Implementation of GPSR Routing Protocol in VANET for Analyzing Black Hole Attack Using CBR/UDP Traffic Pattern With Security Algorithm

Hari Krishan[1], Manish Choubisa[2]
M. Tech Scholar[1] – A. I. E. T, Department of CSE, RTU, Kota, India
Assistant Professor[2]– A. I. E. T, Department of CSE, RTU, Kota, India
yadav.harikrishan3@gmail.com[1], *ermanishchoubisa@gmail.com*[2]

Abstract –In implementing VANET security is one of biggest challenges due to dynamic topology. There are possibilities of active and passive attack in network to alter the authentic data. With pace of time tremendous development occurred in the field of VANET. Security is one of biggest challenges which need to handle effectively in adhoc network. In VANET nodes are mobiles and therefore they continuously change their respective location therefore due to dynamic topology, network becomes prone to attack. With advancement in technology in parallel unethical activity also take place which try to access the data illegally to fetch personnel profit. There are various types of attack possibilities in adhoc network but generally attacks are categorized into active attack and passive attack. Our research article based upon black hole attack which is very common to the networks. In this attack a malicious node with high priority number is deployed in between other nodes and malicious node acquire this data instead of destination node and also send an acknowledgement to source node that data received by destination node successfully. In this research paper proposed work executed by GPSR protocol and performance analysis of the black hole attack in Vehicular Ad Hoc Network is tested. The networking parameters of GPSR routing protocol are better than existed protocol in term of end to end delay, packet loss, energy consumption. Further implemented research work can be extended in better way with help of IoT, M2M and artificial intelligence for various network configurations with security algorithm.

***Key Words –** VANET, Security, Black Hole Attack,, End to End Delay, Adhoc, Protocol, GPSR*

*****

I. INTRODUCTION

Wireless technology is advancing rapidly with time. With the advancement and maturity of the VANET, there will be a great revolution in the field of wireless communication in terms of fast handovers, network availability, security, safety with the use of advanced techniques. VANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. Security parameters in VANET are now receiving popularity in the research community. In VANET environment, significant decision format has to be determined with the problems related to attack modeling, optimizing response and allotment of defense resources in a wide manner. However, a single defense mechanism cannot provide solution to the attack models that are affecting the VANETs. The game theory model is used as a defense mechanism against sophisticated and complex type of attacks arising in VANET. Securing wireless adhoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information [4]. VANET is similar to MANET along with some minute changes. VANET integrated mobile nodes, road side units. Mobile nodes are the sensors embedded in the vehicles that are called as on board units for the signal processing to and from RSUs. RSUs are fixed installed units that are the gateway for the communication between MN and the servers or internet.

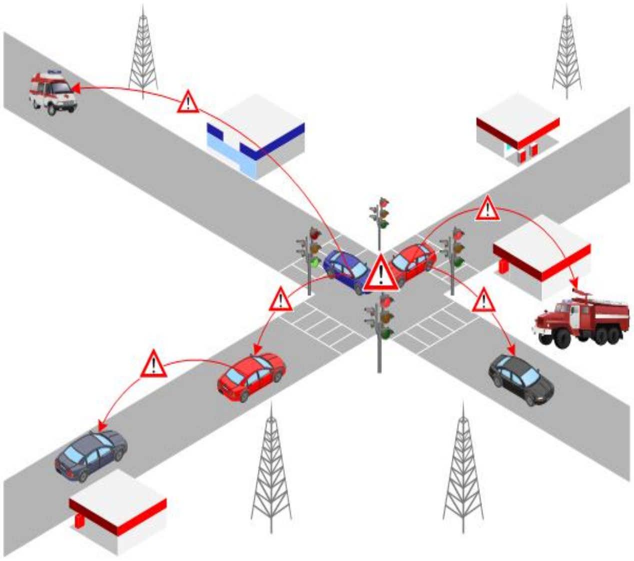

Figure 1 Configuration of Vehicular Ad hoc Networks

Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

Active Attacks: Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks involve some modification of data stream or creation of false stream. Active attacks can be internal or external.

