ISSN : 2231-0711

Gurleen Kaur et al | IJCSET(www.ijcset.net) | July 2015 | Vol 5, Issue 7,234-239

# Improved AODV routing protocol for mitigating effects of Grayhole Attack in VANET using Genetic Algorithm

Gurleen Kaur [#1], Ms. Sudesh Rani[*2], Dr.Trilok C. Aseri[#3]

[1,2,3]*Department of Computer Science & Engineering*
*PEC University of Technology*
*Chandigarh, INDIA*

*Abstract*— **Recent advancement in technology related to wireless communication has given rise to VANET.VANET is the application of MANET that relies on vehicles for network functionality and prone to many kinds of attack. Grayhole attack is one of the common Denial Of service attack that causes malicious change in the routing process of effected nodes.Grayhole attack adversely effects various network parameters like throughput, end to end delay, packet delivery ratio and other concerned parameters. Due to lack of security in Ad hoc on demand distance vector routing protocol, Grayhole attack disrupts the performance of network and render communication impossible.This paper proposes metaheuristic algorithm genetic algorithm for minimizing the effect of grayhole attack in VANET and enhancing the network against attack. The performance of the network has been evaluated using average throughput, bit error rate, average end to end delay, and packet delivery ratio and packet loss. The GA shows a relevant good amount of growth in each and every parameter of the calculations.**

***Keywords***— *Vehicular Ad hoc Network (VANET), Ad-hoc On Demand Distance Vector (AODV), Route Request (RREO),Route Reply(RREP), Denial of Service Attack(DOS),Genetic Algorithm(GA)*

## I. INTRODUCTION

In the recent years, vehicular networking has gained a lot of popularity among the industry and academic research community and is seen to be the most valuable concept for improving efficiency and safety for future transportations. A number of research and studies have been undertaken to develop intelligent systems for interconnecting vehicles and widen the driver's horizon to ascertain the events or incidents which otherwise are hard to observe with the existing common board tools[1]. Being ad-hoc in nature, VANET is a type of network that is created from the concept of establishing a network of cars for a specific need or situation. VANETs have now been established as reliable networks that vehicles use for communication purpose on highways or urban environments [2]. The deployment of VANET's can enhance and improve road safety and comfort level by vehicle to vehicle communication networks. VANET and MANET share some identical features. Nodes in VANET and MANET are localized and characterized by their pattern of movement and self organization properties. Nodes in VANET are not constrained by movement or power availability unlike nodes in MANET.VANET have large network which are publicly available on the road at any time. Security is detrimental factor as it is directly concerned with life threatening conditions on daily basis. 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[3]. The system must be able to verify credible information pertaining to drivers while maintaining their privacy as well. This is an uphill task because of the extensive size of network, geographical positions, irregular connectivity between nodes and varying speed of the vehicles. The system reliability falls under dangerous scrutiny wherein in information collected and transmitted between entities in a network raising concerns about the authenticity of the data. Since majority of VANET messages are concerned with driving conditions and road safety, real time processing of such critical messages are significant. To ensure the given real time constraints the security infrastructure must be highly efficient in terms of computational and bandwidth requirements. This paper is divided into six sections; Section II describes literature survey, Section III describes proposed methodology, Section IV describes design solution and details, Section V describes simulation and results .Finally Section VI concludes the work and describes future scope.

A. *Grayhole attack:* Grayhole attack is a modified version of blackhole attack in which it is difficult to predict the malicious node's behaviour. It can be performed by three ways. The first way is that malicious node may drop incoming packets while allow some packets to pass. In second, malicious node may behave as normal for some time and malicious for a certain time. In third type, malicious node may drop incoming packets from some specified nodes for some time and later on it behaves as a normal node. These different types of behavior make attack difficult to detect. Grayhole attack finally disrupts the network's performance by interfering with the route discovery process [4].

