I. J. Computer Network and Information Security, **2012, 11, 47-54**
Published Online October 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.11.06

Performance Analysis of Black Hole Attack in Vanet

Vimal Bibhu
Research Scholar, Doctor of Philosophy, Department of Computer Science & Information Technology, B.R.A Bihar University, Muzaffarpur, Bihar, India
vimalbibhu@gmail.com
Kumar Roshan
Research Scholar, Department of Computer Science & Engineering, IETE, New Delhi, India
Kmr.roshan1@gmail.com
Dr. Kumar Balwant Singh
Lecturer, Department of Physics, Govt. Polytechnic, Darbhanga, Bihar, India
kbsphysics@yahoo.co.in
Dr. Dhirendra Kumar Singh
Professor, University Department of Mathematics, B.R.A Bihar University, Muzaffarpur, Bihar, India

Abstract — Black hole attack in Vehicular Ad Hoc Network is major problem related with the field of computer networking. In this paper we present the performance analysis of the black hole attack in Vehicular Ad Hoc Network. We elaborate the different types of attacks and their depth in ad hoc network. The performance metric is taken for the evaluation of attack which depends on a packet end to end delay, network throughput and network load. The delay, throughput and load are simulated by the help of OPNET 14.5 modeler. The simulation setup comprises of 30 Vehicular nodes moving with constant speed of 10 meter per second. The data rate of Vehicular nodes is 11 Mbps with default transmitting power of 0.005 watts. With On Demand Distance Vector Routing and Optimized Link State Routing the malicious node buffer size is lowered to a level which increase packet drops.

Index Terms — VANET – Vehicular Ad Hoc Network, DOS – Denial of Service, MAC – Medium Access Control, OPNET – Operation Network, AODV – Ad Hoc On Demand Distance Vector Routing, RREQ – Route Request

I. INTRODUCTION TO BLACK WHOLE ATTACK

VANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. In these attacks, black hole attack is that kind of attack which occurs in Vehicular Ad-Hoc networks (VANET).

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.

This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it . In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it’s up to the node whether to drop all the packets or forward it to the unknown address.

The method how malicious node fits in the data routes varies. Fig.1 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 as soon as it receives RREQ packets. 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” [1]. In this way all the data packet will be lost consumed or lost.

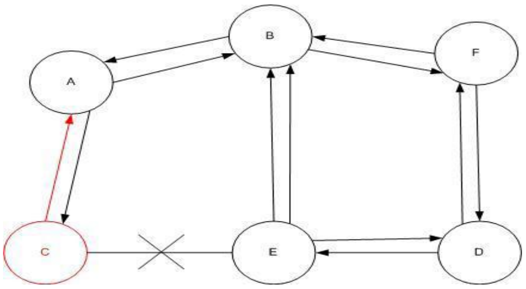

Fig. 1 Black Hole Attack Problem

1.1 Black hole attack in AODV

Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack. First is internal black hole attack which has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself 20 an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node. The second type of black hole attack is External Black hole attack in which attack physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network [2]. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in VANET. External black hole attack can be summarized in following points with fig. 2

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.

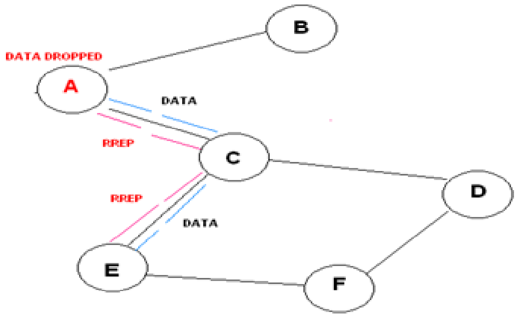

Fig. 2 External Black Hole Attack

In AODV black hole attack the malicious node “A” first detect the active route in between the sender “E” and destination node “D”. The malicious node “A” then send the RREP which contains the spoofed destination address including small hop count and large sequence number than normal to node “C”. This node “C” forwards this RREP to the sender node “E”. Now this route is used by the sender to send the data and in this way data will arrive at the 21 malicious nodes. These data will then be dropped. In this way sender and destination node will be in no position any more to communicate in state of black hole attack.