- External attacks are carried out by nodes that do not belong to the network.
- Internal attacks are from compromised nodes that are part of the network.

Passive Attacks: Passive attacks are the attack that does not disrupt proper operation of network .Attackers snoop data exchanged in network without altering it. Requirement of confidentiality can be violated if an attacker is also able to interpret data gathered through snooping .Detection of these attack is difficult since the operation of network itself does not get affected [7-8]. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation, modification, fabrication and replication

Black hole Attack: In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol [11-13].

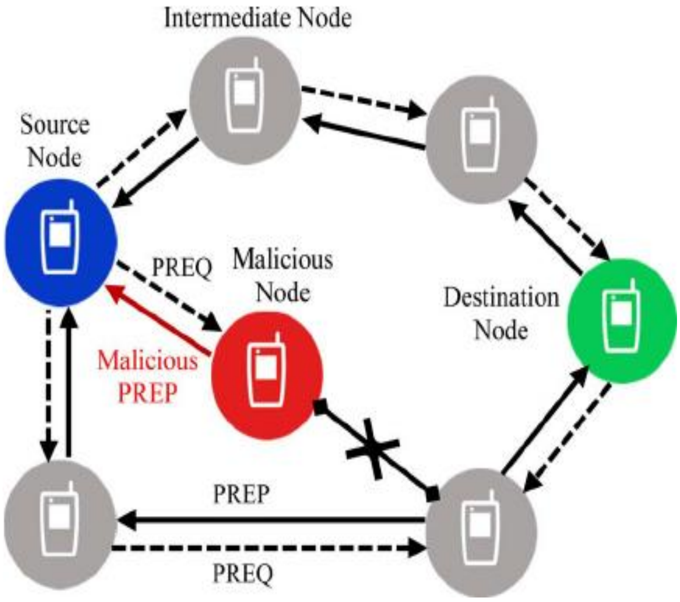

Figure 2 Scenario of Black hole attack in Networks

In VANET various routing protocol are used to give suitable outcome as per demand of applications. There are various way to classify routing protocol but in this context protocol are divided into two category, topology based and geographic based routing as depicted below.

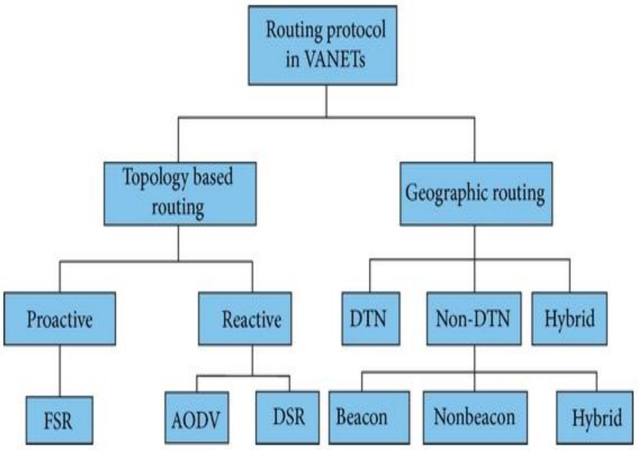

Figure 3 Routing protocols in VANET

II. LITERATURE SURVEY

Salim Lachdhaf et al: VANETs are becoming popular and promising technologies in the modern intelligent transportation world. They are used to provide an efficient Traffic Information System, Intelligent Transportation System. The mobility of the nodes and the volatile nature of the connections in the network have made VANET vulnerable to many security threats. Black hole attack is one of the security threat in which node presents itself in such a way to the other nodes that it has the shortest and the freshest path to the destination. An efficient approach for the detection and removal of the Black hole attack in the VANET is depicted in this article. The proposed AODV Routing protocol one of the most popular and able to detect both the single Black hole attack and the Cooperative black hole attack in the early phase of route discovery. The simulation is carried on NS2 and the results of the proposed scheme are compared and the fundamental AODV routing protocol [1].

