IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Detailed Review on Sybil Attack in Vehicular City Environment

Shilpa Goyal[1], Ms. Nisha Pandey[2]

M. Tech Student, Department of CSE, Shri Ram College of Engg & Mgmt, Palwal, Haryana, India[1]

Assistant Professor, Department of CSE, Shri Ram College of Engg & Mgmt, Palwal, Haryana, India[2]

Abstract: The vision of whole cities covered with dynamic networks of "talking cars" is gradually becoming a reality. The network thus formed is Vehicular Ad hoc Networks (VANETs). Vehicular Ad Hoc Networks (VANET) has become cynosure in the current decade. In the modern era the invention of smart vehicles have made VANET utmost important application to be implemented. But every boon has a curse hidden in it so is the case with the VANET. As VANET is an emerging research area so are its security issues. There are various attacks that can occur on VANET but the most vital is the Sybil Attack. In Sybil attack the attacking node creates multiple forge identities in order to gain a disproportionately large influence. This survey paper briefly presents various Sybil attack detection mechanism in VANET.

Keywords: VANET, MANET, Sybil Attack, Genetic Algorithm.

I. INTRODUCTION

In past few years, there is a fast improvement in the field of wireless and mobile communication. Mobile Communication Technologies have innovatively developed and developing "do it all" devices by leaps and bounds which has explosively triggered the growth of mobile data users: 1.5 billion users will use the new mobile data services by the end of 2017 according to the International Data Corporation [1]. This will led to a significant increase in wireless mobile traffic and demand for network resources in near future.

An important emerging wireless or mobile networking is an infrastructure-less "ad hoc" networking between mobile devices. Such networks are self configuring networks consisting of a set of mobile nodes that are connected by shared wireless channel forming an arbitrary topology without using any existing infrastructure or Central Management System [1]. In an Mobile Ad hoc network, each mobile node acts a host or router and forward the packets to other network in the node. These nodes are distributed randomly in the network and continuously participate or leave the network while moving. Vehicular Ad Hoc Network (VANET) is a special class of MANET in which entities that forms the network are vehicles and gives the concept of ubiquitous computing for future [2]. With VANET, vehicles can be turned into a network that will provide services similar like the ones used in offices and homes**.**

Every envisioned application of VANET requires that the nodes continuously broadcast vital information such as speed, location which will increase the awareness of vehicles about their whereabouts and warn drivers of dangerous situations [3]. Traffic Management Applications require data dissemination in a multi-hop network to alert vehicles regarding traffic situation while Commercial Application require unicast routing. VANET has unique features like high mobility, dynamic topology limited transporting distance, distributed nature of operation which makes routing protocols developed for MANET show degraded performance in VANET scenarios[4].

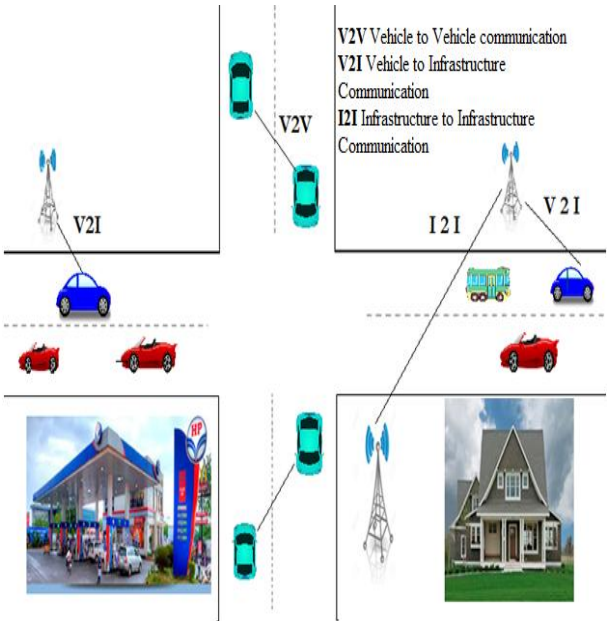

Figure1. Vehicular Ad hoc Network

A routing protocol decides the way of exchanging information between two communication entities. It utilizes the routing information to choose the next link whose maintenance is easy to realize according to performance criteria[5]. It establishes route, forward decision and maintain or recover from route failure. It's main aim is to provide an optimal path via minimum overhead[6].The performance of routing protocols depends on the characteristics of underlying network or

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

environment. For example, at high node density, an on-demand protocol that diffuses requests on entire network at each route discovery may cause an important control traffic that prevents sending data packets. With table-driven protocol, the topology information kept at each node may become obsolete incase of high node mobility [7]. For a highly dynamic topology environment, Pro-active routing protocols need to update routing information more frequent. While Reactive routing protocols maintain routing information only when there is a data packet to send. So, Reactive protocols are best to adapt into VANET environment [8].

