the human lives. Many of the applications require a high level of security in VANET adoption. Security Attacks on VANET can be categories in Routing Attack, Monitoring Attack, Social Attack, Timing Attack, Application Attack and Network Attack. In this paper we focused on Routing Attack detection, specifically Blackhole Attack detection methodologies. We have proposed four different approaches for Blackhole attack detection: Neighborhood based, Sequence Number based, Packet Drop rate based and Cluster Forming based. We analyze the performance of the proposed approaches for different scenario with comparative analysis.

Keywords—Blackhole Attack Detection, AODV, Neighborhood based blackhole detection, Sequence Number based blackhole detection, Packet Drop rate based blackhole detection, Cluster Forming based blackhole detection

I. INTRODUCTION

Routing in VANET is a challenging task due to its high mobility & frequent link disruption topology. A malicious node may spoof, modify or block valid routing protocol messages and spread corrupt or update routing information inside network which might result in redirection of some or all network traffic, connectivity problems, excessive bandwidth consumption and potential denial of service. It creates the need to design secure Framework for managing authenticity and reliability of messages. [3] There are various kinds of Routing attack that can affect the entire system or can degrade the performance of system. Here we mainly discussed about routing attacks which can be categorized into three types: Blackhole attack, Wormhole Attack and Grayhole attack. In Blackhole attack, the malicious node firstly attracts the other nodes to transmit the packet through itself by sending a route reply with shortest route. After attracting the node, when the packet is forwarded through this malicious node, it silently drops the packet and creates the effect like blackhole. In Wormhole Attack an attacker records packets at one location in the network and tunnels them to another location, retransmitting them into the VANET network. Wormhole nodes send a fake route which is a shorter than the original available one in the network. Attacker will try to confuse the routing mechanism which is completely relying on the knowledge of node distance. In such attack one or more node creates the virtual tunnel inside VANET network and tries to disturb the network by capturing a packet from one location and transmit them at other location. In Grayhole attack, malicious node drop packets of a particular node or set of nodes for a specific period of time. Selection of such victim nodes and time is decided randomly. It is difficult to detect such type of attack because of changeable behavior of malicious nodes. In this paper, we have focused on Blackhole attack in details. In blackhole attack, the malicious node firstly attracts the other nodes for transmit the packet through itself by sending Route Reply messages having forged optimal path details. Such kind of optimality can be generated by showing less hop count. Now after finding optimal path other nodes of network will attract to transmit their data through malicious node. Malicious node silently drop messages and create the effect of blackhole. 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.

Figure 1 illustrates an example where Car-A wants to send data packets to Car-E AND Car-G but it doesn't having any route details for both. Therefore, Car-A initiates the route discovery process and RREQ is forwarded to Car-B and Car-H. As a malicious node, Car-H will claim that it is having shortest route to reach at Car-E and Car-G. Based on available reply, Car-A will send all messages to Car-H and becomes the victim of blackhole attack.

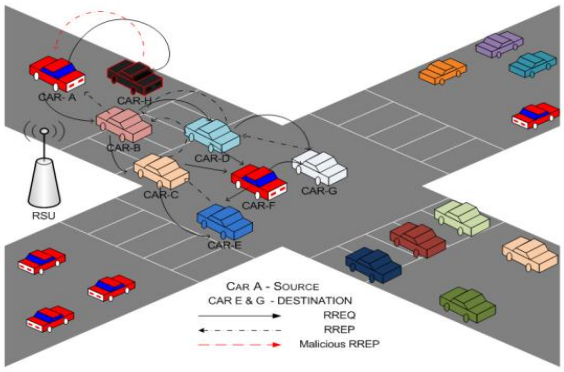

Figure 1. Blackhole Attack in VANET

Work of this paper is mainly divided into four logical parts and we named it as aprroch-1, 2, 3 and 4. In approach-1 we will discuss about blackhole attack detection using Neighborhood based methodology. For approach-2 we will use Sequence Number based blackhole detection methodology and for approach-3 we will use Packet Drop rate based blackhole detection methodology and lastly we will discuss Cluster Forming based Blackhole detection methodology in approach-4.