- Grayhole attack operation:

Fig. 1 shows a VANET using AODV routing protocol. In the first figure, initially, node A acts as normal node and allows all incoming packets from source S to the required destination D. But afterwards it behaves as a malicious node and starts dropping packets that are sent from source S to destination D. After some time, A behaves again as normal node as earlier. Therefore, A behaves maliciously for a certain period and becomes normal again. AODV routing protocol has no feature for finding and blocking a malicious node .Due to lack of security mechanism in AODV routing protocol, malicious nodes can perform many attacks. This attack is represented in Fig.1 given below.

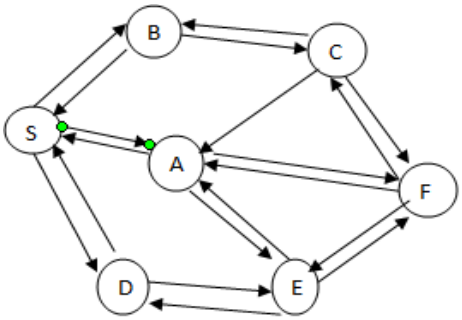


**Fig 1: Grayhole attack**

*B. Genetic Algorithms:*

Genetic algorithms came into existence in 1958and popularized in early 1970s by John Holland [5] .They are population based optimization algorithms that finds optimal solution to difficult problems by motivation from nature. They are based on the phenomenon of general science and natural. Working of GA can be explained as follows:

1) The algorithm starts with a random number generator that generates a set of strings. Each string is called a chromosome. Next fitness evaluation unit evaluates the fitness of each string .A fitness value represents information of how good is each candidate.
2) Next role of genetic operators come. They convert the sets of strings called chromosomes into higher fitness values. The reproduction operator allows that each string is copied based on their fitness values. The higher the fitness value more is the chance of getting selected for the next generation.
3) Crossover operator randomly exchange bits between two selected strings. Mutation operator performs mutation. It reverses the value of bits in a string. Therefore, for a single phase, this algorithm undergoes selection,reproduction,crossover and mutation.

## II. RELATED WORK

Chen *et al.*[6] had proposed a solution against grayhole attack in MANET. Two related algorithms are proposed: the key management algorithms based on gossip protocol and detection algorithm based on aggregate signatures. Most of the malicious nodes could be detected by lowering the false positive rate, routing overhead and improving PDR. Sukhla *et* al.[7] proposed a mechanism for detecting and removing blackhole and grayhole attack that uses the two types of messages: prelude and postlude messaging. The technique is capable of finding cooperating grayhole/blackhole nodes which drop a large fraction of packets. Devu *et al.* proposed channel aware detection algorithm to detect grayhole attack in mesh nodes. A detailed design is also presented that analysis the false alarm and missed detection probabilities of CAD .Gihan et al. [9] had developed a genetic algorithm that finds the shortest path between source and destination. The proposed genetic algorithm is compared with the previous search technique Dijkstra's algorithm and found that it has got the same potential as that of Dijkstra's algorithm. Michael et al.[10] explored the biological inspired research in computer network. The article made a connection between biology and computer networks. A broad survey of biological inspired research that can be fitted in computer network is provided. Ming et al.[11] proposed Antiblackhole mechanism that deployed several IDS nodes to detect and prevent grayhole attack in MANET. This mechanism is based on the suspicious value of a node that is calculated by taking into account the amount of abnormal difference between RREO and RREPs transmitted from a node. With the help of an IDS node broadcasting a block message, all nodes cooperatively isolated and banned the malicious nodes for next routing.