Bharti et al: 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 analyzing the Black hole attack using constant bit rate and transmission control protocol traffic pattern in Manhattan Grid scenario under AODV protocol. The purpose of this paper is to analyzing the different traffic pattern with Black hole attack and without Black hole attack on the basis of Performance metrics Throughput, end-to-end delay and Packet drop ratio. The simulation setup compromises with different no. of Vehicular nodes using Constant speed [2].

Sagar R Deshmukh et al: The self configuring and infrastructure less property of MANETs makes them easily deployable anywhere and extremely dynamic in nature. Lack of centralized administration and coordinator are the reasons for MANET to be vulnerable to active attack like black hole. Black hole attack is ubiquitous in mobile ad hoc as well as wireless sensor networks. Black hole affected node, without knowing actual route to destination, spuriously replies to have shortest route to destination and entice the traffic towards itself to drop it. Network containing such node may not work according to the protocol being used for routing. This article proposes an AODV-based secure routing mechanism to detect and eliminate black hole attack and affected routes in the early phase of route discovery. A validity value is attached with RREP which ensures that there is no attack along the path. The proposed method is simulated in NS2 and performance analysis is carried out [3].

Heithem Nacer et al: VANET was proposed in order to restrict accidents and to enhance road safety. To achieve, IEEE 1609.4 was prepared to back multi-channel mechanism to assist both safety and non-safety applications in various domains. The CCH interval is also a key parameter for the 802.11p MAC protocol. In order to get a wide view of the different techniques used to broadcast a message, we evaluate the performance of the 802.11p MAC protocol with various vehicle densities and different CCH interval settings. Moreover, we propose SABM, a Scheduling Algorithm for vehicles attempting to transmit a Beacon Message, which firstly adjusts the CCH interval according to the road traffic and then schedule the safety messages based their priorities. The simulation results show that SABM outperforms the IEEE 802.11p MAC protocol. On one hand, we can significantly reduce the delivery delay and the collision probability, on the other hand, at the same time equilibrating the channel utilization ratio during CCH interval [4].

Roshan Jahan et al: Routing in vehicular ad-hoc network is current area of research due to fast mobility of vehicles. A new route in very less time has to be developed to communicate with the base station. If any node behaving like malicious and creates attack on network, than whole communication will be squeeze. This paper presents a routing strategy to prevent from attack and identify the malicious node. QualNet 5.0 software used and result compared with other routing protocols in the presence of malicious nodes [5].

Sathish M et al: AODV routing is an extensively accepted routing protocol for Mobile Ad hoc Network. The inadequacy of security considerations in the design of AODV makes it vulnerable to black hole attack. In a black hole attack, malicious nodes attract data packets and drop them instead of forwarding. Among the existing black hole detection schemes, just a few strategies manage both single and collaborative attacks and that too with much routing, storage and computational overhead. This paper describes a novel strategy to reduce single and collaborative black hole attacks, with reduced routing, storage and computational overhead. The method incorporates fake route request, destination sequence number and next hop information to alleviate the limitations of existing schemes [6].

III. TECHNICAL AND SOCIAL CHALLENGES

The technical challenges deals with the technical obstacles which should be resolved before the deployment of MANET. Some challenges are given below:

MAC Design: MANET generally uses the shared medium to communicate hence the MAC design is the key issue. Many approaches have been given like TDMA, SDMA, and CSMA etc. IEEE 802.11 adopted the CSMA based Mac for MANET.

Congestion and collision Control: The unbounded network size also creates a challenge. The traffic load is low in rural areas and night in even urban areas. Due to this, the network partitions frequently occurs while in rush hours the traffic load is very high and hence network is congested and collision occurs in the network.