II. RELATED WORK

In VANET are self-organizing networks established among vehicles equipped with communication facilities. VANET are specially design for nodes having high mobility with unbounded network structure and want to communicate time critical information in a secure way. Secure communication is a basic requirement for the usability and adoptability of VANET. In the recent research work different researcher have proposed different solutions for the domain of blackhole attack. In recent research work [2], the author presented survey of security attacks in VANETs and discussed possible future security attacks with critical analysis and future research possibilities. In [2], the author represented the implementation of grayhole attack and shown the impacts of it on VANET. In [5], [6], [9] and [11], different solutions are proposed for detecting blackhole attacks. In research work [7], the author proposed solution for AODV enhancement by managing the Coming Route Reply table (CRRT), lifetime, sequence number and hop count of packet. In research work [8] author presented the studies of the effect of blackhole attack in AODV based network by considering the different parameters like Throughput, Packet Delivery Ratio and Average End to End Delay for different scenario. In [10], the author discussed about experimental analysis of misbehavior detection and prevention in VANET and shown internal attack detection, blocking and preventing false driver warning. In [12], author proposed cluster based solutions by defining the cluster and responsibilities to detect malicious node is given to cluster coordinator. In [14], author presented the detail survey on node Misbehavior and also discussed different detection techniques in VANET.

III. PROPOSED APPROACH

Here we will discuss about implementation of four different approaches for Blackhole detection. We have taken AODV routing protocol for first three approach and DSR for last approach. Here we will discuss about algorithm, Implementation, Result and conclusion of each approach.

Approach- 1 is based on blackhole attack detection using the awareness of neighbor. It is named as "Neighborhood based blackhole detection". In said approach every node will take care for their neighbors. Neighbor maintains the list of Trusted nodes and Non-trusted nodes. Neighbor node will observe the incoming and outgoing traffic for individual node. Neighbor node will maintain two counters SEND_PKT and RCV_PKT. If the difference between two counter values reaches to threshold value (Th) then particular node will be declared as a malicious node. Initially all nodes will be assumed to be Trusted Nodes and get the entries in the list of Trusted Node. But after declaring as a malicious node it will be deleted from the trusted list and added into Non-Trusted List.

Algorithm: Here we will discuss blackhole detection method using the Neighborhood based approach. We had taken some of the notation like SN for Source Node, DN for Destination Node, SN_ID for Source Node ID,DN_ID for Destination Node ID, MN for Malicious Node, MN_ID for Malicious Node ID, SEND_PKT for Number of packet sent by particular node, RCV_PKT for Number of packet received by particular node, NN for Neighbour Node, EN for Each node, List_Trusted_Node having personal list of trusted node, List_Non-Trusted_Node having personal list of Non-trusted nodes, RSU for Road Side Unit, Block_Node_List for the list of nodes which are blacklisted by RSU, RREQ for Route Request, RREP for Route Reply.

Step 1: Initially source node, which is unaware about the position of destination node broadcast Route Request Message (RREQ). Route Request is broadcasted with the source Node ID, Destination Node ID, Source Node Sequence No and Broadcast ID.

SN → RREQ [SN_ID, DN_ID, SN_SEQ_NO, BROD_ID]

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

SN ← RREP [DN_ID, SN_ID, DN_SEQ_NO, HOP_COUNT, LIFE_TIME]

Step 3: Initially all neighbour nodes will be consider as a Trusted Nodes, List_Trusted_Node will store Node_Id of its neighbours.

Create Trust_Node_List ( )

{

SN [List_Trusted_Node] ← NN[N_ID]

SN [List_Non_Trusted_Node] ← null

}

Step 4: For detecting malicious node, neighbour node will continuously examine in and out data transmission of each node. If the difference is found higher than the threshold value (Th) then particular node will be recognise as a malicious node. Threshold value will be decided based on current average drop rate of network.