II. VANET ARCHITECTURE

VANET architecture uses two kinds of communication devices: (1) On-board Units (OBUs) and (2) Road-side Units (RSUs). As name represents, OBU is equipped in a vehicle and RSUs are positioned on roadside. Every OBU contains a Global Positioning System (GPS) receiver, Event Data Recorder (EDR), a radar and computing platform. GPS recipient gives information about speed, geographic location, acceleration of a node and direction of movement at mentioned time intervals. EDR device stores the received and transmitted messages [3, 5]. Information saved in EDR can help in recreation of an emergency/accident condition for later analysis after the happening of an event. The computing device is utilized to take suitable actions in reply to messages obtained from other nodes. Radar is employed for determining obstacles close to the vehicle. Every vehicle also has an omni-directional antenna that the OBU utilizes to use a wireless channel. An RSU is same as an OBU in that it has a computing device, antenna, sensors and transceiver. It is a static device positioned on roadside. An RSU may be equipped at road intersections or implanted in traffic-light for traffic control. It can be positioned for commercial usage also. For instance, a restaurant can utilize an RSU for advertisement of its existence. An RSU may utilize either omni-directional or directional antenna based on the kind of application.

Fig 2. Illustrates a general VANET architecture. VANET is not a pure ad-hoc network as an infrastructure in the form of RSUs may available in several parts of the network. Sometimes, there may not be any infrastructure on highway. VANETs provide support to two kinds of communications: (1) Vehicle-to-Vehicle and (2) Vehicle-to-RSU. A V2R communication enables vehicular safety applications, involving collision warning as well as other ITS applications i.e. high speed tolling and local traffic information for routing.

All the nodes are aware of their own motion and position details. They exchange this information with neighbouring nodes at periodic intervals. Every vehicle saves information about itself and neighbour vehicles in a local database. This database records are forwarded to neighbouring nodes and roadside resources periodically. These forwarded messages help in managing the information.

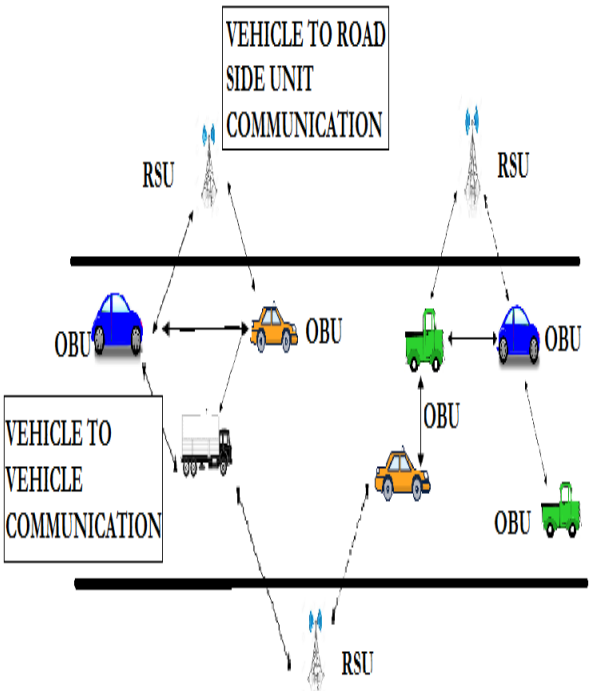

Figure 2: VANET ARCHITECTURE

Consider a vehicular adhoc network with five nodes.The circle represents the communication range of vehicle. Nodes that can communicate directly are neighboring nodes. A node keeps track of its neighboring nodes by listening for HELLO messages at particular intervals[13]. Suppose Node1 wants to send messsage to Node3, shown in Fig 3.