1.2 Black hole attack in OLSR

In OLSR black hole attack, a malicious node forcefully selects itself as MPR which is discussed in chapter 3.Malicious node keep its willingness field to Will always constantly in its HELLO message. So in this case, neighbors of malicious node will always select it as MPR. Hence the malicious node earns a privileged position in the network which it exploits to carry out the denial of service attack. The effect of this attack is much vulnerable when more than one malicious node is present near the sender and destination nodes [3].

1.3 Gray Hole Attack

In this kind of attack the attacker misleads the network by agreeing to forward the packets in the network. As soon as it receive the packets from the neighboring node, the attacker drop the packets. This is a type of active attack. In the beginning the attacker nodes behaves normally and reply true RREP messages to the nodes that started RREQ messages. When it receives the packets it starts dropping the packets and launch Denial of Service (DoS) attack. The malicious behavior of gray hole attack is different in different ways. It drops packets while forwarding them in the network. In some other gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [4][5]. Due this behavior it’s very difficult for the network to figure out such kind of attack. Gray hole attack is also termed as node misbehaving attack.

1.4 Flooding Attack

The flooding attack is easy to implement but cause the most damage. This kind of attack can be achieved either by using RREQ or Data flooding. In RREQ flooding the attacker floods the RREQ in the whole network which takes a lot of the network resources. This can be achieved by the attacker node by selecting such I.P addresses that do not exist in the network. By doing so no node is able to answer RREP packets to these flooded RREQ. In data flooding the attacker get into the network and set up paths between all the nodes in the network. Once the paths are established the attacker injects an immense amount of useless data packets into the network which is directed to all the other nodes in the network. These immense unwanted data packets in the network congest the network. Any node that serves as destination node will be busy all the time by receiving useless and unwanted data all the time.

1.5 Selfish Node

In VANETs the nodes perform collaboratively in order to forward packets from one node to another node. When a node refuse to work in collaboration to forward packets in order to save its limited resources are termed as selfish node, this cause mainly network and traffic disruption. The selfish nodes can refuse by advertising non existing routes among its neighbor nodes or less optimal routes. The concern of the node is only to save and preserves it resources while the network and traffic disruption is the side effect of this behavior. The node can use the network when it needs to use it and after using the network it turn back to its silent mode. In the silent mode the selfish node is not visible to the network [6].

The selfish node can sometime drop the packets. When the selfish node see that the packets need lot of resources, the selfish node is no longer interested in the packets it just simply drop the packets and do not forward it in the network.

1.6 Wormhole Attack

Wormhole attack is a severe attack in which two attackers placed themselves strategically in the network. The attackers then keep on hearing the network, record the wireless data. The two attackers placed themselves in a strong strategic location in the network.

In wormhole attack, the attacker gets themselves in strong strategic location in the network. They make the use of their location i.e. they have shortest path between them. They advertise their path letting the other nodes in the network to know they have the shortest path for the transmitting their data. The wormhole attacker creates a tunnel in order to records the ongoing communication and traffic at one network position and channels them to another position in the network .When the attacker nodes create a direct link between each other in the network. The wormhole attacker then receives packets at one end and transmits the packets to the other end of the network. When the attackers are in such position the attack is known as out of band wormhole.

The other type of wormhole attack is known as in band wormhole attack given under figure 3. In this type of attack the attacker builds an overlay tunnel over the existing wireless medium. This attack is potentially very much harmful and is the most preferred choice for the attacker.

In wormhole attack, the attacker gets themselves in strong strategic location in the network. They make the use of their location i.e. they have shortest path between the nodes as shown in the Figure 3 above. They advertise their path letting the other nodes in the network to know they have the shortest path for the transmitting their data. The wormhole attacker creates a tunnel in order to records the ongoing communication and traffic at one network position and channels them to another position in the network .When the attacker nodes create a direct link between each other in the network. The wormhole attacker then receives packets at one end and transmits the packets to the other end of the network. When the attackers are in such position the attack is known as out of band wormhole[7][8].