Environmental Impact: VANETs use the electromagnetic waves for communication. These waves are affected by the environment. Hence to deploy the VANET the environmental impact must be considered.

Network Management: Due to high mobility, the network topology and channel condition change rapidly. Due to this, we can’t use structures like tree because these structures can’t be set up and maintained as rapidly as the topology changed.

Security Issues in VANET

In VANET various challenges existed but out of them security got less attention so far. VANET packets contains life critical information hence it is necessary to make sure that these packets are not inserted or modified by the attacker; likewise the liability of drivers should also be established that they inform the traffic environment correctly and within time. These security problems do not similar to general communication network. The size of network, mobility, geographic relevancy etc makes the implementation difficult and distinct from other network security.

Real time Constraint: MANET is time critical where safety related message should be delivered with 100ms transmission delay. So to achieve real time constraint, fast cryptographic algorithm should be used. Message and entity authentication must be done in time.

Data Consistency Liability: In MANET even authenticate node can perform malicious activities that can cause accidents or disturb the network. Hence a mechanism should be designed to avoid this inconsistency. Correlation among the received data from different node on particular information may avoid this type of inconsistency.

There are some more issue available in VANET which are listed below

- Low tolerance for error
- Key Distribution:
- Incentives
- High Mobility

IV. METHODOLOGY

In our research work prime task is to simulate proposed protocol GPSR in NS 2 environment with mobility models. Implemented research work executed step by step. First of all using NS-2.35 simulation environment is to be setup. In next step existed work is simulated followed by integration of false node to see the impact on various network parameters. In last step proposed protocol GPSR is implemented and then comparative analysis is being examined for network parameters energy, throughput, packet delivery ratio, end to end delay, Over-Head. Reporting and analysis of the results obtained in graphical form.

Flowcharts for Methodology

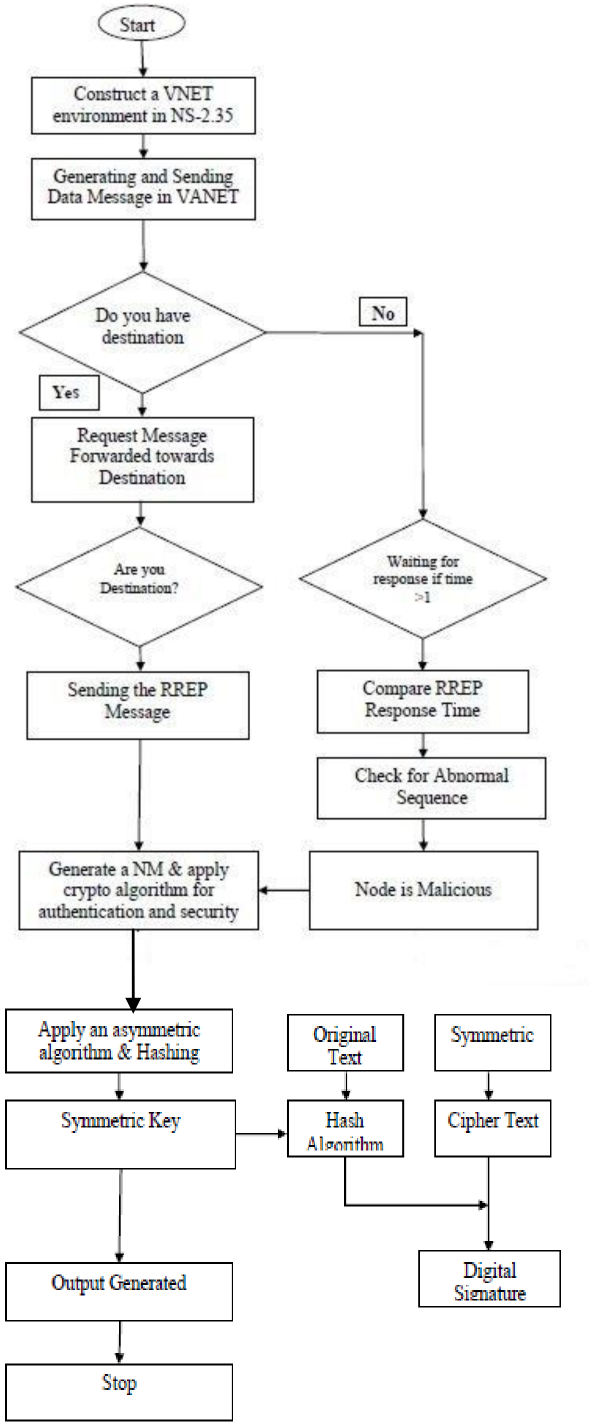
Start
Construct a VNET environment in NS-2.35
Generating and Sending Data Message in VANET
Do you have destination
No
Yes
Request Message Forwarded towards Destination
Are you Destination?
Waiting for response if time >1
Sending the RREP Message
Compare RREP Response Time
Check for Abnormal Sequence
Generate a NM & apply crypto algorithm for authentication and security
Node is Malicious
Apply an asymmetric algorithm & Hashing
Original Text
Symmetric
Symmetric Key
Hash Algorithm
Cipher Text
Output Generated
Digital Signature
Stop

