International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Performance Analysis of Black hole Attack using CBR/UDP Traffic Pattern with AODV routing Protocol in VANET

Bharti[1], D.P.Dvedi[2]

[1]M.Tech Student VIET, G.B. Nagar

[2]Department of Computer Science VIET, G.B. Nagar

Abstract: ***VANET are the promising approach to provide safety to the drivers and which is a growing technology.VANET is the new form of MANET. There are different types of attack but in our paper we are discussing about Black hole attack. There are two types of traffic pattern CBR and TCP. In this paper, we are analysing the Black hole attack using CBR(Constant Bit Rate) and TCP(Transmission control Protocol) traffic pattern in ManhattanGrid scenario under AODV protocol. The purpose of this paper is to analysing the different traffic pattern with Black hole attack and without Black hole attack on the basis of Performance metrices Throughput, end-to-end delay and Packet drop ratio. The simulation setup compromises with different no. of Vehicular nodes using Constant speed. In this we are using simulation NS2 (2.35).***

Keywords: VANET, Black hole Attack, AODV, Traffic pattern, Performance metrices.

1. Introduction

VANET- VANET is new Application of MANET which is using in Vehicular nodes. Vehicular Ad-hoc Networks are the network with no fixed infrastructure. It can be achieved by exchanging the information of traffic environment among vehicles. All the vehicles are mobile in nature, hence a mobile network is needed which can be self-organised and capable of operating without infrastructure support. In VANET, Vehicles that form a communication Network using WiMax IEEE 802.11. Further this network is evolved as mobile ad hoc network [1]. VANET is an application of mobile ad hoc network. More precisely a VANET is self-organised network that can be formed by connecting vehicle aiming to improve driving safety and traffic management with internet access by drivers and programmers. VANET is a highly dynamic topology as compare to MANET. Due to its open access medium, it is more prone to security attacks[2]. Black hole attack is one the common Attack which is using in this paper. The black hole attack is that if the source node send the route request to the destination, then black hole immediately send the false route reply over its route and shown with the highest sequence no. in the route table.

2. Black hole Attack

Security is major issue in the VANET. VANET faces the different types of Attack. In these type of Attack black hole attack is the one which is used in the VANET. In this paper we are using Black hole attack with AODV and observe their impact with AODV. Black hole attack is that which introduces a malicious node for having the direct path to destination and thus cheat with the source node.

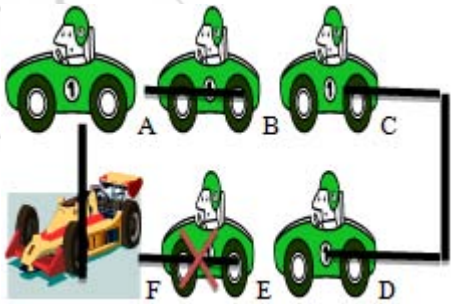


Figure 1: Balck hole attack.

From this figure, we see that node F is the malicious node. Node A wants to send the information to Node D with the shortest path. So, the Node A start the route process and send the packets.. In balck hole attack malicious node does not see in the route table for route information and send the immidietly route reply when it receives the RREQ from the source node before nay other node and reacts that it is freshest route for the destination[3]. This malicious node have the highest sequence no. Due to this the packet does not receive by the destination node and source node thinks that data wiil be send to the destination. So with this malicious node the data wiil be lost. In our paper, we are using Black hole attack with AODV protocol in this we see that what is the effect when we use a malicious node in the AODV protocol with throughput packet drop ratio and end-to-end delay.

The malicious node have other symptoms are following:

1) Packet Dropping: This node does not forward the packet to the other node and just silently drop the packet.
2) RREQ Blocking: In this this malicious node does not forward the RREQ to the nodes but sends the falsely RREP to the source node.

With this Black hole attack, we make a AODV protocol clone to repersent the Black hole with the (DROP_MAL) function which drops the packet. Due to this the AODV with

BLACK node have the more packet drop with this function and the throughput reduced as compared to AODV. Because high throughput shows the best performance but when packet drops in Black hole so the less packet sent to the destination that's why throughput reduced. All these parametrs are effcet by the packet drop and in Black hole Attack packet drops silently. So performance in Black haole attack is poor.

3. Routing Protocol(AODV)

AODV-AODV (Adhoc On Demand Distance Vector Routing Protocol), which is commonly known as reactive routing Protocol where network is silent and connection is needed. AODV creates route between nodes only when the source node request for it. This adds advantage over table Driven Routing Protocol in which every node has to keep up to date routing table[4]. This Routing Protocol used to finding a path to the destination in an Ad-hoc Network.