The other type of wormhole attack is known as in band wormhole attack. In this type of attack the attacker builds an overlay tunnel over the existing wireless medium. This attack is potentially very much harmful and is the most preferred choice for the attacker.

1.7 Sleep Deprivation Torture Attack

One of the most interesting attack in VANETs, where the attacker tries to keep the nodes awake until all its energy is lost and the node go into permanent sleep. This attack is known as sleep Deprivation torture attack. The nodes operating in VANETs have limited resources i.e. battery life, the node remain active for transmitting packets during the communication. When the communication cease these nodes go back to sleep mode in order to preserve their resources [9][10]. The attacker exploit this point of the nodes by making it busy, keeping it awake so as to waste all its energies and make it sleep for the rest of its life. When nodes went to sleep for ever an attacker can easily walk into the network and exploit rest of the network.

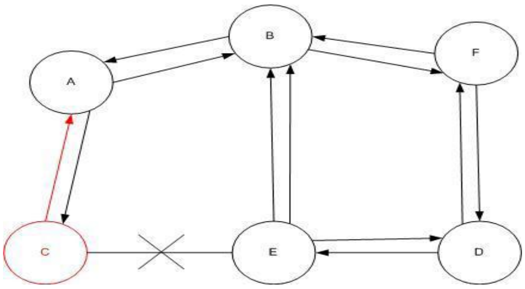

Fig.3 Wormhole attack

1.8 Jellyfish Attack

In jellyfish attack, the attacker attacks in the network and introduce unwanted delays in the network. In this type of attack, the attacker node first get access to the network, once it get into the network and became a part of the network. The attacker then introduce the delays in the network by delaying all the packets that it receives, once delays are propagated then packets are released in the network. This enables the attacker to produce high end-to-end delay, high delay jitter and considerably affect the performance of the network.

1.9 Modification Attack

The nature of Ad-Hoc network is that any node can join freely the network and can leave it. Nodes which want to attack join the network. The malicious node then later exploits the irregularities in the network amongst the nodes. It participates in the transmission process and later on some stage launches the message modification attack. Misrouting and impersonation attacks are two types of modification attack.

1.10 Misrouting Attack

In misrouting attack a malicious node which is part of the network, tries to reroute the traffic from their originating nodes to an unknown and wrong destination node. As long as the packets remain in the network make use of resources of the network. When the packet does not find its destination the network drops the packet.

1.11 Impersonation Attack

In Ad-Hoc networks a node is free to move in and out of the network. There is no secure authentication process in order to make the network secure from malicious nodes. In VANETs IP and MAC address uniquely identifies the host. These measurements are not enough to authenticate sender. The attacker use MAC and IP spoofing in order to get identity of another node and hide into the network. This kind of attack is also known as spoofing attack.

II. PERFORMANCE ANALYSIS

2.1 Performance Metrics

The performance metrics chosen for the evaluation of black hole attack are packet end-to-end delay, network throughput and network load. The packet end-to-end delay is the average time in order to traverse the packet inside the network. This includes the time from generating the packet from sender up till the reception of the packet by receiver or destination and expressed in seconds. This includes the overall delay of networks including buffer queues, transmission time and induced delay due to routing activities. Different application needs different packet delay level. Voice and video transmission require lesser delay and show little tolerance to the delay level.

The second parameter is throughput; it is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet. It is represented in bits per second or packets per seconds [11]. In VANETs throughput is affected by various changes in topology, limited bandwidth and limited power. Unreliable communication is also one of the factors which adversely affect the throughput parameter.

The third parameter is network load, it is the total traffic received by the entire network from higher layer of MAC which is accepted and queued for transmission. It indicates the quantity of traffic in entire network. It represents the total data traffic in bits per seconds received by the entire network from higher layer accepted and queued for transmission. It does not include any higher layer data traffic rejected without queuing due to large data packet size.