## III. PROPOSED METHODOLOGY

Genetic algorithm is one of the most powerful algorithms for the optimization of the data of any kind. The only problem with this algorithm is that it takes everything in terms of numeral data hence if the fitness function is based on some value which must has to be string then either its ASCII or binary value would be utilized. It consists of following features:

- **Selection:** gives preference to better individuals, letting them offer their genetics to another technology. This amazing benefit of every specific is dependent upon the fitness. Fitness may be driven by an objective function or perhaps by way of a very subjective judgment.
- **Crossover:** represents mating concerning individuals; a couple individual is chosen in the population using the selection operator. Any crossover site over the bit strings is actually randomly picked. The significance of every string is actually exchanged up to this point. Each new young offspring made from this specific mating are placed in your next generation from the population. By recombining portions connected with great individuals, this method probably will develop better individuals.
- **Mutation:** features random alterations. The purpose of mutation is always to keep diversity within the population and prevent uncontrolled convergence. With a number of low chances, a small portion of the new individuals will have some of their bits dipped. Mutation as well as assortment (without crossover) develops parallel, noise-tolerant, hill-climbing algorithms. This pseudo rule connected with genetic algorithms is actually found beneath

**1. Stopping criterion:** The goal of stopping criterion is to stop the GA evolutionary process. Here, a pre-set number of iterations is adopted to stop the evolution. It can be explained in Fig.2 below:

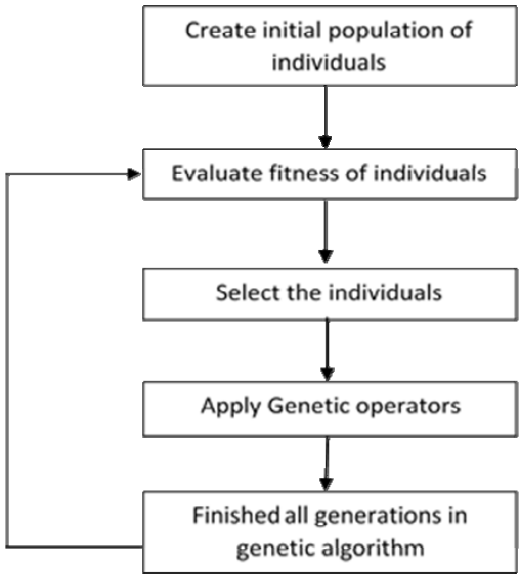


**Fig.2: Flowchart of GA**

**I**n the presented research work, the genetic algorithm has been applied using Matlab and Matlab has an Optim toolbox which has all its fitness function values.

The population size of the Genetic algorithm has been initialized as 50 which is on a later stage is adjusted as the total number of nodes which has been taken as the network nodes. The mutation value would be decided according to the fitness function which is as follows

f=0 if Fs < Ft

f=1 other wise

where Fs is the current feature set of the current node taken under consideration and Ft is the fit value for the same .If the value of fs is less than that of the ft then the node is set to be ok and it is not termed as malicious or a Gray hole node, else it is considered as a gray hole node and the fit value for the same is reduced accordingly. To apply genetic algorithm in MATLAB first of all , all its options is set with the use of gaoptimset command which may have the value of the population size , mutation , crossover which is linear in this case and then the fitness function which must be a separate file which would be called from the ga() function.

## IV. DESIGN SOLUTION AND DETAILS

The design solution is designed and detailed keeping in view the nature of the vehicular ad-hoc network as well as the characteristics of the Grayhole attack. The attack pattern was closely studied and observed through existing works presented on the attacks and its impact on the VANET. The nodes were configured to a mobility model to portray a vehicular ad-hoc environment constantly in mobile fashion. The structure of the proposed algorithm is designed in such a manner that it takes care of the architecture of VANET and the entire basic design model AODV protocol. The network has been designed with a 1000 meter width and 1000 meter length and nodes varying from 20 to 80 nodes in which the 3rd node each and every time would be the source node and the 8th node would be destination. The location of the source and destination is also fixed and the other nodes are moving with a speed of maximum 10 km/h. The entire network has been designed using MATLAB 2010 and communication system toolbox .The system has been tested with the Artificial Bee Colony Algorithm and Genetic algorithm. A fitness function for the genetic algorithm has been designed which has been called with the help of the optimization tool box (in built with MATLAB SETUP).Fig 3 below describes design flowchart .