Detect Malicious Node ( )

{

Th ← AVG (Pkt_Drop_Rate)/2;

For Each (NN)

{ **If** (Diff (NN_SEND_PKT, NN_RCV_PKT) > Th) **then**

NN = MN

Update_Trust__Node_List ( )

{ SN [List_Trusted_Node] ← Remove (NN[N_ID])

SN [List_Non_Trusted_Node] ← Add (NN[N_ID]) }

End if } }

Step 5: After managing the list of trusted and non trusted nodes, every node will send their non trusted node list to respective RSU. RSU will collect list of all Non-trusted node list from each node inside the range and based on that prepare the block node list. This block node list will be forwarded to each node in the range of RSU.

Manage Block_node_List( )

{

RSU[Block_Node_List] ←

SN [SN_ID, List_Non_Trusted_Node] }

EN ← RSU [Block_Node_List]

Step 6: All Nodes will update Trusted and non trusted Node list based on the updates given by RSU.

Update_Trust_Node_List ( )

{

SN [List_Trusted_Node] ← Remove (MN[MN_ID])

SN [List_Non_Trusted_Node] ← Add (MN[MN_ID])}

Approach - 2 is mainly based on the concept of Identification of higher Sequence Number. It is named as "Sequence Number based blackhole detection". In said approach every node will maintain the list of Trusted nodes and Non-trusted nodes. If source node will receive reply from any node with largest sequence number then it will be considered as a malicious node. As discussed in apperoach-1 initially all nodes will be considered as trusted nodes and if such malicious node found then remove it from trusted node list and then add it into Non-trusted node list.

Algorithm: Here we will discuss blackhole detection method using the sequence number identification method. We had taken some other notation then approach-1 like SN_SEQ for Source Sequence Number, DN_SEQ for Destination Sequence Number, RT for Routing Table.

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

SN → RREQ [SN_ID, DN_ID, SN_SEQ_NO, BROD_ID]

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

SN ← RREP [DN_ID, SN_ID, DN_SEQ_NO, HOP_COUNT, LIFE_TIME]

Step 3: Initially all neighbour nodes will be consider as a Trusted Nodes, List_Trusted_Node will store Node_Id of its neighbours.

Create Trust_Node_List ( )

{

SN [List_Trusted_Node] ← NN[N_ID]

SN [List_Non_Trusted_Node] ← null }

Step 4: If source node receives any route reply with very larger Sequence Number then particular node, will be treated as malicious node.

RREP_CHECK ()

{

For each (NN (RREP))

{ **If** (DN_SEQ>>>=SN_SEQ) **then**

DN = MN

Update_Trust__Node_List ()

{SN [List_Trusted_Node] ← Remove (DN[N_ID])

SN [List_Non_Trusted_Node] ← Add (DN[N_ID])}

End if

} }

Step 5: After managing the list of trusted and non trusted nodes, every node will send their non trusted node list to respective RSU. RSU will collect list of all Non-trusted node list from each node inside the range and based on that prepare the block node list. This block node list will be forwarded to each node in the range of RSU.

Manage Block_node_List()

{

RSU [Block_Node_List] ← SN [SN_ID, List_Non_Trusted_Node] }

EN ← RSU [Block_Node_List]

}

Step 6: All Nodes will update Trusted and non trusted Node list based on the updates given by RSU.

Update_Trust_Node_List ()

{

SN [List_Trusted_Node] ← Remove (MN[MN_ID])

SN [List_Non_Trusted_Node] ← Add (MN[MN_ID])

}

Approach-3 is based on packet drop. It is named as "Packet Drop rate based blackhole detection". In said approach RSU is having a responsibility to detect malicious node. RSU will manage List of Trusted node and Non-Trusted node. At regular interval of time, RSU will calculate packet drop rate, If found that packet drop rate is more than the threshold value then RSU will declare that it is Blackhole Attack. RSU will collect details of transmission from each node, in which each node has to send details of nodes to which node they transmitted data in last time span. Based on the collected details, RSU will check the repeated entry for a particular node. RSU will consider particular node as a suspected node and declared all nodes not to send any data to or through particular node for a specific period of time. RSU will also calculate the Packet drop rate for next time span. If reduction is found in packet drop rate then decision is taken that suspected node is a malicious node and permanently block that node in the network and same details is forwarded to all other RSU. If improvement is not found in packet drop rate then RSU will search the other node which is repeated in the list with the same manner.