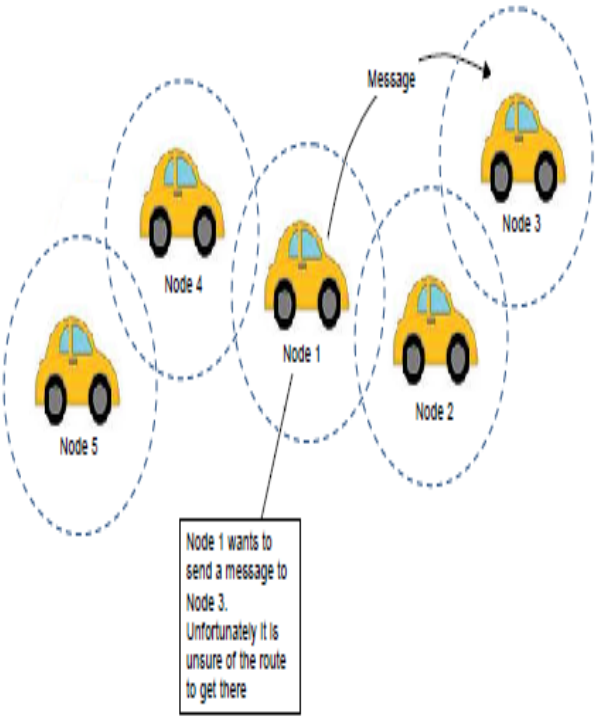

Fig 3: Node1 broadcasts RREQ

Since Node1 can not communicate directly with Node 3, so it broadcasts RREQ into the network as shown in Fig 4.

DOI 10.17148/IJARCCE.2016.54121

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

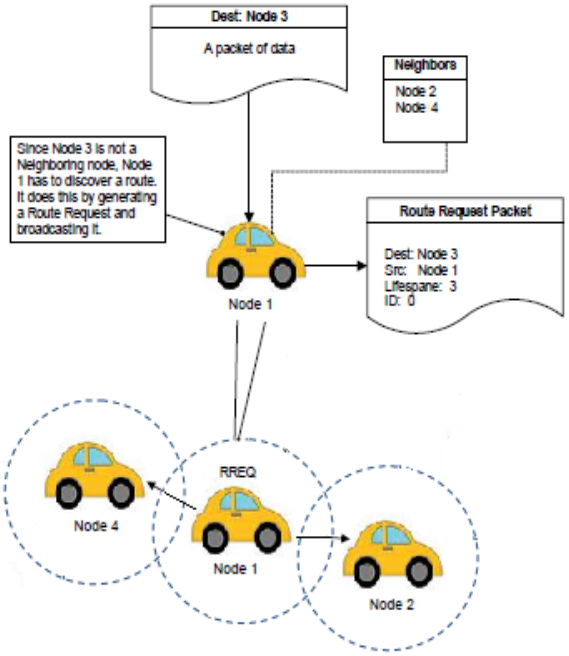

Fig 4. Node2 sends RREP and Node4 send RREQ to Node3

Node2 and Node4 listens to RREQ. Node2 has route to Node3 ,so it sends reply to Node1 by sending RREP[14]. On the other hand, Node4 does not have a route to Node3 so it rebroadcast the RREQ, shown in Figure 5.

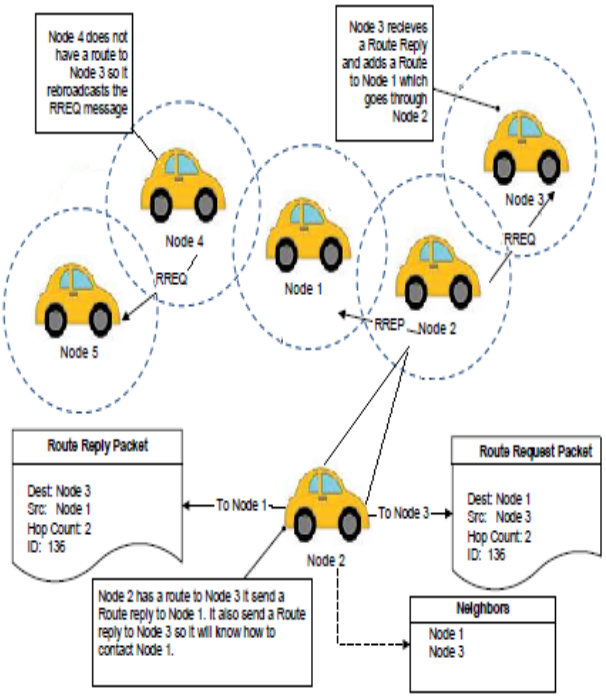

Fig 5: Node1 forwarding RREP to Node4

Node3 receives RREQ from Node2 and adds a route to Node1 via Node2. Node1 compares the sequence number in RREQ and RREP. It notices the route in RREP has better route so it replaces the route it currently has in its routing table with the route in Route Reply, shown in Fig 6 [15][16].