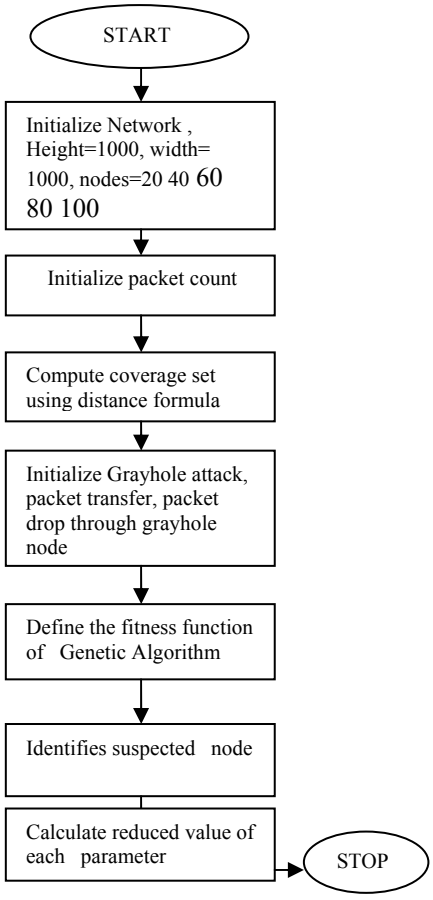


Fig 3: Design flowchart

## V. SIMULATION AND RESULTS

The Simulations were carried out in MATLAB version 7.11.0.584 (R2010b) software and results were obtained comparing the network efficiency and stability through the parameters: Throughput, end to end delay, packet delivery ratio, bit error rate and packet loss.

### *A. Simulation Environment*

The simulations have been carried out in MATLAB version 7.11.0.584 (R2010b) software for the VANET. The analysis of various population based optimizations revealed that genetic algorithm is the most suitable optimization technique. The structure of the proposed algorithm is designed in such a manner that it takes care of the architecture of VANET and the entire basic design model AODV protocol. The network has been designed with a 1000 meter width and 1000 meter length and nodes varying

from 20 to 80 nodes in which the 3rd node each and every time would be the source node and the 8th node would be destination. The location of the source and destination is also fixed and the other nodes are moving with a speed of maximum 10 km/h. The system has been tested with attack and after applying genetic algorithm.

**Table I**
**Simulation Parameters**

| Parameter | Values |
|---|---|
| Simulator Used | MATLAB |
| Routing protocol | AODV |
| Area | 1000*1000 m |
| No of vehicles | 20,40,60,80,100 |
| Mobility | 10km/h |
| Packet Size | 512 bytes |

*B. Performance metrics:* Various performance metrics are used for comparison like average end to end delay, packet delivery ratio, average throughput, packet loss, bit error rate.

1) **Average end to end delay:** When a data packet is sent by the source node to the destination, then the time taken by the data packet to reach the destination from source node is known as end to end delay. The average end to end delay for all successfully delivered packets is calculated by taking its mean value.

$D = (1/n)*\Sigma_{i=1} (T_r - T_s) * 1000$ [ms]

Where

D = Average E2E Delay

i = packet identifier

$T_r$ = Reception time

Ts = Send time

n = Number of packets successfully delivered

2) **Packet Delivery Ratio:** The ratio of data packets received by the destination node to the data packet sent by the source node is defined as the packet delivery ratio.

3) **Average Throughput:** This is the measure of the rate at which data being successfully delivered over a communication channel. It is usually measured in bits per second (bit/s or bps).

4) **Packet Loss:** This metrics measure the number of data packets created by the source node but never been reached to the destination node.

5) **Bit error rate:** BER is number of bit errors divided by total number of transferred bits in a specified time interval. It is measured in percentage.

*C. Simulation Results: Simulation results are shown below:*

***1) Network Simulation:*** The nodes are configured to a mobility model to portray a vehicular Adhoc network constantly in mobile fashion. Network has been created which consists of length and width of size 1000*1000m.Fig 4 shows the network simulation.

