IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

MITIGATION OF BLACK HOLE ATTACK USING GENERIC ALGORITHMS AND FUZZY LOGIC

Rajesh Kumar*, Dr. Raman Chadha
* M.Tech(CSE), Chandigarh Group of Colleges Technical Campus, Mohali
Professor, Head(CSE), Chandigarh Group of Colleges Technical Campus, Mohali

ABSTRACT

A black hole is a node that always responds positively to every PREQ, even though it does not really have a valid route to the destination node. Since a black hole does not have to check its routing table, it is the first to respond to the PREQ in most cases. There are two sorts of black hole attack could be defined in AODV with the purpose of differentiate the type of black hole attack. At present, several efficient routing protocols have been proposed for VANET. Most of these protocols assume a trusted and cooperative environment. However, in the presence of malicious nodes, the networks are vulnerable to various kinds of attacks. In VANET, routing attacks are particularly serious. So, this proposed work tries to design and implement fuzzy and GA algorithm with Black hole attack in AODV and prevent the system for threat using this hybridization.

KEYWORDS: Black hole attack, AODV, VANET, Genetic Algorithm.

INTRODUCTION

Black hole attack in Vehicular Ad Hoc Network is major problem related with the field of computer networking. 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. In order to form a communication system, the vehicles weave an unstructured network known as Vehicular Ad-hoc Network (VANET) [1]. The forecast of vehicle position and their developments is extremely troublesome. This highlights of portability demonstrating and forecast in VANETs is in view of the accessibility of predefined guide's models. The rate of the vehicles is again an imperative for productive system outline. In this work, we present the performance analysis of the black hole attack in Vehicular 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. Ad-Hoc network routing protocols are commonly divided into three main classes; Proactive, Reactive and Hybrid protocols as shown in figure below:

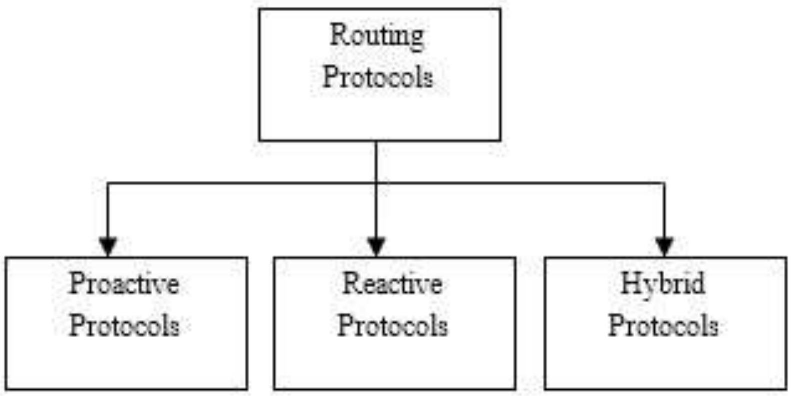

Figure 1: Routing protocols in VANET

Proactive Protocols

Proactive Protocol or table driven directing protocol In proactive routing, every hub needs to keep up one or more tables to store directing data, and any adjustments in system topology should be reflected by spreading upgrades all through the system to keep up a steady system view. e.g.: Destination sequenced distance vector (DSDV). They try to look after predictable, up and coming directing data of the entire system. It minimizes the delay in correspondence and permit hubs to rapidly figure out which hubs are available or reachable in the system.

Reactive Protocols

Reactive protocols is otherwise called on-demand directing protocol since they don't keep up directing data or directing action at the system hubs if there is no correspondence. In the event that a hub needs to send a bundle to another hub then this convention scans for the route in an on-interest way and sets up the connection so as to transmit and get the packet. E.g. Ad-hoc On-interest Distance Vector protocol (AODV) and Dynamic Source Routing (DSR).

Hybrid Protocols

It consolidates receptive and proactive directing protocols. The Zone Routing Protocol (ZRP) is a half breed directing protocol that partitions the system into zones. ZRP gives a various leveled structural engineering where every hub needs to keep up extra topological data obliging additional memory.