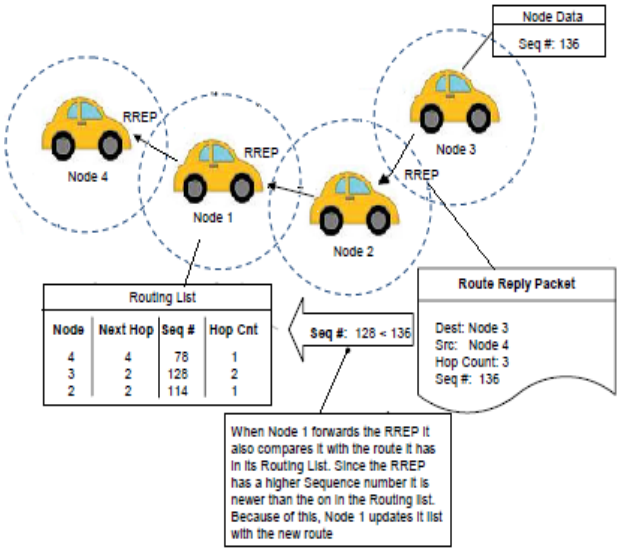

Fig 6: Node1 forwarding RREP to Node4

III. SYBIL ATTACK

As VANET is an emerging research area and so are its security issues. There are many security issues in VANET but here in this section we will be dealing with one of its major security issue i.e the Sybil Attack. Sybil attack is a malicious attack in which the attacker creates multiple identities and uses them to gain a disproportionately large influence. SYBIL attack is very grievous as the attacker can play any kind of attack with the system scaling down the efficiency of VANET to a larger extent and thus making it less feasible for practical approach. These forge identities also creates a semblance that there are additional vehicles on the road.

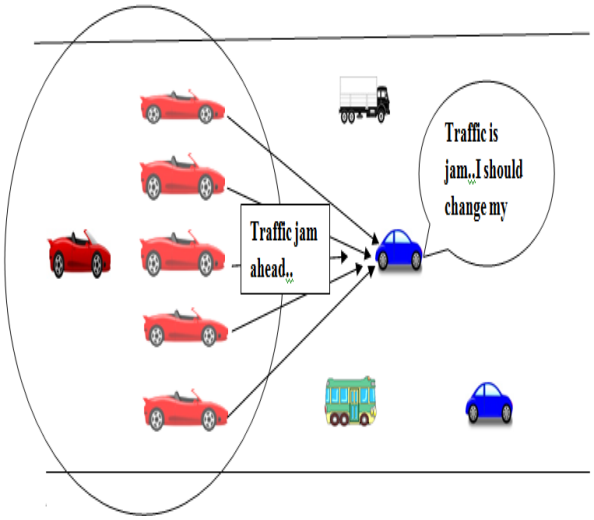

Figure 7: SYBIL ATTACK

Thus the need of ensuring that any confidential information is neither modified nor misused by an attacker. For the prevention various strategies have been developed to prevent intruders from attacking the system. Some of it includes resource testing, public key cryptography, Passive Detection through Single Observer,

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Passive Detection through Multiple Observer, Propagation model, Active Detection by Position Verification, Sensor-Based Position Verification. Now we will discuss all of these one by one.

Resource Testing: - proposed by Douceur, this technique can be utilized to detect Sybil attack. It is based on the assumption that every single node has confined computational resources. But this technique has few limitations too. The first one is any malicious node may have more resources as compared to authenticated nodes. Secondly, this can bring out network congestion as there is a large number of replies/requests messages on the network.

Public Key Cryptography:- another mechanism of resolving Sybil attack is by the use of public key authentication. In this technique the digital certificates provided by TTP are combined with signatures utilizing the asymmetric cryptography. There is a CA for each region which issues certificates. The CA follows a hierarchy.

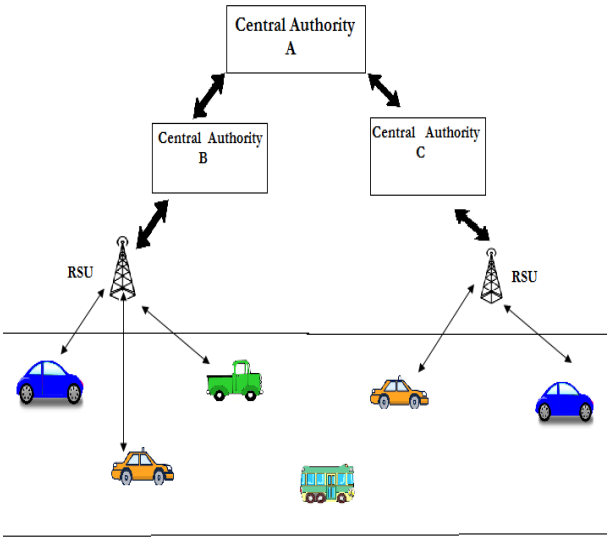

Figure 8: HIERARCHY OF CA

The nodes communicate with each other by sending signed messages. The authenticated messages are kept and rest are ignored thus preventing Sybil attacker from intruding into the system. The problem with this approach is that it is very complex, time consuming and requires large memory.