Algorithm: Here we will discuss blackhole detection method using the packet drop rate method. We had taken some other notation along with approach-1 like PDR for Packet Drop Rate, Next_Node for Next node to whom data is transmitted, Th_PDR for Threshold value for Packet drop rate, Check_Point_Time for the period of time after which calculation is done for packet drop, Check_List for managing the list of next node details forwarded by each node to RSU, Suspected_Node for node which will be treated as suspected node.

Step 1: Here we have to identify the value for check point timer, after that particular time whole procedure is repeated. By considering Total time 500 sec we take here 100 sec for check point timer. Initially all nodes in the range will be consider as a Trusted Nodes.

Create Trust_Node_List ()

{ {

RSU[List_Trusted_Node] ← NN[N_ID]

RSU [List_Non_Trusted_Node] ← null }

SET Check_Point_Time → 100 Sec}

Step 2: After each check point time span, RSU will calculate PDR. If Packet drop rate is higher than threshold value then transmission details is collected from each node for the last time span.

For each(N_ID)

{

Calculate_PDR ()

{ PDR= Total no. of packets send – Total no. of packets received. **}**

If (PDR>TH_PDR) **then**

RSU [Check_List] ← Add(N_ID)

End if }

Step 3: After preparing Check list, RSU will search the node which is having highest PDR and consider that particular node as suspected node.

Detect Suspected Node ()

{ **If** (PDR=Max (PDR) **then**

Node=Suspected_Node

End if }

Step 4: After identifying suspected node send its details to each node inside the range of RSU and inform them not to transmit any of their packet from suspected node for the time period of (2* Check_Point_Time) for avoiding loss. Up to this, suspected node is not identified as a malicious node so such mechanism is adopted. If suspected node is victim node then automatically it becomes eligible for transmission after two checkpoint time span and if it founds guilty then it will be block permanently from the network.

Declare Blocking of Suspected Node ()

{ RSU (N_ID,2* Check_Point_Time) → EN **}**

Step 5: After doing declaration of suspected node, calculate PDR further for the time of last span. If it found less than the threshold value then consider suspected node as a malicious

node and send this information to all nodes inside the network and other RSU and if it is not less than the threshold value then repeat from Step 4.

For each(N_ID)

{

Re_Calculate_PDR ()

{ PDR= Total no. of packets send – Total no. of packets received. **}**

If (PDR<TH_PDR) **then**

Node = MN

Update_Trust__Node_List ()

{ RSU [List_Trusted_Node] ← Remove (Node[N_ID])

RSU [List_Non_Trusted_Node] ← Add (Node[N_ID])}

Else

RSU[Check_List] ← Remove(N_ID)

End if

}

Approach-4 is based on blackhole detection based on Cluster mechanism. It is named as "Cluster Forming based Blackhole detection". In said approach RSU is having a responsibility to detect malicious node. RSU will randomly select some of the nodes as a cluster head based on their position inside the network. After identifying different cluster and cluster head, RSU will broadcast checking message to each and every node via cluster head node which will be return back through cluster head node using reverse path methodology. Now after receiving such message malicious node will drop it and message will not forward to further. RSU will prepare the list which nodes have not forwarded such message and based on it malicious node can be easily detected from the network. Directly decision is not taken but after identifying the particular node consider it as suspected node and send some messages again to suspected node and if found the same packet drop then decision is taken that suspected node is malicious node. To reduce the load on network, RSU will randomly apply such method on specific region of network. Here we have used DSR (Dynamic Source Routing) Protocol which is having different functionalities compare to AODV (Ad hoc On Demand distance Vector). AODV data packets carry the destination address, whereas in DSR, data packets carry the full routing information. Another difference is that in AODV, route reply packets carry the destination address and the sequence number, whereas, in DSR, route reply packets carry the address of each node along the route.

Algorithm: Here we will discuss blackhole detection method using the cluster mechanism. We had taken some other notation along with approach-1 like CH- Cluster Head.