III. SIMULATION TOOL

The tool used for the simulation study is OPNET 14.5 modeler. OPNET is a network and application based software used for network management and analysis. OPNET models communication devices, various protocols, architecture of different networks and technologies and provide simulation of their performances in virtual environment. OPNET provides various research and development solution which helps in research of analysis and improvement of wireless technologies like WIMAX, Wi Fi, UMTS, analysis and designing of VANET protocols, improving core network technology, providing power management solutions in wireless sensor networks. In our case we used OPNET for modeling of network nodes, selecting its statistics and then running its simulation to get the result for analysis [12].

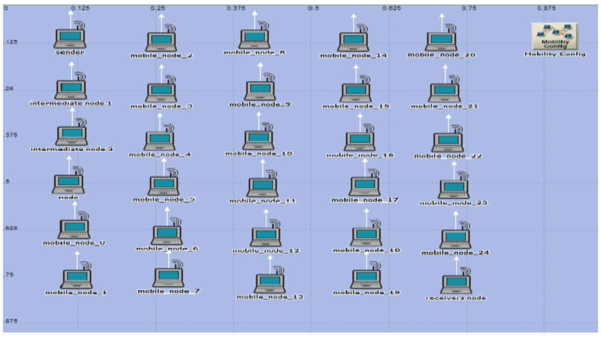

Fig. 4 Simulation Environment for 30 nodes

Table 1. Simulations Parameters

SIMULATION PARAMETERS Examined protocols AODV and OLSR Simulation time1000 seconds Simulation area (m x m)1000 x 1000	
Number of Nodes	16 and 30
Traffic Type	TCP
Performance Parameter	Throughput, delay, Network Load
Pause time	100 seconds
Mobility (m/s)	10 meter/second
Packet Inter-Arrival Time (s)	exponential(1)
Packet size (bits)	exponential(1024)
Transmit Power(W)	0.005
Date Rate (Mbps)	11 Mbps
Mobility Model	Random waypoint

3.1 Modeling of Network

At first network is created with a blank scenario using startup wizard. Initial topology is selected by creating the empty scenario and network scale is chosen by selecting the network scale. In our case we have selected campus as our network scale. Size of the network scale is specified by selecting the X span and Y span in given units. We have selected 1000 * 1000 meters as our network size. Further technologies are specified which are used in the simulation. We have selected VANET model in the technologies. After this manual configuration various topologies can be generated by dragging objects from the palette of the project editor workspace. After the design of network, nodes are properly configured manually.

3.2 Collection of Results and Statistics

Two types of statistics are involved in OPNET simulation. Global and object statistics, global statistics is for entire network's collection of data. Whereas object statistics involves individual nodes statistics. After the selection of statistics and running the simulation, results are taken and analyzed. In our case we have used global discrete event statistics (DES).

3.3 Simulation Setup

The simulation setup of a single scenario comprising of 30 Vehicular nodes moving at a constant speed of 10 meters per second. Total of 12 scenarios have been developed, all of them with mobility of 10 m/s. Number of nodes were varied and simulation time was taken 1000 seconds. Simulation area taken is 1000 x 1000 meters. Packet Inter-Arrival Time (sec) is taken exponential (1) and packet size (bits) is exponential (1024). Simulation environment of 30 nodes is given in fig. 4.

The data rates of Vehicular nodes are 11 Mbps with the default transmitting power of 0.005 watts. Random way point mobility is selected with constant speed of 10 meter/seconds and with pause time of constant 100 seconds. This pause time is taken after data reaches the destination only.

Our goal was to determine the protocol which shows less vulnerability in case of black hole attack. We choose AODV and OLSR routing protocol which are reactive and proactive protocols respectively. In both case of AODV and OLSR, malicious node buffer size is lowered to a level which increase packet drop. Furthermore the simulation parameters are given in Table I.

IV. RESULTS

Its analysis based on the simulation performed in OPNET modeler 14.5. Our simulated results are provided in Figures (1-10) gives the variation in network nodes while under Black Hole attack. To evaluate the behavior of simulated intrusion based black hole attack, we considered the performance metrics of packet end-to-end delay, throughput and network load.