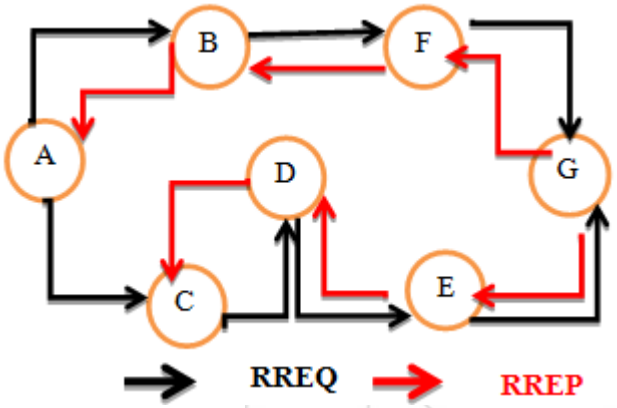


Figure 2: AODV route discovery

AODV use control messages to find the route from source to destination node[5]. These control messages are:
1) Route Request Message (RREQ)
2) Route Reply Message(RREP)
3) Route Error Message (RRER)

AODV uses sequence no. to determine the freshness of routing information. This process is continuous until the packet is received by destination node.

4. Performance Evaluation

In VANET there are many performance evaluation but in this paper we are evaluate throughput, packet drop ratio, and end-to-end delay[6].

Throughput: It is an important parameter which is considered in sending and receiving the data packets is throughput rate.

$$\textbf{Avg Throughput} = \frac{\textbf{Sum of bytes sent through the data packets}}{\textbf{time}}$$

Packet Drop Ratio: Packet drop ratio is the ratio of the no. of packets drop by the malicious node to the total no. of packet send.

$$\textbf{Packet Drop Ratio} = \frac{\sum(\textbf{Sent Packet} - \textbf{Received Packet})}{\textbf{Sent Packet}}$$

*End-to-end delay:*End-to-end delay is average time taken by the data packet to reach the destination. Also includes the delay caused by route discovery and queue in data packet transmission only the successfully delivered data packet is counted. We can calculatedit by this:

$$\textbf{End to end delay} = \frac{\sum(\textbf{Arrival time of packet} - \textbf{Sending time of the packet})}{\sum \textbf{No. of connection}}$$

5. Data Traffic/ Traffic Pattern

Network layer and Transport layer have the different types of Data Traffic respectively which is responsible to transportdata in the network. There are two types of traffic pattern namely UDP/CBR and TCP/FTP[7].

6. TCP/FTP

In such a traffic scenario, TCP represents the data type and FTP represents the application traffic of any application which transport TCP data. TCP is the Transport layer Protocol. This scenario offers connection oriented transmission environment, where communication occurs. In TCP Transmission is done using stream based. It has lower speed than the UDP. It has basic characteristics following:
a) Reliable
b) Bi-directional
c) Conforming

7. UDP/CBR

This type of traffic pattern implies data of UDP type and application traffic is CBR. It offers the constant Bit Rate and does not communicate in phases and movements in only one direction and does not have any feedback from destination. UDP uses the Message based transmission. It has more speed as compared to TCP. It has basic characteristics as:
a) Unreliable
b) Unidirectional
c) Predictable

8. Simulation

In this paper, we are studying the impact of Black hole attackwith AODV on the performance of VANET when we increase the no. of nodes [8]. We are using the NS2 simulator to simulate the work with the NAM Animator. We are using Ns2 (2.35)[9].

Parameter	Value
Simulator	NS2 (2.35)
PROTOCOL	AODV
MAC Layer	802.11
No. of nodes	20
Movement Model	ManhattanGrid/Random way Point
Traffic Pattern	CBR and TCP
Malicious Node	1
Channel	Wireless
Simultion time	1000 s

We analyzing the traffics by analyzing the throughput and packet drop ratio at every 200s simulation time.

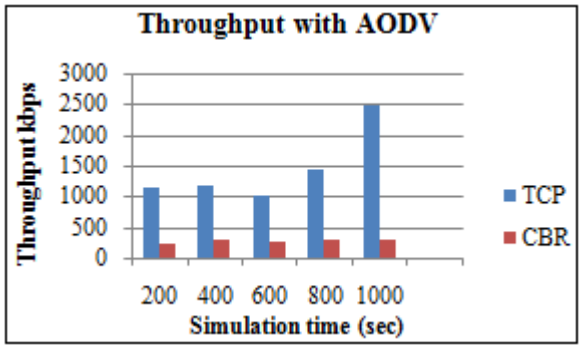
a) Throughput Analysis

We analyzed the throughput for every 200 sec. Following graphs have been found after the simulation.