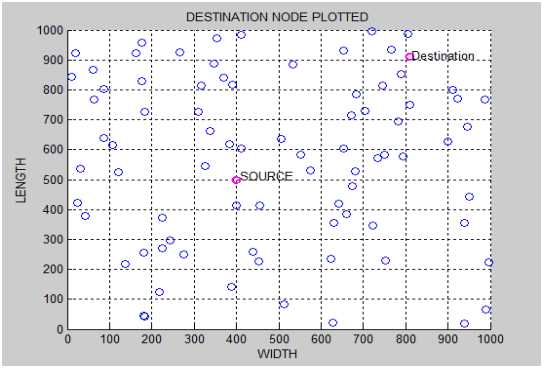


**Fig 4: Network Simulation**

***2) Grayhole Attack simulation:***

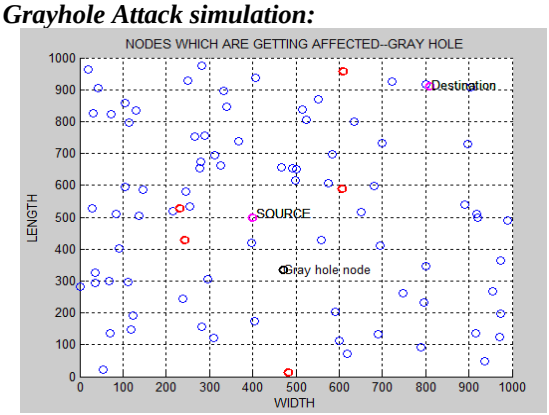


**Fig.5: Grayhole Attack Simulation**

The above figure demonstrates the total number of nodes, source node and the destination node along with those nodes which are getting affected. It is sort of obvious that a node which is under attack will not remain silent and it will leave effects over others. The malicious nodes may redirect the packets to their preferred location or may discard them. As a result of which the legitimate nodes within a network may be devoid of emergency warning or alert messages or route path to their destinations.

***3) Comparison of average throughput of AODV under attack and under optimization with genetic algorithm:*** The figure 7 shows that result has been made for one of the major factor to be demonstrated named throughput with varying number of nodes. It shows the comparative analysis of the parameter average throughput under attack and after optimization with genetic algorithm. It shows that throughput of the AODV routing protocol with genetic algorithm is improved than throughput under attack.

Table II
**Average throughput in bps**

| No of nodes | With Attack | With GA |
|---|---|---|
| 20 | 327.68 | 415.48 |
| 40 | 237.568 | 389.12 |
| 60 | 241.664 | 397.312 |
| 80 | 294.912 | 401.408 |
| 100 | 306.22 | 405.279 |

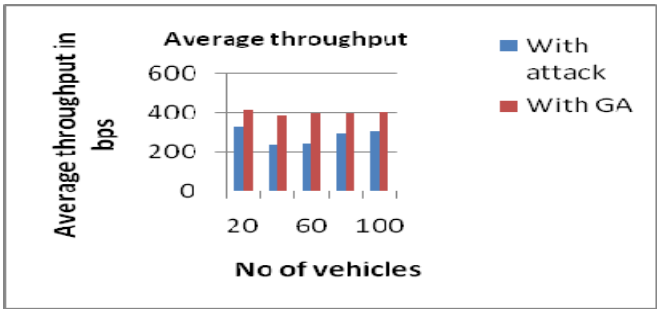


**Fig 6: Average throughput with attack and with GA vs. no of vehicles**

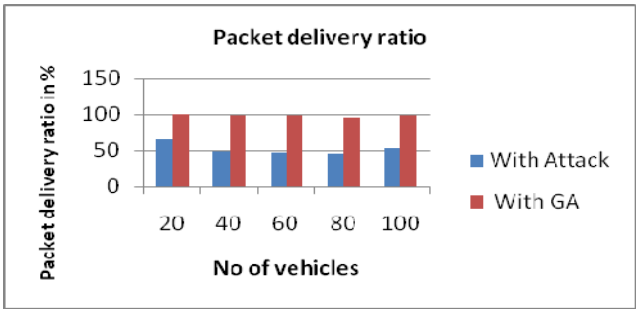


**Fig 8. Packet delivery ratio**

***4) Comparison of average end to end delay of AODV under attack and under optimization with genetic algorithm:*** Table III shows simulation results with respect to average end to end delay vs. number of nodes. Our proposed scheme using AODV with GA considerably reduces end to end delay