Sensor-Based Position Verification:- malicious nature of the nodes is detected by using multiple sensors rather than using stationary infrastructure. The verification of the location information given by GPS system and detection of forge position information is done by using sensor data. The authentication of a node is done by calculating a trust value.

Active Detection By Positioning Verification:- this technique is based on the position based cells. It uses the front and back radar for detection of obstacles in its path. Each cell broadcast a beacon message. After receiving the message the GPS position and position calculated by radar are matched if both the positions match than the message is accepted else ignored.

IV. RELATED WORK

There are various techniques being developed to prevent and detect Sybil attack so far.

Harsimrat Kaur et al. [1]; Here another approach uses genetic algorithm for the efficient detection and prevention of Sybil attack in vehicular city environment. This approach is based on the fitness function optimization. Initially a network is deployed than Sybil attack is shown on it. Finally the values for the parameters such as network load, throughput, packet delivery ratio and end delay is checked. Than genetic algorithm is applied on the network and values are rechecked. Finally comparison between both the values is done and Sybil attack is detected. The results of this approach can be further improved by using hybridization of genetic algorithm.

Priyanka Soni et. al. [2]; Here authors showing a new approach to avoid Sybil attack and that is GPRS algorithm. The methodology includes deployment of a scenario in which required number of nodes will be initialized and then GPSR (Geographic routing protocol) will be deployed. If some node is intersecting the range of another node then its verification will be done on the bases of coordinates, in this way attacker nodes can be identified and authentication will be done by the RSU (Road Side Unit) by checking the identities of nodes and comparing them with its node table, if two or more than two identities exist then malicious node is identified. The problem with this technique is that it requires large memory storage and is also a time consuming process.

Soyoung Park et. al. [3]; In this paper authors using a time stamp series approach to detect Sybil attack. Initially a network is created with some vehicles having communicating capability and road side infrastructure. It is rare that two vehicles pass different RSU at the same time. This correlation between the vehicles is used for the authentication of messages. The main challenge in this scheme is that it becomes very complex in the urban city environment.

V. GENETIC ALGORITHM

Genetic algorithms (GAs) are search mechanisms depending on natural selection and genetics principles. We begin with a summarized introduction to simple genetic algorithms and related terms. GAs encodes the variables of decision of a search problem into finite-length strings of alphabets of particular cardinality. The strings that are candidate solutions to the search problem are called chromosomes, the alphabets are called genes and the genes values are referred as alleles. For instance, in a problem i.e. the travelling salesman problem, a chromosome indicates a route, and a gene may indicate a city. In opposite to conventional optimization mechanisms, GAs work with parameters coding, instead of parameters themselves. To develop good solutions and to carry out natural selection, we require a evaluation for differentiating good solutions from bad solutions. The evaluation could be an objective function that is a computer simulation or a computational model, or it can

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

be a subjective function where humans select better solutions over bad ones. In essence, the fitness evaluation must find a candidate solution's relative fitness, which will later be utilized by the GA to guide the development of good solutions. Another significant concept of GAs is the population notion. Unlike conventional search techniques, genetic algorithms depend on a population of candidate solutions. The population size, which is normally a user-mentioned parameter, is one of the significant element influencing the scalability and genetic algorithms performance. For e.g., small population sizes might cause to premature GOLDBERG, 98 SASTRY AND KENDALL convergence and results substandard solutions. On the other side, large population sizes cause to unessential expenditure of important calculation time. Once the problem is encoded in a chromosomal way and a fitness evaluation for distinguishing good solutions from bad ones has been selected, we can begin to develop solutions to the search problem utilizing the adopting.