Step 1: RSU will divide total area into different cluster and decide cluster head for each. Selection of cluster head is done on random bases. Initially all nodes will be consider as a Trusted Nodes, List_Trusted_Node will store Node_Id and Cluster_ID.

Create Trust_Node_List ()

{

RSU [List_Trusted_Node] ← Node[N_ID, Cluster_ID]

RSU [List_Non_Trusted_Node] ← null

}

Create Cluster Head ()

{

For each (Cluster_ID)

{ CH ← RSU (Random (List_Trusted_Node)) **}**

}

Step 2: After identifying cluster head, RSU will send message to Cluster head and Cluster Head will forward this message to each node in his cluster.

Send Msg Request()

{ RSU [RREQ] → CH(Cluster_ID)

CH [RREQ] → EN(N_ID, Clsuter_ID) }

Step 3: Now each node has to give the reply with the details of node_id via reverse path methodology in which node will send message to cluster head and which later it will be forwarded to RSU.

Send Msg Reply ()

{ Node [ID, Cluster_ID, RREP] → CH

CH<N_ID,Cluster_ID] → RSU **}**

Step 4: RSU will identify the list of nodes which not gave such response. RSU will consider particular node as a suspected node and send other message with the same manner for checking the activities of suspected node.

Check Reply ( )

{ If (N_Id(send_msg_req) not in(send_msg_rep)) then

Node=Suspected_Node

Observe (Suspected_Node)

End if }

Step 5: After detecting the same activities again, RSU will declare particular suspected node as a malicious node.

If Found **then**

Node = MN

Update_Trust__Node_List ()

{ RSU [List_Trusted_Node] ← Remove (Node[N_ID])

RSU [List_Non_Trusted_Node] ← Add (Node[N_ID]) }

Else

RSU[Check_List] ← Remove(N_ID)

End if

IV. SIMULATION AND DISCUSSION

A. Simulation Parameters

TABLE I. SIMULATION PARAMETERS

Parameters	Approaches			
	1	2	3	4
Area	5000 × 5000 meter			
Description	Real City Road map			
No. Of Vehicle	100			
Simulation Time	500 Sec			
Type of Vehicle	Car			
Traffic Light Support	Yes			
Type of Packet Send	UDP			
Max. Speed of Vehicle	10/20/30 m/s			
Length of Vehicle	3 meter			
Safe Distance	Front and Rear -2 m			
Allow Overtaking	Yes			
No. of LAN of Road	2			
Width of LAN	6m			
Transmission of OBU	100 m			
Transmission of RSU	250m			
Routing Protocol	AODV	AODV	AODV	DSR
Simulator	SUMO 0.15.0, MOVE, NS2-2.34			
Traffic model	CBR			
Mobility Model	Random Waypoint Model			

B. Approaches with their outcome

Here we have represented four approaches for blackhole detection. In Approach-1, we have taken 100 vehicles and we run the simulation by considering the different parameters as given in Table-I. First we run the simulation in simple way then we run the simulation with the effect of malicious node and then we run the simulation with different blackhole detection approaches.

In Table-II, we presented the result of approach-1 of Neighborhood based blackhole detection. Here we presented Average packet loss in simple mode, Average packet loss in the effect of blackhole attack and Average packet loss under Neighborhood based detection in a time slot of 50 second for the total duration of 500 second. Initially in simple condition we received 3.7791% Packet loss which is increased under blackhole attack and reached to 80.0733% and with the implementation of Neighborhood based detection approach we can reduce the packet loss and finally received 27.7830% Packet loss. Figure 2 is a graphical presentation of Table-II for understanding the effectiveness of approach-1.