4.1 Packet End-to-End Delay

Packet end-to-end delay in case of Black Hole attack and without attack depends on the protocol routing procedure and number of nodes involved. In Fig. 5, delay in case of 16 nodes for AODV and OLSR is high in case when there is no attack on the network nodes. This is because during the Black Hole attack, there is no need of RREQs and RREPs because the malicious node already sends its RREQs to the sender node before the destination node reply having less delay. Also comparatively AODV shows more delay than OLSR because of its route search and reactive nature.

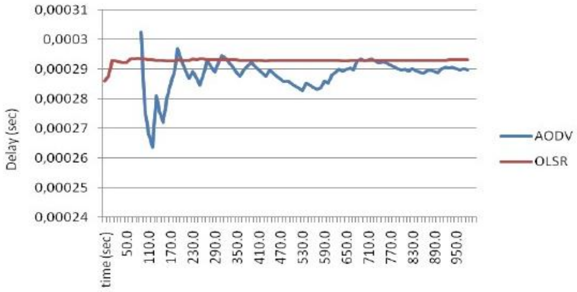

Fig. 5 End-to-end delay of OLSR and AODV with vs. without attack for 16 nodes

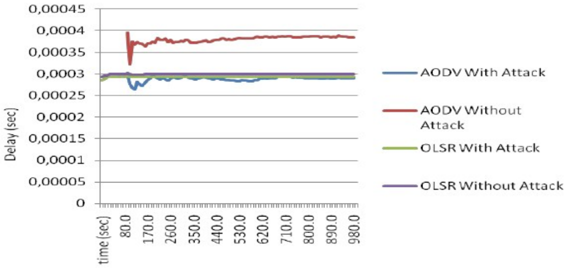

Fig. 6 End-to-end delay of OLSR and AODV with vs. without attack for 16 nodes

In case of 30 nodes the delay is 5 percent more as compared to the case of 16 nodes. The overall impact of delay on AODV and OLSR is same as it was observed in 16 nodes. The increase in numbers of nodes also increases the difference of delay in AODV in case of Black Hole attack with comparison to a simple AODV scenario.

The average packet end-to-end delay in presence of a malicious node only is shown in Figure 5 and Figure 6. Fig. 7 show that OLSR has slightly higher delay than AODV. This is consistent if the numbers of nodes are less. However with the increase in number of node an increase in the delay of AODV has been observed. In Fig. 8, for 30 nodes, AODV show high delay in comparison with OLSR. In terms of delay the performance of OLSR improves with the increase in number of nodes because of its table driven nature. It maintains up to date routing information from each node to every other node in the network.