Table 1: Difference between VANET and MANET

MANET	VANET
A mobile ad-hoc network (MANET) is a self-configuring infrastructure- less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently	Vehicular Ad hoc Network (VANET) is a subclass of mobile Ad Hoc networks (MANETs). These networks have no fixed infrastructure and instead rely on the vehicles themselves to provide network functionality. While such a network does pose certain safety concerns but this does not limit VANET's potential as a productivity tool. GPS and navigation systems can benefit, as they can be integrated with traffic reports to provide the fastest route to work [16]
MANET can contain many nodes that have un-controlled moving patterns	VANET is formed mainly by vehicles so node movement is restricted by factors like road course, traffic and traffic regulations. Because of the restricted node movement it is quite likely that the VANET will be supported by some fixed infrastructure that provide some services and access to stationary networks. The fixed infrastructure will be deployed at critical locations like slip roads, service stations, dangerous intersections or places well-known for hazardous weather condition.

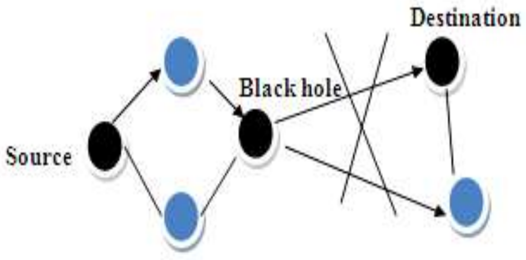

Figure 2: Black hole attack

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 [7]. 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.

There is growing age and there is important need of communication protocol over wireless system. Then AODV protocol came into existence. AODV is an on –Demand routing protocol which is confluence of DSDV as well as DSR. Route is computed on request, at the same time as it is in actual DSR by means of route detection process. That is why it is called reactive protocol.

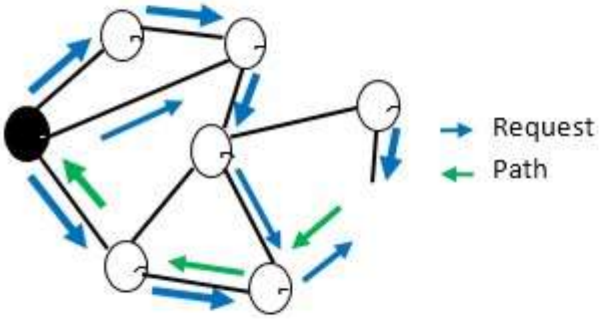

Figure 3: AODV protocol

An ad-hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure. AODV sends packets only when there is need, so the bandwidth wastage has been reduced.

Fuzzy logic provides the strength to obtain the uncertainties associated with human process. The need of fuzzy logic arises in the time to describe the principle of and problem of uncertainty. It is a rigorous mathematical field, and it provides an effective vehicle for modeling the uncertainty in human reasoning. In fuzzy logic, the knowledge of experts is modeled by linguistic rules represented in the form of IF-THEN logic. A fuzzy set is uniquely determined by its membership function (MF), and it is also associated with a linguistically meaningful term. Fuzzy logic provides a systematic tool to incorporate human experience. It is based on three core concepts, namely, fuzzy sets, linguistic variables, and possibility distributions.

The importance of fuzzy logic derives from the fact that most modes of human thinking and especially common sense reasoning are approximate in nature. The essential features of fuzzy logic are as follows [21]:

- In fuzzy logic everything is a matter of degree.
- Any logical system can be fuzzified.
- In fuzzy logic, knowledge is interpreted as a collection of elastic or, equivalently, fuzzy constraint on a collection of variables.
- Inference is viewed as a process of propagation of elastic constraints.

As genetic algorithm optimize the searching problem using intelligent exploitation method and it is the main technique to simulate the processes for evolution. They work on the fitness function. Each generation consists of the population as we can see in our DNA [24]. Each individual of population represents the search space or possible solution. Each individual in population leads to the evolution.

Steps of Genetic Algorithm

Step 1: Initialize random population consists of chromosomes.
Step 2: Compute fitness function in the population.
Step 3: Develop new population consists of individuals.
Step 4: Selection of parent chromosomes to get best fitness function.

Step 5: Perform crossover to get copy of parents.
Step 6: Perform mutation to mutate new off springs.
Step 7: Place new offspring into the population.
Step 8: Repeat steps to get a satisfied solution.
Step 9: Stop