TABLE II. RESULT FOR APPROACH-1 – NEIGHBORHOOD BASED BLACKHOLE DETECTION

Time	Avg. Pkt Loss in Simple Mode (%)	Avg. Packet Loss under Blackhole Attack (%)	Average packet loss under Neighborhood based Detection (%)
0	0.0000	0.0000	0.0000
50	2.9703	86.6234	73.8065
100	3.4704	87.2327	53.0519
150	3.6554	87.5000	45.2335
200	4.0989	86.2758	40.5778
250	4.5137	90.1887	31.8528
300	4.3934	88.6816	26.7925
350	5.5234	89.1492	16.5572
400	4.4888	88.1013	8.0445
450	4.0252	88.3049	5.5877
500	4.4304	88.7483	4.1087
Average	**3.7791**	**80.0733**	**27.7830**

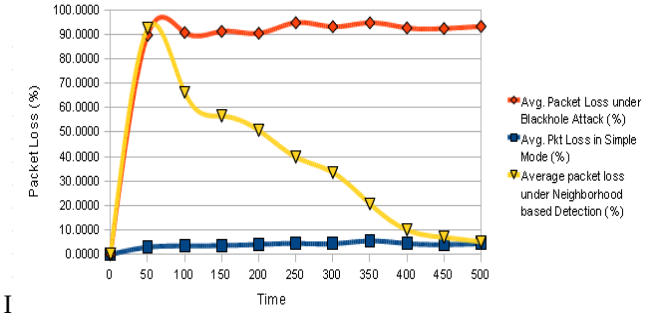

Figure 2. Analysis for Approach-1 under each case

In Table-III, we presented the result of approach-2 of Sequence number based blackhole detection. Same as approach-1, here we presented Average packet loss in simple mode, Average packet loss in the effect of blackhole attack and Average packet loss under Sequence number based blackhole detection in a time slot of 50 second for the total duration of 500 second. Initially in simple condition we received 3.7679% Packet loss which is increased under blackhole attack and reached to 80.0252% and with the implementation of Sequence number based detection approach we can reduce the packet loss and finally received 39.7906% Packet loss. Figure 3 is a graphical presentation of Table-III for understanding the effectiveness of approach-2.

TABLE III. RESULT FOR APPROACH-2 – SEQUENCE NUMBER BASED BLACKHOLE DETECTION

Time	Avg. Pkt Loss in Simple Mode (%)	Avg. Packet Loss under Blackhole Attack (%)	Average packet loss under Sequence number based Detection (%)
0	0.0000	0.0000	0.0000
50	3.2279	89.4366	82.4204
100	4.2969	87.2368	65.5790
150	3.4618	88.1727	57.5130
200	3.6770	85.6771	53.5602
250	3.9795	88.8962	49.0637

300	4.9544	85.0336	41.2821
350	4.8512	90.1119	33.9908
400	4.6388	87.8676	21.0352
450	3.7290	89.4631	18.3893
500	4.6302	88.3812	14.8631
Average	**3.7679**	**80.0252**	**39.7906**

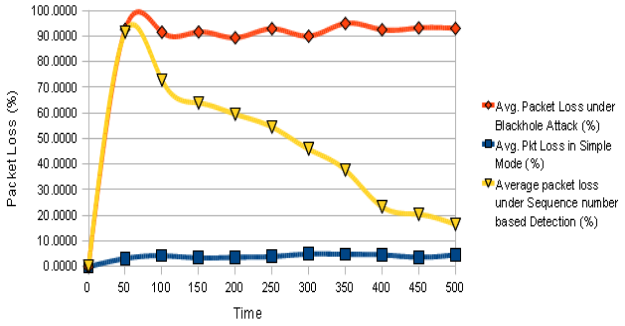

Figure 3. Analysis for Approach-2 under each case

In Table-IV, we presented the result of approach-3 of Packet drop rate based blackhole detection. Initially in simple condition we received 3.8151% Packet loss which is increased under blackhole attack and reached to 80.0484% and with the implementation of Packet drop rate based detection approach we can reduce the packet loss and finally received 44.6563% Packet loss. Figure 4 is a graphical presentation of Table-IV for understanding the effectiveness of approach-3.