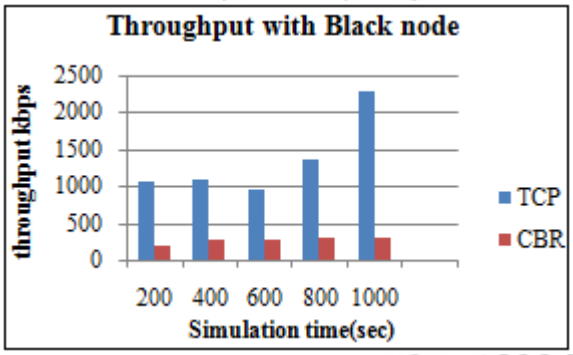
$$Avg\ Throughput = \frac{Sum\ of\ bytes\ sent\ through\ the\ data\ packets}{time}$$

Table 2: Throughput for 20 nodes

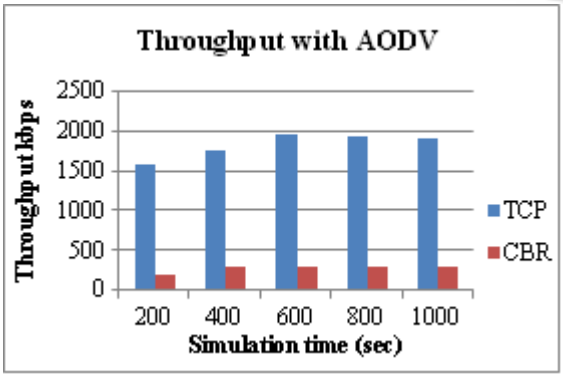
Simulation time	Throughput							
	AODV				Black hole			
	Manhattan Grid		Random Way point		Manhattan Grid		Random Way point	
	TCP	CBR	TCP	CBR	TCP	CBR	TCP	CBR
200	1133	212	1580	210	1063	200	1579	203
400	1172	303	1754	311	1075	267	1833	295
600	1001	277	1957	311	942	265	1880	295
800	1442	306	1916	310	1362	292	1814	292
1000	2468	309	1910	312	2276	291	1812	295



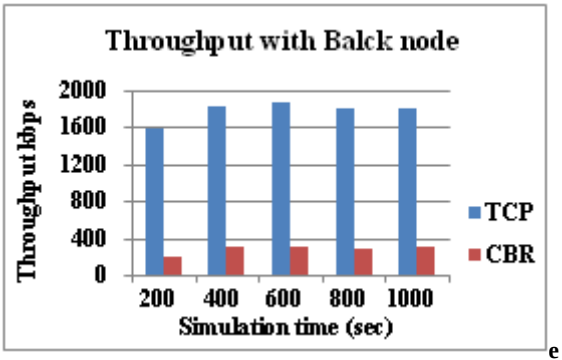
Graph 1: Throughput with AODV in Manhattan Grid



Graph 2: Throughput with Black node in Manhattan Grid



Graph 3: Throughput with AODV in Random Way point



Graph 4: Throughput with Black node in Random Way point

Throughput has been reduced significantly as it is shown in the Graph (2) and Graph (4) for 20 nodes but TCP traffic pattern has the best performance with respect to the CBR. It is clear from these graph that throughput has been reduced up to 50-60 kbps due to Black hole attack(shown in Graph 2 and graph 4)with respect to the normal AODV(shown in graph 1 and graph 3) in ManhattanGrid and random way point. And we compare Random Way point and ManhattanGrid than Random way point has Better performance than the ManhattanGrid movements model, but with the Black node packet drops so that's why the throughput reduced.

b) Packet Drop Ratio Analysis

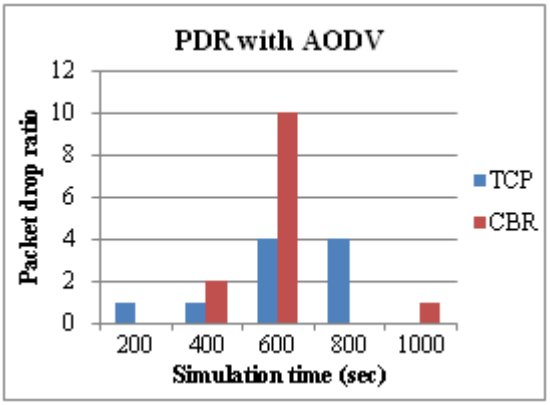
We calculated the packet drop for every 200sec by calculating the difference of sent packet and receive packets by using this formula we calculate the packet drop ratio:

$$Packet\ Drop\ Ratio = \frac{\sum(Sent\ Packet - Received\ Packet)}{Sent\ Packet}$$