RELATED WORK

D. E. Tim Lienmullar et.al, 2009, has conducted a security analysis to understand the behavior of attackers that causes security attacks in the network. Saira Gillani, et.al, 2013, has reviewed the various dimensions of VANETs security including security threats, challenges in providing security in vehicular networks environment, requirements and attributes of security solutions. Sedjelmaci, H. and Senouci, S.M., 2014, has designed and implemented a new Intrusion Detection Framework for Vehicular Networks (IDFV). These networks are vulnerable to various security attacks due to the lack of centralized infrastructure. The aim of this framework is then to secure them against the most dangerous routing attacks that have a high severity damage such as selective forwarding, black hole, wormhole, packets duplication and resource exhaustion attacks that can target such networks. Hanin Almutairi, et.al, 2014, has addressed a key topic in the field of computer networking security which is the detection of black hole nodes in VANETs "Vehicular Ad Hoc Networks" that are vulnerable to security attacks due to its infrastructure less nature. Bassem Mokhtar, and Mohamed Azab, 2015, has overviewed VANETs for clarifying their security requirements and challenges. Vehicular Ad hoc Networks are special case of ad hoc networks that, besides lacking infrastructure, communicating entities move with various accelerations. Tans et.al, allows mobile hosts to begin a communication with each other over a network without an established infrastructure or a central network authority. Because of this, MANETs have active topologies because nodes can easily join or leave the network at any time. Wei Li, has proposed a Genetic Algorithm based intrusion detection system which was tested with TCP/I networks. This made use of spatial and temporal29 ICRTIT-2012implementations of network based connections in encoding the network based rules.

SIMULATION MODEL

This paper discusses one of the most advanced security threats in the ad-hoc routing and enhancement namely BLACK HOLE ATTACK. In this attack all the network traffic is redirected to a specific node which does not exist at all. This specific node is known as black hole. The defending mechanism would be classified using fuzzy logic to check the effectiveness of the evaluated discovery mechanism. This research work also aims to mitigate the effects of black hole attack by designing a unique fitness function which would be applied over Genetic Algorithm.

In the end proposed technique measurement will be done using basic matrices like throughput, End to End Delay, Bit Error Rate, and Packet Delivery Ratio. In which network will be developed based on given no. of nodes as well as specification of area having breadth and length.

X and y locations of the nodes
%net_area=net_length*net_width;
calculate the xloc yloc and time_stamp of each nodes
Select the cluster head by considering the time_stamp of the current block with avg time_stamp measure of x and y location distance find the coverage set of each node from others check that whether destination is available or not selecting any node from the coverage set of the current node plot the source and destination in the same figure where the other nodes are already plotted plotting the route nodes Identify black node Optimize using trained fuzzy and GA algorithm Calculate parameters.

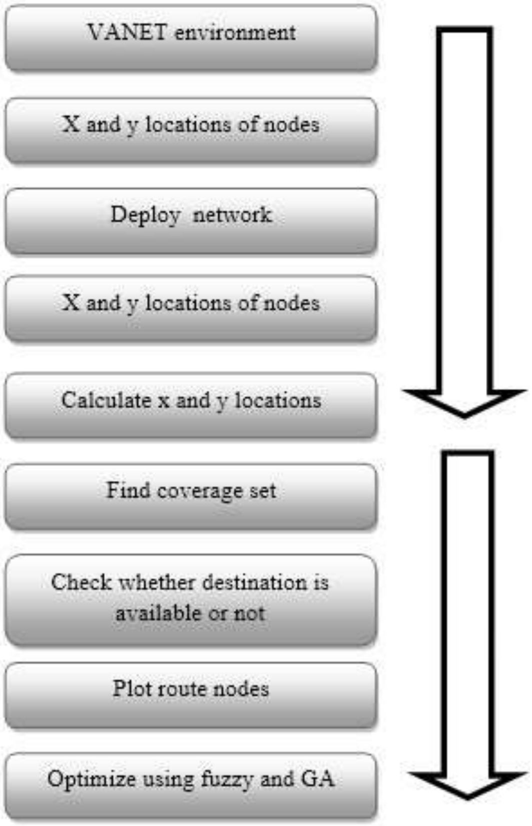
VANET environment
X and y locations of nodes
Deploy network
X and y locations of nodes
Calculate x and y locations
Find coverage set
Check whether destination is available or not
Plot route nodes
Optimize using fuzzy and GA

Figure 5: Simulation Model

The simulations were carried out by using MATLAB as the language that used to develop the proposed framework. In the simulation the following steps are to be followed by user:

1. Firstly ENTER the number of nodes

2 Then a network will appear of 1000 height and 1000 width.

5. Then the black attack which produces the number of multiple copies in the network which increases the load in the network will appear in the network.

6. The original nodes in the network having ids N1, N2, N3.....like this and all other all the multiple copies which increases the load.