TABLE IV. RESULT FOR APPROACH-3 – PACKET DROP RATE BASED BLACKHOLE DETECTION

Time	Avg. Pkt Loss in Simple Mode (%)	Avg. Packet Loss under Blackhole Attack (%)	Average packet loss under packet drop rate based Detection (%)
0	0.0000	0.0000	0.0000
50	3.7158	88.8962	84.0078
100	3.7402	88.9594	67.9949
150	3.6122	90.8138	62.2715
200	4.4726	86.0656	59.4560
250	4.9748	85.5959	54.6944
300	4.4888	89.7436	44.9770
350	4.8562	88.8539	38.8356
400	4.1035	88.7186	30.7057
450	4.1775	87.7837	26.6497
500	3.8241	85.1020	21.6267
Average	**3.8151**	**80.0484**	**44.6563**

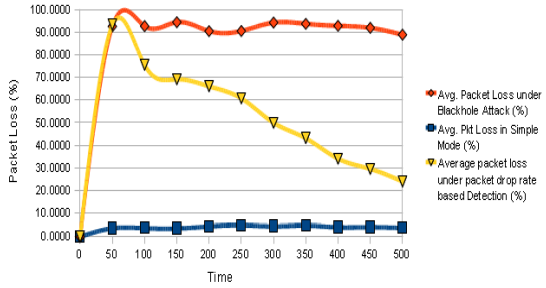

Figure 4. Analysis for Approach-3 under each case

In Table-V, we presented the result of approach-4 of cluster forming based blackhole detection. Initially in simple condition we received 3.7859% Packet loss which is increased under blackhole attack and reached to 80.0647% and with the implementation of Cluster Forming based detection approach we can reduce the packet loss and finally received 36.5737% Packet loss. Figure 5 is a graphical presentation of Table-V for understanding the effectiveness of approach-4.

TABLE V. RESULT FOR APPROACH-4 – CLUSTER FORMING BASED BLACKHOLE DETECTION

Time	Avg. Pkt Loss in Simple Mode (%)	Avg. Packet Loss under Blackhole Attack (%)	Average packet loss under Cluster forming based Detection (%)
0	0.0000	0.0000	0.0000
50	3.7863	89.3427	80.3650
100	3.8025	89.4704	68.4790
150	3.6554	89.4770	56.1892
200	4.8193	85.0965	47.5791
250	4.6700	89.4276	42.6342
300	4.8718	86.0194	34.6743
350	4.0583	88.8325	27.8539
400	4.2910	88.6108	20.9585
450	3.8388	87.0839	15.4893
500	3.8510	87.3505	8.0887
Average	**3.7859**	**80.0647**	**36.5737**

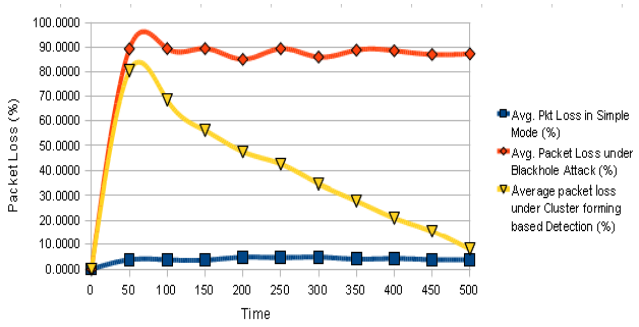

Figure 5. Analysis for Approach-4 under each case

V. CONCLUSION AND FUTURE SCOPE

In this paper we proposed an effect of blackhole attack and ways for its detection in VANETs. We have implemented different detection solutions and simulated the scenarios using simulation. From the results we can conclude that by adopting different detection solutions suggested here, we can reduce the effects of black hole attack. Table VI is representing comparative analysis of each approach. By adopting approach-1, which is based on Neighborhood based blackhole detection, we get the reduction effect in black hole attack is 52.2903%, by approach-2 which is based on Sequence Number based blackhole detection, we get it 40.2346%, by adopting approach-3 which is based on Packet Drop rate based blackhole detection, we get the reduction of 35.3921% and by adopting approach-4 which is based on Cluster forming based Blackhole detection, we get

the reduction of 43.4909%. So based on that we can say that approach-1 Neighborhood based blackhole detection is provide better result compare to other implemented approaches. In future, we plan to analyze different blackhole preventive approaches for better results with the heterogeneous traffic scenario.