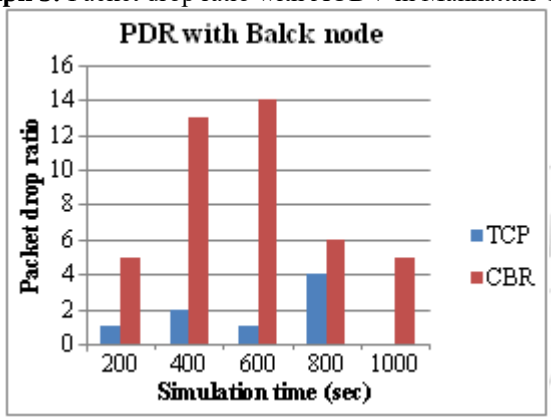
In this paper, we calculate the packet drop ratio with AODV protocol and the impact of black hole attack when we add a ***DROP_MAL*** function with AODV to define the Black hole Attack in AODV. By this function packet drops with black hole and the packet does not received by the destination. So the packet drop ratio in Black hole Attack is increased with respect to the AODV.

Table 3: Packet drop Ratio Result

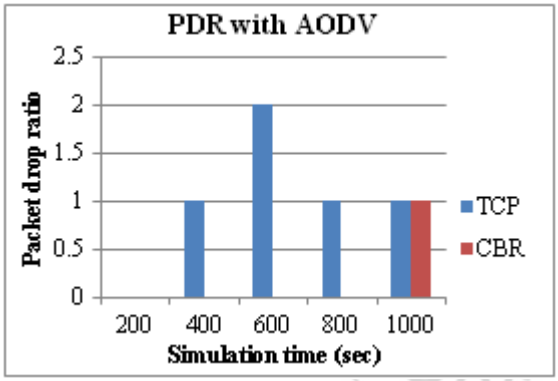
Simulation time	Packet drop ratio							
	AODV				Black hole			
	Manhattan Grid		Random Way point		Manhattan Grid		Random Way point	
	TCP	CBR	TCP	CBR	TCP	CBR	TCP	CBR
200	1	0	0	0	1	5	1	4
400	1	2	1	0	2	13	2	5
600	4	10	2	0	1	14	1	5
800	4	0	1	0	4	6	1	5
1000	0	1	1	1	0	5	1	5



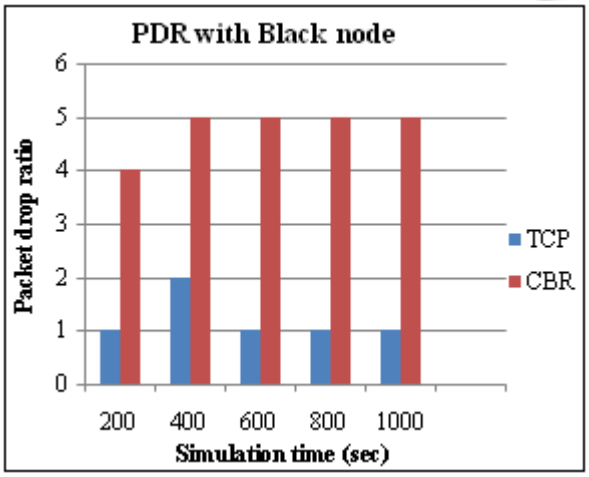
Graph 5: Packet drop ratio with AODV in Manhattan Grid



Graph 5: Packet drop ratio with Black node in Manhattan Grid



Graph 7: Packet drop ratio with AODV in Random Way point



Graph 8: Packet drop ratio with Black node in Random Way point

From the Graph (5) and Graph (7), for the 20 nodes it is clearly shown that Packet Drop Ratio with Black Hole attack (shown in Graph (6) and Graph (8)) is increased by 5% to 10% with respect to the normal AODV (shown in Graph (5) and Graph (7)). But TCP has low packet drop as compared to CBR. From the all above graph we analysed that TCP has low packet drop ratio with respect to the CBR and CBR has higher packet drop ratio .And we observe that Random way point has less packet drop than the ManhattanGrid model. Random way point is better than ManhattanGrid.