7. Plot graph for proposed parameters.

8. Call fuzzy and GA algorithm.

9. Evaluate parameters with optimization.

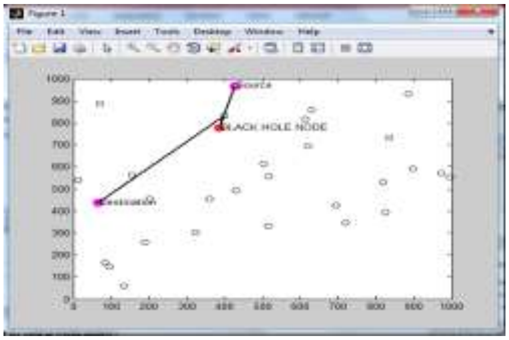

Figure 6: Searching for black node

Above figure, initially the network simulation model is formed which contains 30 nodes as given input and after that we enter Length vs breadth of the network is 1000*1000. Here, black line shows the path from source to destination. The channel (CH) captures the routing information from the initiator (source node) and then sends the data from the source to destination node.

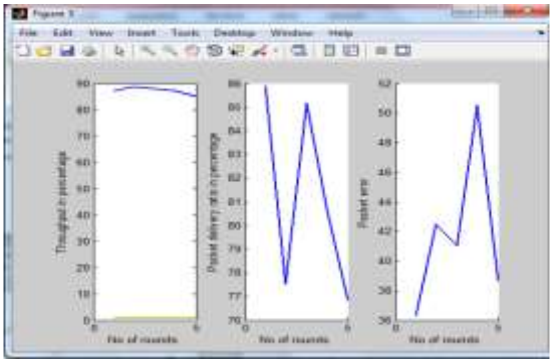

Figure 7: Throughput, PDR and error rate

In above figure, we have plotted graph between throughputs, PDR, error rate in percentage with respect to round of data transfer. It is shown that the throughput initially increases as round of data transfer increases and then decreases after adhoc attack is introduced as shown in above figure. Also error rate is normally decreases as round of data transfer increases but when attack happens then error rate start increasing as shown above due to the attack.

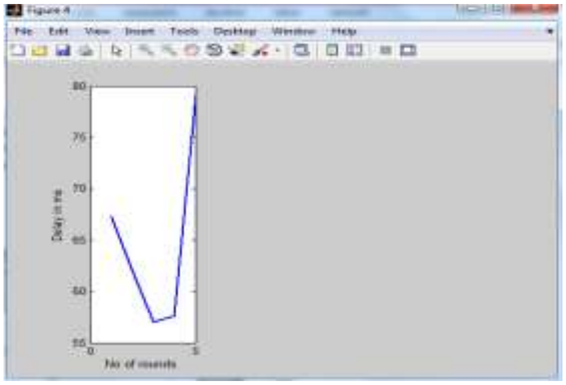

Figure 8: Delay in Network

The end delay increases when attack is introduced due to greater number of identities the number of attackers as shown above.

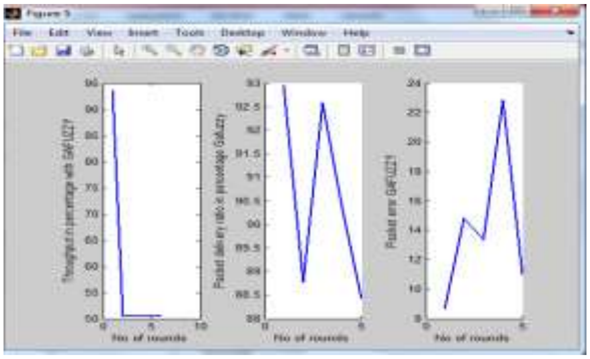

Figure 9: Throughput, PDR and error rate with optimization

The attacker nodes causes decrease in the throughput of the network. It is because number of collisions is more in system and it is optimized using fuzzy and GA algorithm as shown above. Above figure shows that throughput, BER, PDR value with fuzzy and G A. Total data from the source to the receiver more than the time it takes until the recipient receives the last packet. Less time translates into higher productivity.

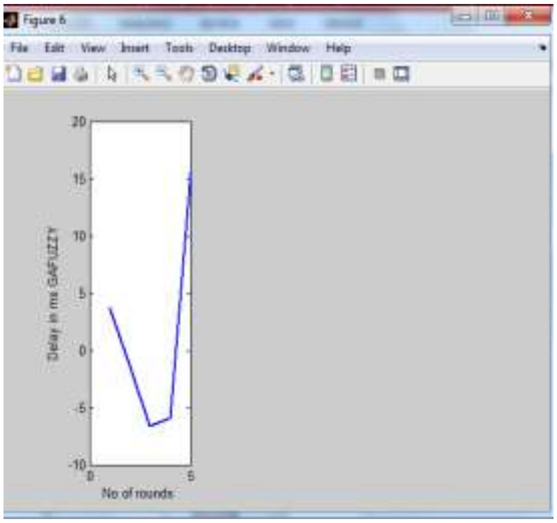

Figure 10: End delay with optimization method

The End to End Delay is a significant parameter for evaluating a protocol which must be low for good performance. Above figure shows the end to end delay with Fuzzy and GA. This increase in delay is due to the black nodes through which then passes to the destination node. However increase in the numbers of nodes also increases the difference of delay.