Step: 1 Initialization. The starting population of candidate solutions is normally produced randomly throughout the search space. Since, domain-specific knowledge or other information can be easily integrated.
Step 2 Evaluations. Once the population is started or an offspring population is generated, the fitness values of the candidate solutions are measured.
Step 3 Selections. Selection assigns more copies of those solutions with greater fitness values and hence enforces the survival-of-the-fittest technique on the candidate solutions. The significant concept of selection is to choose better solutions to bad ones, and several selection mechanisms have been introduced to achieve this idea, involving stochastic universal selection, roulette-wheel selection, and tournament selection and ranking selection, many of which are explained in the next section.
Step 4 Recombination: It integrates parts of two or more parental solutions to generate novel, possibly better solutions (such as offspring). There are several ways of achieving this (some of which are talked about in the next section), and competent performance rely on a suitably designed recombination technique. The offspring under recombination will not be similar to any specific parent and will instead integrate parental traits in a new way.
Step 5 Mutation: While recombination works on two or more parental chromosomes, mutation temporarily but changes a solution in a random way. Again, there are several mutation variations, but it normally includes one or more changes being built to an individual's trait. In other words, mutation represents a random walk in the candidate solution vicinity.
Step 6 Replacement: The offspring population generated by selection, recombination, and mutation substitutes the real parental population. Some replacement mechanisms i.e. Generation-wise replacement, elitist replacement and steady-state replacement mechanisms are utilized in GAs.
Step 7 Repeat steps 2–6 until a ceasing condition is achieved. Goldberg has compared GAs to mechanistic versions of specific modes of human innovation and has indicated that these operators when examined individually are inefficient, but when integrated together they can Genetic Algorithms work well. This view has been described with the fundamental intuition and innovation intuition concepts. The similar study compares a integration of selection and mutation to continual enhancement (a form of hill climbing), and the integration of recombination and selection to innovation (cross-fertilizing). These analogies have been utilized to evolve a design-decomposition mechanism and known as competent GAs—that solve complicated problems reliably, frequently and accurately—both of which are described in the later sections. This chapter is scheduled as follows. The next section offers explanation of individual steps of a typical genetic algorithm and proposes various famous genetic operators.

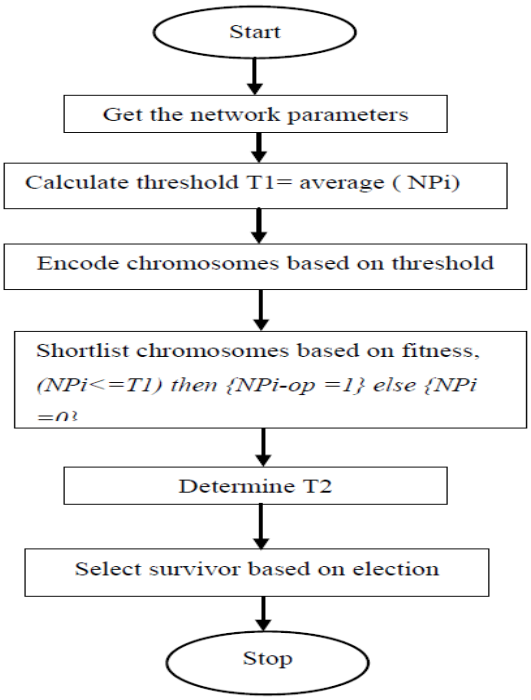

Fig. 9 Flowchart of GA

This is the mechanism for determination of Sybil attack Adopted by the framework flow chart:

Step 1: Start
Step 2: obtain the parameters of network from the provided VANET system. Every chromosome is then measured for a fitness function by taking several network parameters.
Step 3 : Compute threshold T1= average (NPi). Then the threshold is found by computing the average of the individual parameters of network. Then the fitness value for every network parameter is determined
Where, T1 = First Threshold
NPi = Network Parameter i.e. throughput, network delay, for I = 1, 2, 3….N. N= Total no of nodes in the network.
Step 4 : Encode chromosomes depending on threshold measured.
Step 5 : Then arrange chromosomes depending on fitness, (NPi<=T1) then {NPiop =1} else {NPi =0}.
Step 6: Now, determine T2 as the weighted average of the network parameters. Then the supporting Sybil nodes are

the ones with the value of all the optimum parameters to be zero. Hence these nodes are determined and drawn versus their node identification no.

Step 7: Stop.

Below flowchart is the introduced mechanism to prevent Sybil attack in the network. The very first step is the collection of network parameters i.e. , no. of rounds, no. of nodes, network width and network length. After that network deployment occurs that represent the data packets transmission from source node to destination node. After that detection of Sybil nodes occurs in the network. After this evaluation of Sybil attack parameters occur. Then employ genetic algorithm to analyse these parameters so that Sybil attack prevention occurs. In the end again parameter measurement has been performed while optimizing with genetic algorithm. Optimization has been performed utilizing combination of fitness function and thresholding.