Figure 4 Proposed work flow-chart

Algorithm

With the assistance of node in ns-2.35 generate a road topology. Every vehicle keeps a neighbouring database based on their current location after regular interval of time. Information data are transfer to next-hop neighbour. If a Vehicle does not receive messages from hop neighbour during a certain time duration, after then the link is lost and for route estimation a graph *G(V, E)* theory is used to consisting of a road inter-section point or topographic point $j \in J$ and road segments $c \in C$ here every portion are attached with the inter-section point.

Optimal Route Selection

```
Procedure 1: Route Discovery
Input: ID of source node S and destination node E
Outputs: Optimal routr from source to destination
Begin
If (ID E= ID N)
Forward packet to E;
Else
Determine the rectangle restricted searching area
Searching _ area=[Xmin, Xmax, Xmin, Xmax];
Broadcast RREQ to E in the searching _area
Activate (BROADCAST _TIMER)
Calculate route discovery, connectivity and packet dropping
If (p max-p other >F
Return route with discovery of connectivity pmax;
Else
Delete route with discovery of connectivity p other <pmax-p threshold;
Return route with a packet delay d min;
End if
End if
End of route discovery
```

V. RESULT AND DISCUSSION

SOFTWARE: There are several simulation tools available for validating the behavioral pattern of a wireless network environment but we opted out NS-2.35 as our tool in simulating the proposed protocol. For implementing proposed work there are various parameters required with specification so that virtual environment can be set up perfectly. In this section, we will depicts how the proposed protocol performs better in terms of energy, Throughput, PDR, average end-to-end delay of WSN.

Table 1: Simulation parameters in NS2

PARAMETERS	VALUES
Operating System	Linux (Ubuntu 12.04)
NS-2 version	NS-2.35 for IEEE 802.11Ext
No. of vehicles	10, 20, 30, 40,50
Number of Road Segments	4
Speed of vehicles	20 m/sec.
Radio propagation model	Propagation/Two Ray Ground
Network interface type	Phy /Wireless PhyExts

Packet Size	512
Traffic Type	UDP-CBR
Execution Time	100sec
Antenna Type	Omni-Antenna
Transmission Range	1000*1000 m
Routing Protocol (Proposed)	AODV,GPSR, CA, Hash function
Rx power	0.3
Tx power	0.6
Initial Energy	90
Interface Queue Length	200
Mobility Model	Manhattan Mobility Model

Table 1 shows various parameters values required to simulate virtual environment so that result can be verified. In networking always omnidirectional antenna is used.