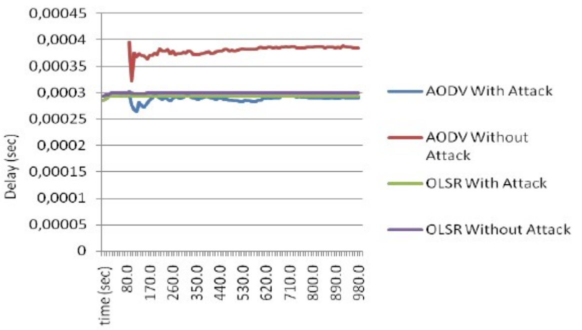

Fig. 7 End-to-end delay for OLSR and AODV with vs. without attack for 30 nodes

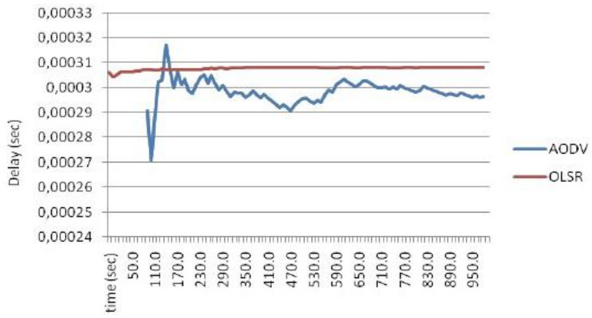

Fig. 8 End-to-end delay 30 nodes AODV vs. OLSR with attack

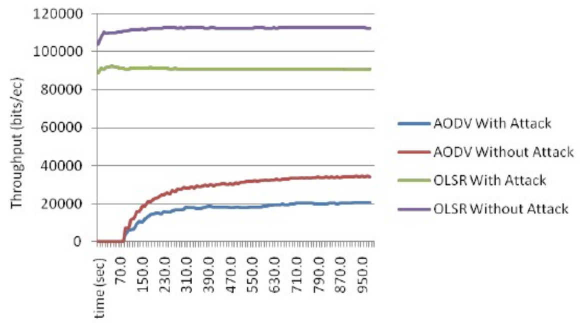

Fig. 9 Throughput of OLSR and AODV with vs. without attack for 16 nodes

From Fig. 9 for 16 nodes, it is obvious that the throughput for OLSR is high compared to that of AODV. Also in OLSR throughput for the case with no attack is higher than the throughput of OLSR under attack. This is because of the fewer routing forwarding and routing traffic. Here the malicious node discards the data rather than forwarding it to the destination, thus effecting throughput. The same is observed in the case with AODV, without attack, its throughput is higher than in the case with under attack because of the packets discarded by the malicious node. Similarly in Fig. 7 for 30 nodes, the throughput is high because of the higher number of nodes but the trend of throughput with attack and without attack remains the same as in 16 numbers of nodes.

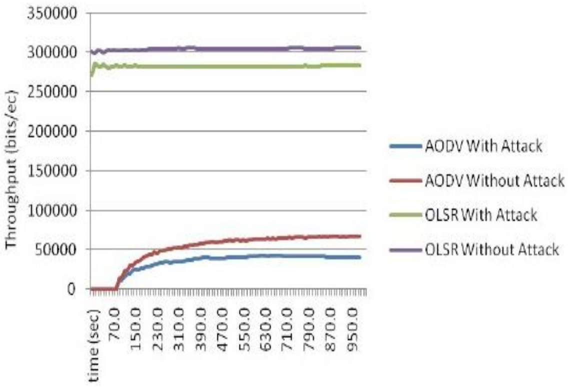

Fig 10. Throughput of OLSR and AODV with vs. without attack for 30 nodes attack

The throughput of AODV and OLSR in the presence of single malicious nodes shown in figure 9 and figure 10. It is obvious from both figures that OLSR by far outperforms AODV in case of both 16 and 30 sources. OLSR being proactive routing protocols makes sure that the availability of routing path exists, before routing the traffic. We have observed that the higher number of sources gives less difference in throughput as compare to less number of sources. This is because the higher the number of sources is the more congestion there is. Over all, OLSR ensures consistent routing paths with in the network, helping in lowering the delay. As throughput is the ratio of the total data received from source to the time it takes till the receiver receives the last packet. A lower delay translates into higher throughput. The overall low throughput of AODV is due to route reply. As the malicious node immediately sends its route reply and the data is sent to the malicious node which discard all the data. The network throughput is much lower is shown in figure 11 and fig. 12.