VI. CONCLUSION

In this paper, we have talked about defence techniques against Sybil attack in VANETs. With respect to the studies in this field, every technique has some benefits and drawbacks for implementing. Resource testing mechanisms are not enough to implement for Sybil attack detection with high accuracy in VANETs. Authorization techniques are more useful and reliable for message authenticity, integrity and privacy and there are proper mechanisms in this category for practical implementation in urban fields. In opposite, position verification techniques are easy and lightweight for implementation and if they possess high accuracy for position verification, we can employ them for other security objectives such as position verification after obtaining location information that periodically forward by vehicles for position regarded applications. So choice between two latest techniques is based on schemes, needs and assigned cost in every country.

REFERENCES

[1] Priyanka Soni and Abhilash Sharma, "Sybil Node Detection and Prevention Approach on Physical Location in VANET" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 7, July 2015, pp.1161-1164

[2] Harsimrat Kaur & Preeti Bansal," Efficient Detection & Prevention of Sybil Attack in VANET" International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 9, September 2015.

[3] Soyoung Park, Baber Aslam, Damla Turgut and Cliff C. Zou,' Defense Against Sybil Attack In Vehicular Ad Hoc Network Based On Roadside Unit Support , Springer Science, Business Media.2010

[4] Samara, Wafaa A.H. Al-Salihy, R.sures, "Ghassan Security Analysis of Vehicular Ad hoc Networks"2010 International Conference on Network Applications,Protocols and Services.

[5] Verma, K.; Hasbullah, H.; Kumar, A., "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," Advance Computing Conference (IACC), 2013 IEEE 3rd International , vol., no., pp.550,555, 22-23 Feb. 2013

[6] Grzybek, A.; Seredynski, M.; Danoy, G.; Bouvry, P., "Aspects and trends in realistic VANET simulations, Wireless, Mobile and Multimedia Network, 2012 IEEE International Symposium on a , vol., no., pp.1,6, 25-28 June 2012

[7] Jie Li, Huang Lu, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs", IEEE Transactions on Parallel and Distributed Systems, 2012

[8] Chim, T.W.; Yiu, S.M.; Hui, L.C.K.; Li, V.O.K., "VSPN: VANET-Based Secure and Privacy-Preserving Navigation," Computers, IEEE Transactions on , vol.63, no.2, pp.510,524, Feb. 2014

[9] Yen-Wen Lin; Guo-Tang Huang, "Optimal next hop selection for VANET routing," Communications and Networking in China (CHINACOM), 2012 7th International ICST Conference on , vol., no., pp.611,615, 8-10 Aug. 2012

[10] Performance Comparison Of AODV and DSDV Routing Protocols in Mobile Ad Hoc Networks, Aditi Sharma,Sonal Rana, Leena Kalia, International Journal of Emerging Research in Management and Technology, ISSN:2278-9359 Volume-3, Issue-7, July 2014.

[11] Ait Ali, K.; Baala, O.; Caminada, A., "Routing Mechanisms Analysis in Vehicular City Environment," Vehicular Technology Conference, 2011 IEEE 73rd , vol., no., pp.1,5, 15-18 May 2011

[12] Bhoi, S.K.; Khilar, P.M., "A secure routing protocol for Vehicular Ad Hoc Network to provide ITS services," Communications and Signal Processing (ICCSP), 2013 International Conference on , vol., no., pp.1170,1174, 3-5 April 2013

[13] Pathre, A.; Agrawal, C.; Jain, A., "A novel defense scheme against DDOS attack in VANET," Wireless and Optical Communications Networks (WOCN), 2013 Tenth International Conference on , vol., no., pp.1,5, 26-28 July 2013

[14] Hamieh, A.; Ben-othman, J.; Mokdad, L., "Detection of Radio Interference Attacks in VANET," Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE , vol., no., pp.1,5, Nov. 30 2009-Dec. 4 2009

[14] Lyamin, N.; Vinel, A.; Jonsson, M.; Loo, J., "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks," Communications Letters, IEEE , vol.18, no.1, pp.110,113, January 2014

[15] Yeongkwun Kim; Injoo Kim; Shim, C.Y., "A taxonomy for DOS attacks in VANET," Communications and Information Technologies (ISCIT), 2014 14th International Symposium on , vol., no., pp.26,27, 24-26 Sept. 2014

[16] Verma, K.; Hasbullah, H.; Kumar, A., "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," Advance Computing Conference (IACC), 2013 IEEE 3rd International , vol., no., pp.550,555, 22-23 Feb. 2013

[17] Li He; Wen Tao Zhu, "Mitigating DoS attacks against signature-based authentication in VANETs," Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on , vol.3, no., pp.261,265, 25-27 May 2012