**TABLE III**
**Average end to end delay in ms**

| No of nodes | With attack | With GA |
|---|---|---|
| 20 | 5.474 | 0.2017 |
| 40 | 5.547 | 0.2518 |
| 60 | 6.568 | 0.2647 |
| 80 | 6.782 | 0.3046 |
| 100 | 6.829 | 0.3192 |

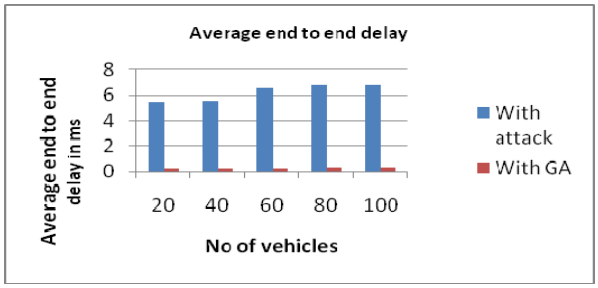


**Fig 7**

Figure 7 shows that end to end delay is considerably reduced with our proposed mitigation strategy.AODV with attack has more end to end delay than our proposed AODV with GA.

***4) Comparison of packet delivery ratio of AODV under attack and under optimization with genetic algorithm*:**
Table IV shows simulation results of Packet delivery ratio of AODV routing protocol with attack and with GA vs. varying number no nodes with attack and with GA

**Table IV**
**Packet delivery ratio in %**

| No of nodes | With attack | With GA |
|---|---|---|
| 20 | 65.7349 | 99.8755 |
| 40 | 48.2514 | 98.6405 |
| 60 | 46.5103 | 97.8821 |
| 80 | 44.7552 | 95.8951 |
| 100 | 52.8741 | 98.2598 |

Figure 8 denotes that packet delivery ratio of AODV routing protocol with genetic algorithm is more than AODV with attack.

***6) Comparison of Bit error rate of AODV under attack and under optimization with genetic algorithm:***
Table V shows Bit error rate of AODV with attack and with genetic algorithm

**Table V**
**Bit error rate**

| No of nodes | With attack | With GA |
|---|---|---|
| 20 | 0.427 | 0.223 |
| 40 | 0.618 | 0.489 |
| 60 | 1.842 | 1.676 |
| 80 | 1.889 | 1.726 |
| 100 | 1.928 | 1.749 |

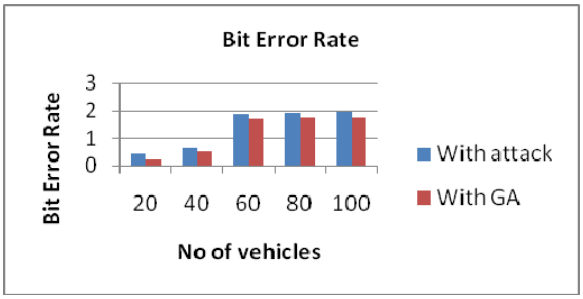


**Figure 9: Bit error rate**

Figure 9 shows that bit error rate in the network using AODV with attack is more than our proposed scheme using AODV with genetic algorithm**.**

***7) Comparison of packet loss of AODV under attack and under optimization with genetic algorithm*:**
Table VI shows simulation results of packet loss of AODV with attack and with GA with varying number of nodes

**Table VI**
**Packet loss**

| No of nodes | With attack | With GA |
|---|---|---|
| 20 | 0.3321 | 0.0069 |
| 40 | 0.5174 | 0.0174 |
| 60 | 0.5384 | 0.0279 |
| 80 | 0.5454 | 0.0489 |
| 100 | 0.5174 | 0.0139 |