TABLE VI. CONCLUSION TABLE

Approaches	Average packet loss (%)	Black Hole Packet Loss (%)	Black Hole Packet Loss under Preventive Mode (%)	Reduction in Black hole Effect (%)
Approach-1 (Neighborhood based blackhole detection)	3.7791 %	80.0733 %	27.7830%	52.2903%
Approach-2 (Sequence Number based blackhole detection)	3.7679 %	80.0252%	39.7906%	40.2346%
Approach-3 (Packet Drop rate based blackhole detection)	3.8151%	80.0484%	44.6563%	35.3921%
Approach-4 (Cluster forming based Blackhole detection)	3.7859%	80.0647%	36.5737%	43.4909%

REFERENCES

[1]. Zeadally, S., Hunt, R., Chen, YS. et al. Telecommun Syst (2012) 50: 217. doi:10.1007/s11235-010-9400-5

[2]. M. S. Al-kahtani, "*Survey on security attacks in Vehicular Ad hoc Networks (VANETs),"* 2012 6th International Conference on Signal Processing and Communication Systems, Gold Coast, QLD, 2012, pp. 1-9.doi:10.1109/ICSPCS.2012.6507953

[3]. S. Verma, B. Mallick and P. Verma, *"Impact of gray hole attack in VANET,"* 2015 1st International Conference on Next Generation Computing Technologies (NGCT), pp. 127-130. http://doi.org/10.1109/NGCT.2015.7375097

[4]. J. Li, H. Lu and M. Guizani, "*ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs*," in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 4, pp. 938-948, April 2015. doi:10.1109/TPDS.2014.2308215

[5]. A. D. Patel and K. Chawda, "*Blackhole and grayhole attacks in MANET*," International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, 2014, pp. 1-6. doi:10.1109/ICICES.2014.7033859
Meenakshi Jamgade and Vimal Shukla , "*Comparative on AODV and DSR under Black Hole Attacks Detection Scheme Using Secure RSA Algorithms in MANET*", International Journal of Computer Sciences and Engineering, Vol.4, Issue.2, pp.145-150, 2016.

[6]. Pradeep Kumar Sharma, Shivlal Mewada and Pratiksha Nigam, "*Investigation Based Performance of Black and Gray Hole Attack in Mobile Ad-Hoc Network*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.4, pp.8-11, 2013.

[7]. R. Kumari, P. Nand, "*Performance Analysis of Existing Routing Protocols*", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.5, pp.47-50, 2017.

[8]. Umesh Kumar Singh, Jalaj Patidar and Kailash Chandra Phuleriya, "*On Mechanism to Prevent Cooperative Black Hole Attack in Mobile Ad Hoc Networks*", International Journal of Scientific Research in Computer Science and Engineering, Vol.3, Issue.1, pp.11-15, 2015.

[9]. Bissmeyer, N.; Schroder, K.H.; Petit, J.; Mauthofer, S.; Bayarou, K.M., "*Experimental analysis of misbehavior detection and prevention in VANETs,"* in Vehicular Networking Conference (VNC), 2013 IEEE , vol., no., pp.198-201, 16-18 Dec. 2013

[10]. Bala, Anu; Bansal, M.; Singh, J., "*Performance Analysis of MANET under Blackhole Attack*," in Networks and Communications, 2009. NETCOM '09. First International Conference on ,IEEE vol., no., pp.141-145, 27-29 Dec. 2009

[11]. Wazid, M.; Katal, A.; Singh Sachan, R.; Goudar, R.H.; Singh, D.P., "*Detection and prevention mechanism for Blackhole attack in Wireless Sensor Network*," in Communications and Signal Processing (ICCSP), 2013 International Conference on , IEEE vol., no., pp.576-581, 3-5 April 2013

[12]. Junhai Luo; Mingyu Fan; Danxia Ye, "*Black hole attack prevention based on authentication mechanism,"* in Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on , vol., no., pp.173-177, 19-21 Nov. 2008.

[13]. Khan U, Agrawal S, Silakari S. *"A detailed survey on misbehavior node detection techniques invehicular ad hoc networks"*. In: SC Satapathy (ed.) Information systems design and intelligent applications. Berlin: Springer, 2015, pp.11–19.