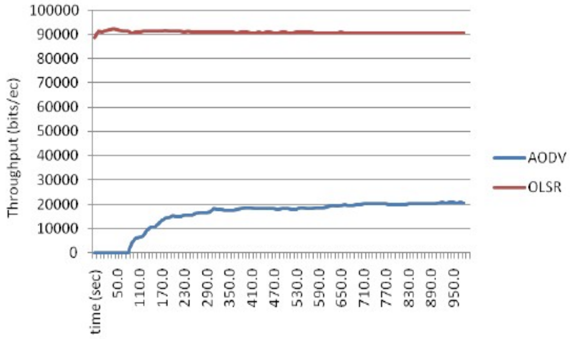

Fig. 11 Throughputv16 nodes AODV vs. SLR With Attack

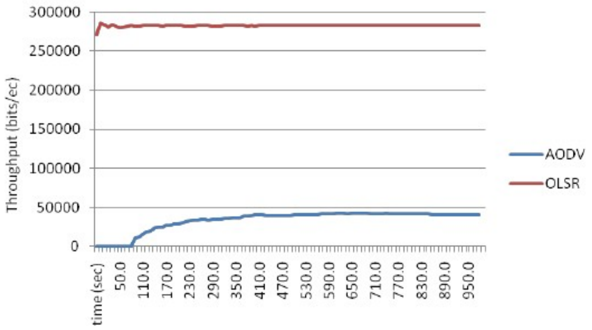

Fig. 12 Throughput 30 nodes AODV vs. OLSR with attack

V. NETWORK LOAD

The network load graph of OLSR and AODV with and without presence of a malicious node has been shown in the Fig. 7, 9 and 10. The network load of OLSR is much high as compare to AODV. In case of attack OLSR has less network load as compare to without attack. In case of 16 nodes the network load of OLSR is 3 times higher in case of without attack which implies that it is actually routing its packet to the entire destination properly. But under attack it cannot send its packet i.e. packet discarding leads to a reduction of network load.

In case of 30 nodes there is a slight variation in between OLSR with and without attack. This is due to the high number of nodes which leads to more increase in routing traffic. However AODV show no changes in both cases of 16 and 30 number of nodes given in fig. 13 and figure14.

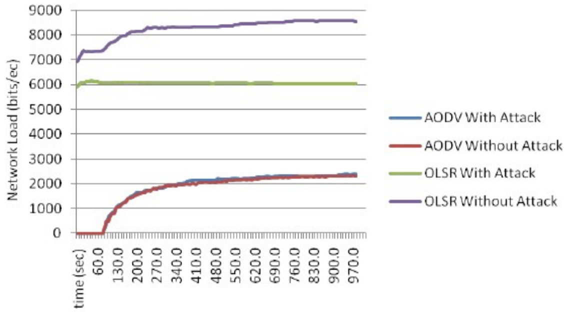

Fig. 13 Network Load of OLSR and AODV with vs. without attack for 16 nodes

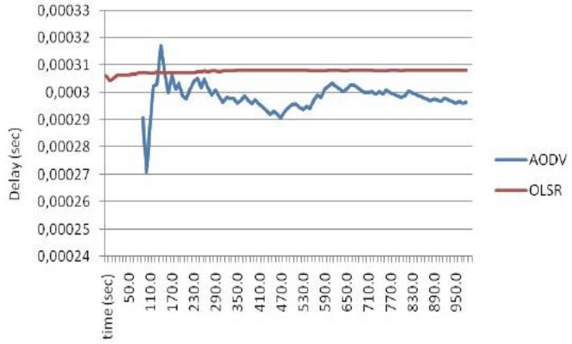

Fig. 14 Network Load of OLSR and AODV with vs. without attack for 30 nodes

VI. CONCLUSION

Vehicular Ad-Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of VANET comparative to its vast potential it has still many challenges left in order to overcome. Security of VANET is one of the important features for its deployment. In our thesis, we have analyzed the behavior and challenges of security threats in Vehicular Ad-Hoc networks with solution finding technique. Although many solutions have been proposed but still these solutions are not perfect in terms of effectiveness and efficiency. If any solution works well in the presence of single malicious node, it cannot be applicable in case of multiple malicious nodes. After studying all the approaches, our conclusion is that the approach offered by Deng suit well in our scenario. The intermediate reply messages if disabled leads to the delivery of message to the destination node will not only improve the performance of network, but it will also secure the network from Black Hole attack. In our study we analyzed that Black Hole attack with four different scenarios with respect to the performance parameters of end-to-end delay, throughput and network load. In a network it is important for a protocol to be redundant and efficient in term of security. We have analyzed the vulnerability of two protocols OLSR and AODV have more severe effect when there is higher number of nodes and more route requests. The percentage of severances in delay under attack is 2 to 5 percent and in case of OLSR, where as it is 5 to 10 percent for AODV. The throughput of AODV is effected by twice as compare of OLSR. In case of network load however, there is effect on AODV by the malicious node is less as compare to OLSR. Based on our research and analysis of simulation result we draw the conclusion that AODV is more vulnerable to Black Hole attack than OLSR.