End-to-End Delay

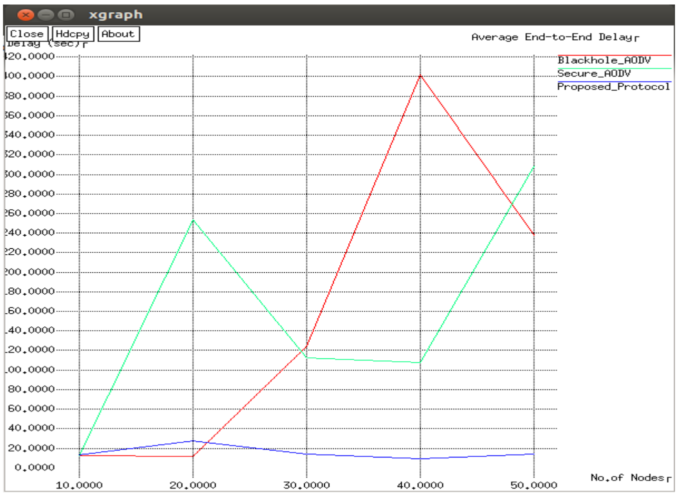

Figure 5 Comparison of average end-to-end delay

Energy Consumption

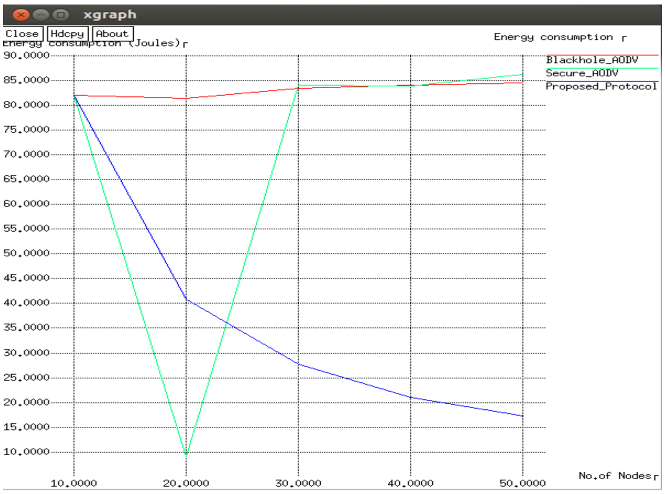

Figure 6 Comparison of Energy Consumption

Packet Delivery Ratio

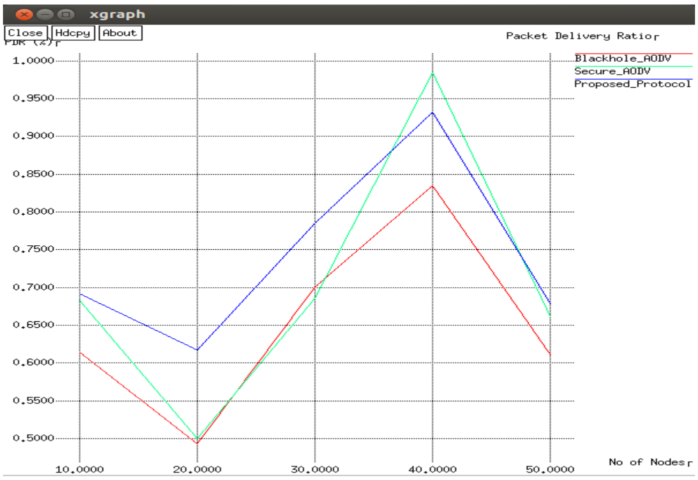

Figure 7 Comparison of Packet Delivery Ratio

Throughput

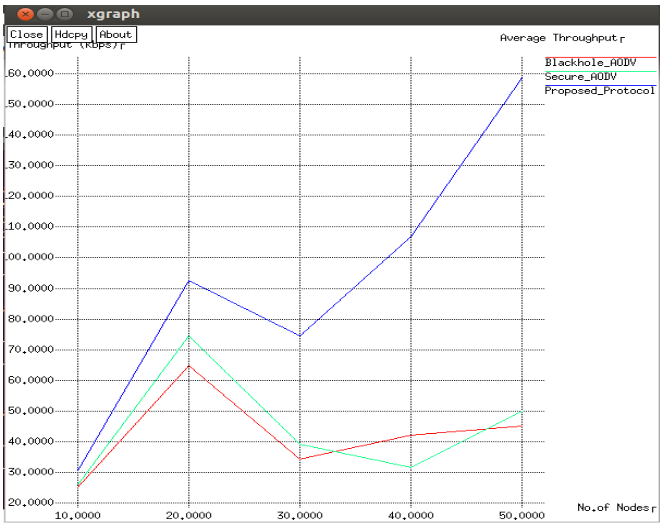

Figure 8 Comparison of Throughput

Overhead

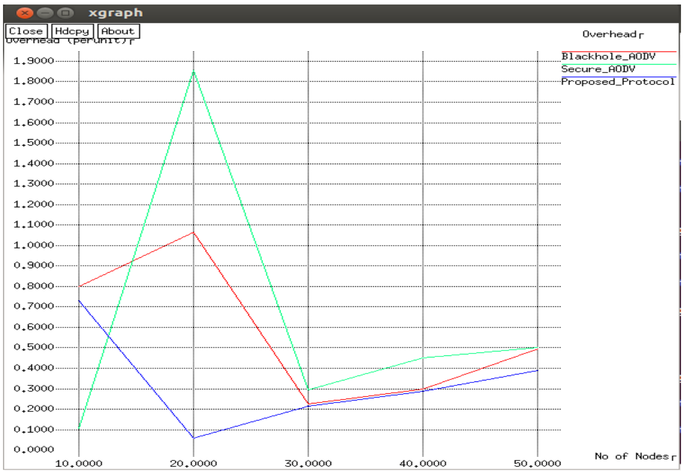

Figure 9 Comparison of Overhead

Malicious Node Simulation Result for 50 Nodes

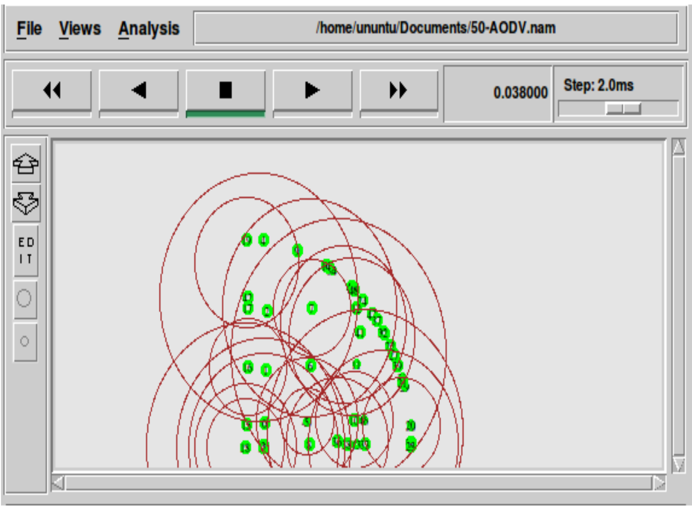

Figure 10 Initial stages for nodes showing their respective position

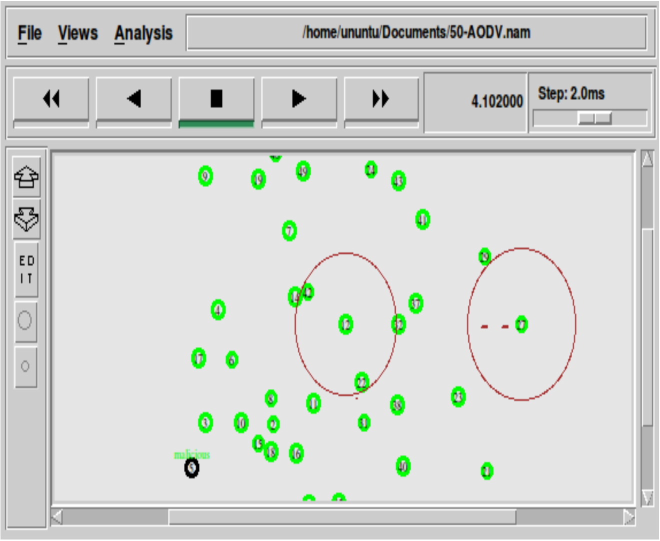

Figure 11 Transmission between node 12 and 27, Node 5 is malicious node

AODV Protocol Simulation Result for 50 Nodes

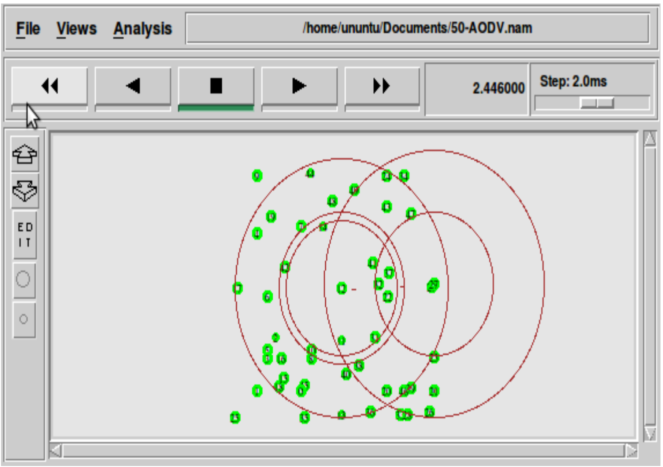

Figure 15 Cluster formed and data transmission between node 27 and 12

VI. CONCLUSION

Vehicular ad hoc networks are wireless and infrastructure less networks created spontaneously. The black hole attack is an attack vector that can significantly reduce the availability of Vehicular Ad Hoc Networks and prevent communication between devices entirely. The