CONCLUSION

In this research, the effects of black hole attack in the performance of fuzzy and GA are analyzed. The simulation results show that when the black hole node exists in the network, it can be affected and decreased the performance of network and it can be optimized by using fuzzy and GA algorithm. A hypothetical network was constructed for the simulation purpose and then monitored for a number of parameters. The model for various nodes is simulated. Initial position for the node is specified in a movement scenario file created for the simulation using a MATLAB. The nodes move randomly among the simulation area. So, the detection and prevention of black hole attack in the network exists as a challenging task.

REFERENCES

[1] C. Hernandez-Goya et al., "Cooperation Requirements for Packet Forwarding in Vehicular Ad-Hoc Networks (VANETs)", ACM International Conference On Computer Systems and Technologies, 2009, pp. 1-6.

[2] Fan-Hsun Tseng, Li-Der Chou, and Han-Chieh Chao , "A Survey of black hole attacks in Wireless Mobile Ad Hoc Networks ", SPRINGER Human-centric Computing and Information Sciences, 2011, 22 Nov. 2011, pp. 1-16 .

[3] Vimal Bibhu et al., "Performance Analysis of black hole attack in VANET ", International Journal Of Computer Network and Information Security, Oct. 2012, pp. 47-54.

[4] Ajay Rawat, Santosh Sharma, and Rama Sushil, "VANET: Security Attacks and its possible solution", Journal of Information and Operations Management, vol. 3, Issue 1, 2012, pp. 301-304 .

[5] Arti Sharma, Satendra Jain, "A Behavioral 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.

[6] P. Manickam et al., "Performance Comparison of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Wireless & Mobile Networking (IJWMN), vol. 3, no. 1, Feb. 2011 , pp. 98-106.

[7] M.Geetha et al. , "Performance Comparison and Analysis of AODV and DSDV Gateway Discovery Protocol in MANET ", International Journal of Engineering Science and Technology , vol. 2(11), 2010, pp. 6521-6531

[8] Anuj K. Gupta, Dr. Harsh Sadawarti, and Dr. Anil K. Verma , "Performance analysis of AODV, DSR & TORA Routing Protocols", IACSIT International Journal of Engineering and Technology, vol. 2, no. 2, April 2010, pp. 226-231

[9] Yih-Chun Hu and David B.Johnson, "Caching Strategies in On-Demand Routing Protocols for Wireless Ad hoc Networks", ACM 2000, pp. 1-12.

[10] Karan Verma, Halabi Hasbullah, Ashok Kumar, "Prevention of DoS Attacks in VANET", in Wireless Personal Communications, November 2013, Volume 73, Issue 1, pp 95-126.

[11] Adil Mudasir Malla and Ravi Kant Sahu, "Security Attacks with an Effective Solution for DOS Attacks in VANET", in International Journal of Computer Applications, March 2013, Volume 66 - Number 22.

[12] M.Raya, P. Papadimitratos, and JP. Hubaux, "Securing Vehicular Communications", in IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, 2006, pp. 8- 15.

[13] 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.

[14] 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.

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

[16] 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.

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

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

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

[20] Uma Nagaraj, Dr. M. U. Kharat, Poonam Dhamal, "Study of Various Routing Protocols in VANET," IJCST International Journal of Computer Science & Technology, vol. 2, Dec. 2011, pp. 45-52.

[21] Dickerson, et al, "Fuzzy Network Profiling for Intrusion Detection, " 19th International Conference of the North American Fuzzy Information Processing Society, 2000, 301–306.

[22] Orchard, R. Fuzzy, " Reasoning in Jess : The FuzzyJ Toolkit and FuzzyJess," Third International Conference on Enterprise Information Systems, 533–542, 2001.

[23] Aly El-Samary et al, "Applying data mining of fuzzy association rules to network intrusion detection," Proceedings of IEEE workshop on Information Assurance, 2006.