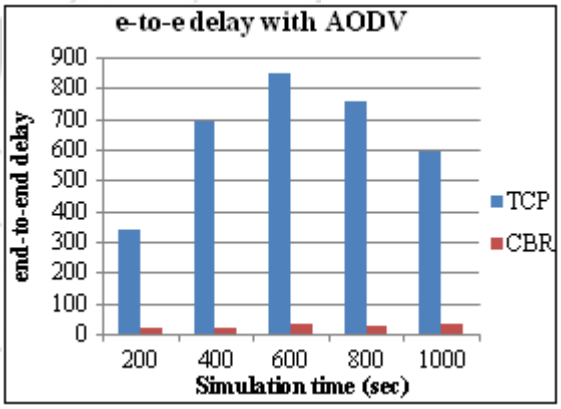
c) End-to end delay

End-to-end delay is, time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in the data packet transmission. Only the data packet that successfully delivered to destination is counted.

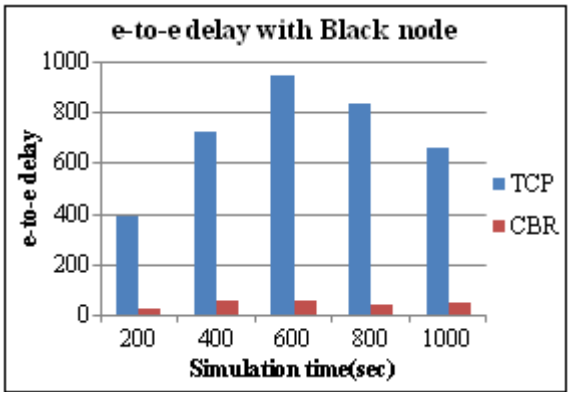
$$end-to-end\ delay = \frac{\sum(Arrival\ time\ of\ packet - sending\ time\ of\ the\ packet)}{\sum No.\ of\ connections}$$

Table 4: End-to-end delay rasult

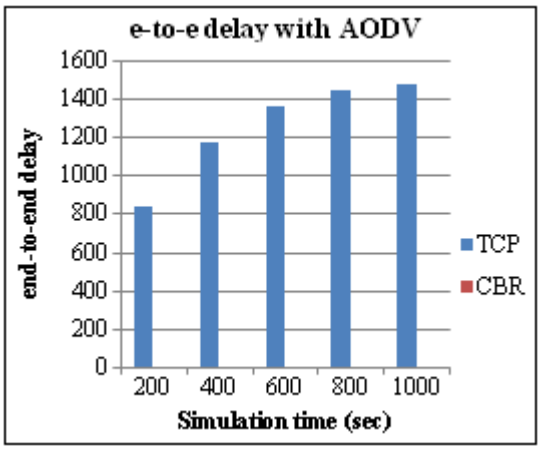
Simulation time	End-to-end delay							
	AODV				Balck hole			
	Manhattan Grid		Random way point		Manhatan Grid		Random Way point	
	TCP	CBR	TCP	CBR	TCP	CBR	TCP	CBR
200	341.7	19.1	831.4	6.24	389.4	21.8	822.6	6.29
400	689.3	18.6	1170.9	6.17	721.8	52.9	1298.1	6.23
600	849.6	29.5	1359.4	6.16	946.7	54.8	1462.3	6.19
800	755.3	26.6	1447.1	6.16	836.1	43.3	1511.9	6.17
1000	594.5	34.7	1477.7	6.16	662.5	48.3	1531.5	6.16



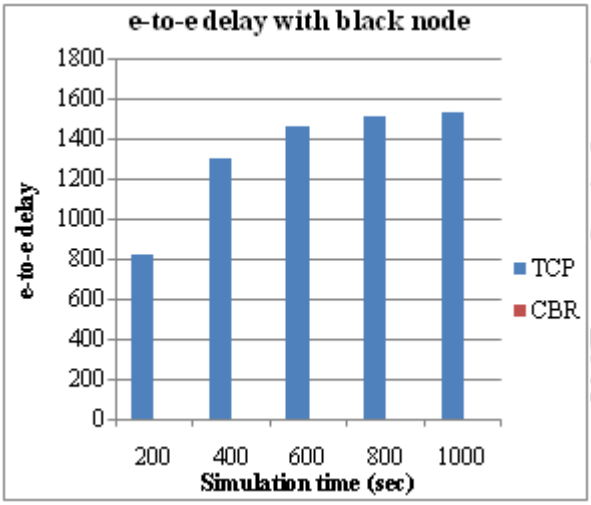
Graph 9: End-to-end delay with AODV in Manhattan Grid