network vulnerability is more possible with the sensor nodes in an unattended environment. Wireless Sensor networks are gradually increased used by military, health, environmental and commercial applications. VANET is a part of MANET and it is specific application oriented. This network can be established at nadir situation where a conventional network cannot be deployed. Deploying VANET there are technical and social challenges. Concern of security in implementing of VANET is crucial parameter. In our base work black hole attack used in network communication using AODV protocol. In NS 2 environment implementation of black hole attack, secure black hole attack and GPSR protocol executed and a comparative analysis of these executed successfully and result of proposed protocol is better than existed protocol. As technology came into existence side by side unethical activity also take place which try to access the data illegally. In our research work, implemented GPSR protocol is integrated with security algorithm to provide secure networks against this vulnerability by detecting the attack and removing the malicious node from the network.

REFERENCES

[1]. Waleed Kh. Alzubaidi, Shaimaa H. Shaker, “Methods of Secure Routing Protocol in Wireless Sensor Networks”, Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.3 Year 2018, 2521 – 3504

[2]. Jyoti Neeli, N K Cauvery, “Insight to Research Progress on Secure Routing in Wireless Ad hoc Network ”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017

[3]. Mahesh Kumar, Mr. Kuldeep Bhardwaj,”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]. 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

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

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

[7]. C. Li, Z. Wang, and C. Yang, "Secure routing for wireless mesh networks", International Journal of Network Security, vol 13, no 2, pp. 109-120, 2011

[8]. P. Tomar, P.K. Suri, M.K. Soni, "A Comparative Study for Secure Routing in MANET", International Journal of Computer Applications, Vol.4(5), pp.17-22, 2010

[9]. M. Yu, M. Zhou and W. Su, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments," in IEEE Transactions on Vehicular Technology, vol. 58, no. 1, pp. 449-460, 2009.

[10]. Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", In Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), Callicoon, NY, USA, pp. 3 – 13, 2002