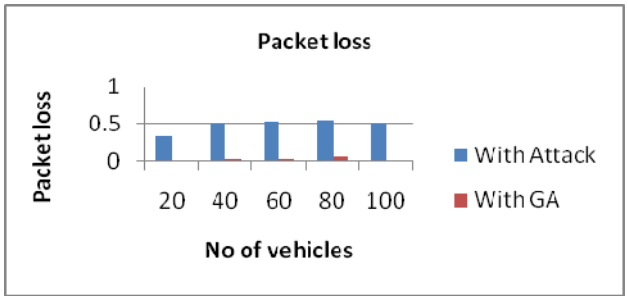


**Figure 10: Packet loss**

Figure 10 show that AODV with attack incur more packet loss than our proposed AODV with GA.

## VI. CONCLUSION AND FUTURE SCOPE

Applications in VANET are important and these applications must be secured; if attackers change the content of these applications then users are directly affected from it. It is very difficult to monitor the behaviour of attacker, attackers change his/her attacking behaviour and they launch different attacks at different time frame. In this paper, the proposed algorithm presents a unique solution to mitigate the effects of gray hole attack in AODV routing protocol in VANET. In the proposed system, a node range of 20 to 100 has been taken over a network with the height and width of 1000 meters. The mobility of nodes can gain a maximum of 10km/hour & the source and the destination has been kept fixed. The system has been evaluated 10 times under the effects of gray hole attack & the effects of the attack has been tried to be removed using using Genetic Algorithm .The experimental results shows that the performance of GA in mitigation of the gray hole attack in AODV routing protocol in VANET is pretty good. The performance of the network has been evaluated using average throughput, bit error rate, average end to end delay, and packet delivery ratio and packet loss. The GA shows a relevant good amount of growth in each and every parameter of the calculations.

## REFERENCES

[1] Chandrasekaran, Gayathri. "Vanets: The networking platform for future vehicular applications." *Department of Computer Science, Rutgers University*(2008).

[2] ur Rehman, Sabih, et al. "Vehicular Ad-Hoc Networks (VANETs)-An Overview and Challenges." *Journal of Wireless Networking and Communications* 3.3 (2013): 29-38.

[3] Raw, Ram Shringar, Manish Kumar, and Nanhay Singh. "Security challenges, issues and their Solutions for VANET." *International Journal of Network Security & Its Applications (IJNSA)* 5.5 (2013).

[4] Jhaveri, Rutvij H., Sankita J. Patel, and Devesh C. Jinwala. "DoS attacks in mobile ad hoc networks: A survey." *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on*. IEEE, 2012.

[5] Raghay, S., S. El Hadaj, and T. Noel. "A GENETIC ALGORITHM FOR MANAGEMENT DATA STREAM IN VANET." *International Journal of Information Technology* 4.1 (2011): 315-318.

[6] Chen Wei, Long Xiang, Bai Yuebin and Gao Xiaopeng.,2007, New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks, Second International Conference on communications and Networking ,China, pp. 366-370.

[9] Nagib, Gihan, and Wahied G. Ali. "Network routing protocol using Genetic Algorithms." *International Journal of Electrical & Computer Sciences IJECS-IJENS* 10.02 (2010): 40-44.

[7] Sukla Banerjee,2008.Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks, World Congress on Engineering and Computer Science , pp. 337-342.

[8] Devu Manikantan Shila, Yu Cheng_ and Tricha Anjali,2009,Channel-Aware Detection of Gray Hole Attacks in Wireless Mesh Networks,IEEE Global Telecommunications Conference, pp. 1-6.

[10] Meisel,Michael,Vasileios Pappas, and Lixia Zhang2010,A taxonomy of biologically inspired research in computer networking,pp.901-916

[11] Ming-Yang Su.,2010,Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", Computer Communications.