Graph 10: End-to-end delay with Black node in Manhattan Grid



Graph 11: End-to-end delay with AODV in Random Way point



Graph 12: End-to-end delay with Black node in Random Way point

From Graph (9), Graph (10), Graph (11) and Graph (12), We have seen that the end-to-end delay with Black hole attack(shown in Graph (10) and graph (12) for ManhattanGrid and Random way point) is increased 10% to 15% with respect to the normal AODV(shown in Graph (9) and Graph (11) for ManhattanGrid and Random way point). And we see that TCP has more delay with respect to the CBR. CBR has less end-to-end delay. And we also observe that Random Way point has better performance than the ManhattanGrid and we see that Random way point has low delay.

From the above graph we observe that TCP has the better performance than CBR and also observe that Random Way point also has the better performance than the ManhattanGrid movements model. So after observing these models using different traffic pattern we see that random way point has better performance than the ManhattanGrid model with CBR pattern.

9. Conclusion

Vehicular Ad-hoc network (VANETs) are a subcategory of Mobile ad-hoc Network which are recently being discussed in great extent. The main intention with VANET's is to enhance vehicles, passengers, safety and comfort by distributing traffic and other conditions among nearby vehicles.

In this research work, we worked with Black hole attack using different traffic pattern CBR and TCP with 10 and 20 nodes with ManhattanGrid scenario. We analyzed the behavior of the Black hole attack with AODV protocol by using the DROP_MAL() function which silently drop the packet when we send the data from source to destination but with this function destination does not receive any data or we lost the data.. We observe that as we increase the no. of nodes then the speed of the vehicles movements increased as shown in the above graphs. We also see that the performance of the black hole attack in packet drop ratio and end-to-end increased with respect to the nodes mean if we increase the no. of nodes then the packet drop ratio increase and the end to end delay in TCP is decreased and in CBR is increased but the throughput is reduced significantly. And we analyzed that the TCP has the better performance than the CBR.

10. Future Work

An ample amount of research work has been carried out for the improvement towards the security of the VANET but still there are some issues to resolve. To perform a research work within a given time is never easy, as time increases the pressure on researchers to perform. Because of the time constraint, this research work focused only on the single attack. In future we would like to perform following tasks regarding black hole attacks:

- The co-operative black hole can be implemented and evaluated on three scenarios.
- The scenario can be made very realistic with the use of SUMO with NS2.
- The mitigation scheme can also be implemented with variable destination sequence no.
- The effect of the black hole attack can be evaluated with some other protocol like DSR and other VANET routing protocol.

References

[1] S. Sesay, Z Yang and Jianhua He, *"A survey on Mobile Ad-hoc Network*", Information Technology Journal 3 (2), pp. 168-175, 2004.

[2] Vimal Bibhu, Kumar Roshan,"*Performance analysis of Black hole Attack in VANET*". International Journal Computer Network and Information security, 2012,11 pp-47-54.

[3] Mahesh Kumar, Mr.Kuldeepbhardwaj*,"Impact of Black hole on AODV based routing in Vehicular Ad-hoc Networks*", International Journal of Wired and wireless communication, Vol 4, issue 1, oct 2015.

[4] C. E. Perkins, E.M.B. Royer and S. R. Das, *"Ad Hoc On-Demand Distance Vector (AODV) routing"*, RFC 3561, July 2003.

[5] Sonia and Padmavati,"*Performace analysis of Black hole Attack on VANET'S Reactive Routing Protocols*", International Journal of Computer Applications(0975-8887) Vol. 73-No.9, July 2013.

[6] Arti Sharma, Satendra Jain, "*A behavioural study of AODV with and without Black hole attack in MANET*". IJMER international Journal of Modern Engineering Research (IJMER), vol. 1 Issue 2. Pp. 391-395.

[7] Ritika Sharma and Kamlesh Gupta,*"Comparision based performance analysis of UDP/CBR and TCP/FTP traffic under AODV routing protocol in MANET* ", International Journal of Computer application(0975-8887), Vol. 56-No.-15 Oct 2012.
[8] Network Simulator Official Site for Package Distribution, web reference, *http://www.isi.edu/nsnam.*
[9] Sheenu Sharma, Roopam Gupta, "*Simulation Study of Black hole attack in Mobile Ad-hoc Networks*", Journal of Engineering Science and Technology, vol. 4, no.2, 2009. Pp.243-250.