[18] Pooja, B.; Manohara Pai, M.M.; Pai, R.M.; Ajam, N.; Mouzna, J., "Mitigation of insider and outsider DoS attack against signature based authentication in VANETs," Computer Aided System Engineering (APCASE), 2014 Asia-Pacific Conference on , vol., no., pp.152,157, 10-12 Feb. 2014

[19] Durech, J.; Franekova, M.; Holecko, P.; Bubenikova, E., "Security analysis of cryptographic constructions used within communications in modern transportation systems on the base of modelling," ELEKTRO, 2014 , vol., no., pp.424,429, 19-20 May 2014

[20] Nafi, N.S.; Khan, R.H.; Khan, J.Y.; Gregory, M., "A predictive road traffic management system based on vehicular ad-hoc network," Telecommunication Networks and Applications Conference (ATNAC), 2014 Australasian , vol., no., pp.135,140, 26-28 Nov. 2014

[21] Kumar, A.; Sinha, M., "Overview on vehicular ad hoc network and its security issues," Computing for Sustainable Global Development (INDIACom), 2014 International Conference on , vol., no., pp.792,797, 5-7 March 2014

[22] Mehta, K.; Malik, L.G.; Bajaj, P., "VANET: Challenges, Issues and Solutions," Emerging Trends in Engineering and Technology (ICETET), 2013 6th International Conference on , vol., no., pp.78,79, 16-18 Dec. 2013

[23] Nafi, N.S.; Khan, J.Y., "A VANET based Intelligent Road Traffic Signalling System," Telecommunication Networks and

Applications Conference (ATNAC), 2012 Australasian , vol., no., pp.1,6, 7-9 Nov. 2012

[24] Shuai Yang; Rongxi He; Ying Wang; Sen Li; Bin Lin, "OPNET-based modeling and simulations on routing protocols in VANETs with IEEE 802.11p," Systems and Informatics (ICSAI), 2014 2nd International Conference on , vol., no., pp.536,541, 15-17 Nov. 2014

[25] Sadeghi, M.; Yahya, S., "Analysis of Wormhole attack on MANETs using different MANET routing protocols," Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on , vol., no., pp.301,305, 4-6 July 2012

[26] Jhaveri, Rutvij H.; Patel, Ashish D.; Dangarwala, Kruti J., "Comprehensive Study of various DoS attacks and defense approaches in MANETs," Emerging Trends in Science, Engineering and Technology (INCOSET), 2012 International Conference on , vol., no., pp.25,31, 13-14 Dec. 2012

[26] C. Sommer, Z. Yao, R. German, and F. Dressler, "On the need for bidirectional coupling of road traffic micro simulation and network simulation," in Mobility Models '08: Proceeding of the 1st ACM SIGMOBILE workshop on Mobility models. New York, NY, USA: ACM, 2008, pp. 41–48

[27] Zhao and G. Cao, "Vadd: Vehicle-assisted data delivery in vehicular ad hoc networks," Vehicular Technology, IEEE Transactions on, vol. 57, no. 3, pp. 1910 –1922, may 2008.

[28] Q. Chen, D. Jiang, and L. Delgrossi, "Ieee 1609.4 dsrc multi-channel operations and its implications on vehicle safety communications," in Vehicular Networking Conference (VNC), 2009 IEEE, oct. 2009, pp. 1 –8.

[29] Y. H. Choi, R. Rajkumar, P. Mudalige, and F. Bai, "Adaptive location division multiple access for reliable safety message dissemination in vanets," in Wireless Communication Systems, 2009. ISWCS 2009. 6th International Symposium on, sept. 2009, pp. 565 –569.

[30] Biswas, S., & Misic, J to Privacy-preser. (2013). "A Cross-layer Approach ving Authentication in WAVE-enabled VANETs." Vehicular Technology, IEEE Transactions on 62(5): 2182 – 2192

[31] Pradweap, R. V., & Hansdah, R. C. (2013). A Novel RSU-Aided Hybrid Architecture for Anonymous Authentication (RAHAA) in VANET. In Information Systems Security (pp. 314-328). Springer Berlin Heidelberg.

[32] Prado, A., Ruj, S., & Nayak, A. (2013, June). "Enhanced privacy and reliability for secure geocasting in VANET." In Communications (ICC), 2013 IEEE International Conference on (pp. 1599-1603). IEEE.

[33] Gupta, D.; Kumar, R., "An improved genetic based Routing Protocol for VANETs," Confluence The Next Generation Information Technology Summit, 2014 5th International Conference -, vol., no., pp.347, 353, 25-26 Sept. 2014

DOI 10.17148/IJARCCE.2016.54121