VII. FUTURE WORK

Wireless Ad-Hoc networks are widely used networks due to their flexible nature i.e. easy to deploy regardless of geographic constraints. These networks are exposed to both external and internal attacks as there is not centralized security mechanism. A lot of research work is still need in this area. We tried to discover and analyze the impact of Black Hole attack in VANETs using AODV and OLSR protocols. There is a need to analyze Black Hole attack in other VANETs routing protocols such as DSR, TORA and GRP. Other types of attacks such as Wormhole, Jellyfish and Sybil attacks are needed to be studied in comparison with Black Hole attack. They can be categorized on the basis of how much they affect the performance of the network. Black Hole attack can also attack the other way around i.e. as Sleep Deprivation attack. The detection of this behavior of Black Hole attack as well as the elimination strategy for such behavior has to be carried out for further research.

REFERENCES

[1] D. Djenouri, L. Khelladi and N. Badache, A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks, IEEE Communication Surveys & Tutorials, Vol. 7, No. 4, 4th Quarter 2005.

[2] E. A. Mary Anita and V. Vasudevan, Performance Evaluation of mesh based multicast reactive routing protocol under black hole attack, IJCSIS, Vol.3, No.1, 2009.

[3] Al-Shurman, M. Yoo, S. Park, Black hole attack in Mobile Ad Hoc Networks, ACM Southeast Regional Conference, 2004, pp. 96-97.

[4] S. Buchegger, C. Tissieres, and J. Y. Le Boudec. A test bed for misbehavior detection in mobile ad-hoc networks –how much can watchdogs really do. Technical Report IC/2003/72, EPFL-DI-ICA, November 2003. Available on:citeseer.ist.psu.edu/645200.html.

[5] C. Srdjan, B. Levente, and H. Jean-Pierre, Self-Organized Public-Key Management for Mobile Ad Hoc Networks, IEEE Transactions on Mobile Computing, vol. 2, pp. 52-64, 2003.

[6] Satoshi Kurosawa; Hidehisa Nakayama; Nei Kato; Abbas Jamalipour; and Yoshiaki Nemoto (2007). Detecting blackhole attack on AODV based mobile Ad hoc networks by dynamic learning method. International Journal of Network Security, 5(3), 338–346.

[7] Chen Hongsong; Ji Zhenzhou; and Hu Mingzeng (2006). A novel security agent scheme for AODV routing protocol based on thread state transition. Asian Journal of Information Technology, 5(1), 54-60.

[8] Saini A, Kumar H (2010) Comparison between Various Black Hole Detection Techniques in VANET. Paper presented at the National Conference on Computational Instrumentation, Chandigarh, India, 19-20 March 2010

[9] Deng H, Li W, Agrawal DP (2002) Routing Security in Wireless Ad-hoc Networks. IEEE Communications Magazine 40(10):70–75. doi: 10.1109/MCOM.2002.1039859

[10] Sun B, Guan Y, Chen J, Pooch UW (2003) Detecting Black-hole Attack in Mobile Ad Hoc Networks. Paper presented at the 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003

[11] Dokurer, Semih “Simulation of Black hole attack in wireless Ad-Hoc networks” Master’s thesis, Atihm University, September 2006.

[12] Santoshi Kurosawal, hidehisa, Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto. “Detecting Blackhole Attack on AODV – based Mobile Ad Hoc Networks by Dynamic Learning Method” in International Journal of Network Security, Vol.5, No.3, pp.338-346, Nov.2007.

Author Profiles:

Kumar Roshan is currently pursuing M.Tech in Computer Science & Engineering. He has published many papers.

Vimal Bibhu is M.Tech in Computer Science & Engineering and pursuing Ph.D in Computer Science. He has published many papers.

Dr. Kumar Balwant Singh is Ph.D in Physics. He is currently working on the post of Lecturer in Department of Physics in Govt. Polytechnic Darbhanga, Bihar, India

Dr. Dhirendra Kumar Singh is Ph.D in Mathematics. He is Professor in University Department of Mathematics, Bhim Rao Ambedkar Bihar University, Bihar, India.