[24] GEATbx: Genetic and Evolutionary AlgorithmToolbox for use with MATLAB, http://www.geatbx.com/links/ea_matlab.html

[25] D. E. Tim Lienmullar, Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", In proceedings of (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[26] Ahmad Yusri Dak, Saadiah Yahya, and Murizah Kassim, ―A Literature Survey on Security Challenges in VANETs‖. In the proceedings of International Journal of Computer Theory and Engineering, Vol. 4, No. 6, December 2012.

[27] Saira Gillani, Farrukh Shahzad, Amir Qayyum, and Rashid Mehmood, "A Survey on Security in Vehicular Ad Hoc Networks", Volume 7865 of the series Lecture Notes in Computer Science, 2013, pp 59-74.

[28] Sedjelmaci, H.; Senouci, S.M., "A new Intrusion Detection Framework for Vehicular Networks," in Communications (ICC), 2014 IEEE International Conference on , vol., no., pp.538-543, 10-14 June 2014.

[29] Hanin Almutairi, Samia Chelloug, Hanan Alqarni, Raghda Aljaber, Alyah Alshehri, and Dima Alotaish, "A New Black Hole Detection Scheme for VANETs", Proceedings of the 6th International Conference on Management of Emergent Digital EcoSystems, 2014 pp.-133-138, ACM.

[30] Manish Kumar Soni and Ashish Vashistha, "HAP: Hybrid Authentication Protocol for Vehicular Ad Hoc Network", National Seminar on Recent Advances in Wireless Networks and Communications, NWNC-2014.

[31] Bassem Mokhtar, and Mohamed Azab, "Survey on Security Issues in Vehicular Ad Hoc Networks" Alexandria Engineering Journal, Vol. 54, Issue 4, December 2015, Pp. 1115–1126.

[32] Rooshabh Kothari, Deepak Dembla "Implementation of Black Hole Security Attack Using Malicious Node for Enhanced-DSA Routing Protocol of MANET" International journal of computer applications (IJCA).VO.64-NO.18, 2013.

[33] Wahane, Gayatri, and Savita Lonare, "Technique for detection of cooperative black hole attack in MANET", 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT). IEEE, 2013.Zhu.

[34] Tan, Seryvuth, and Keecheon Kim, "Secure Route Discovery for preventing black hole attacks on AODV-based MANETs", ICT Convergence (ICTC), 2013 International Conference on. IEEE, 2013.

[35] Prachi et.al, "Hybrid Method for MANET Security against Jelly Fish, Black hole and DoS", International Journal of Computer Applications (0975 – 8887) Volume 139 – No.11, April 2016.

[36] Isaac Woungang et.al, "Detecting Black hole Attacks on DSR-based Mobile Ad Hoc Networks" 978-1-4673-1550-0/12/$31.00 ©2012 IEEE, 2012.

[37] Yang, Bo, Ryo Yamamoto, and Yoshiaki Tanaka, "Historical evidence based trust management strategy against black hole attacks in MANET", Advanced Communication Technology (ICACT), 2012 14th International Conference on. IEEE, 2012.

[38] K.S. Sujatha, V. Dharmar. R.S. Bhuvaneswaran, "Design of genetic algorithm based IDS for MANET", Conference: Recent Trends in Information Technology (ICRTIT), IEEE, pp.28-33, 2012.

[39] Anup Goyal and Chetan Kumar, "GA-NIDS: A Genetic Algorithm based Intrusion Detection System", 2010.

[40] Yuteng Guo, Beizeng Wang, Xingxing Zhao, Xiaobiao Xie, Lida lin and Qinda Zhou,"Feature Selection based on Rough Set and modified Genetic programming for Intrusion Detection", In 33 ICRTIT-2012 proceedings of 5th International Conference of Computer Science and Education, IEEE, August 2010.

[41] Wei Li, "Using Genetic Algorithm for Network Intrusion Detection", IEEE, pp.1-8, 2010.

[42] Al-Shurman, Mohammad, Seong-Moo Yoo, and Seungjin Park, "Black hole attack in mobile ad hoc networks", Proceedings of the 42nd annual southeast regional conference.ACM, 2004.

[43] Manvi Arya, "BFO Based Optimized Positioning For Black Hole Attack Mitigation in WSN", International Journal of Engineering Trends and Technology (IJETT) – Volume 14 Number 1 – Aug 2014.

[44] Kanika Bawa, " Prevention of Black Hole Attack in MANET using Addition of Genetic Algorithm to Bacterial Foraging Optimization", International Journal of Current Engineering and Technology 2015.