ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 4, April 2016

Review on Sybil Attack in Vehicular Ad Hoc Network

Preeti Rawat[1], Shikha Sharma[2],

M-Tech Student, Department of CSE, Advance Institute of Technology and Mgt, Palwal, Haryana, India[1]
Assit. Prof., Department of CSE, Advance Institute of Technology and Mgt. Palwal, Haryana, India [2]

ABSTRACT

The VANET security has become a important and active area within the research community. Despite the various attacks aimed at particular nodes in VANET that have been revealed, many attacks including multiple nodes still achieve little care. Furthermore, it might also have to do with the conception in which no taxonomy or survey has been performed to clarify the features of several multiple node attacks. This paper presents the aforesaid gap by offering a suitable definition and classification of Sybil attacks in VANET. In the suggested work GA has been employed with fitness function optimization. Genetic Algorithm can be utilized to invent elementary principles for networks traffic. At first, we establish a network according to our requirement, then show Sybil attack on the network and examine some particular parameters value on these attacks on the network which are provided as throughput, network load, end delay and packet delivery ratio. Then, we present genetic algorithm for optimization of fraud nodes then again examine the value depending on some particular parameters.

Keywords*:* VANET, Genetic Optimization Algorithm, Security.

I. INTRODUCTION

VANETs are one kind of mechanism to apply Intelligent Transportation System, which is a system designed for conveying communication technology as well as data in the direction of carrying vehicles as well as infrastructure[4,5]. The aforesaid is performed on IEEE 802.11p standard meant for Wireless Access intended for Vehicular Environment (WAVE). These networks have no fixed infrastructure; in summation to they are based on themselves for performing any type of network functionality
[6]. Security of vehicular networks is however principally a disclosed part. VANET, availability as a wireless network, take over altogether type of the security dangers which is a Wireless framework has to deal with. VANET security is Dangerous because a poorly considered Vehicular Ad hoc Network is susceptible to network attacks, also this know how to compromise the drivers of security [7,8]. A security framework must ensure which of the broadcast produces beginning a reliable source as well as it is not a tampered route by any other sources. It must also incursion a balance with confidentiality as for performing privacy as well as security consisted in a framework is inconsistent [9].

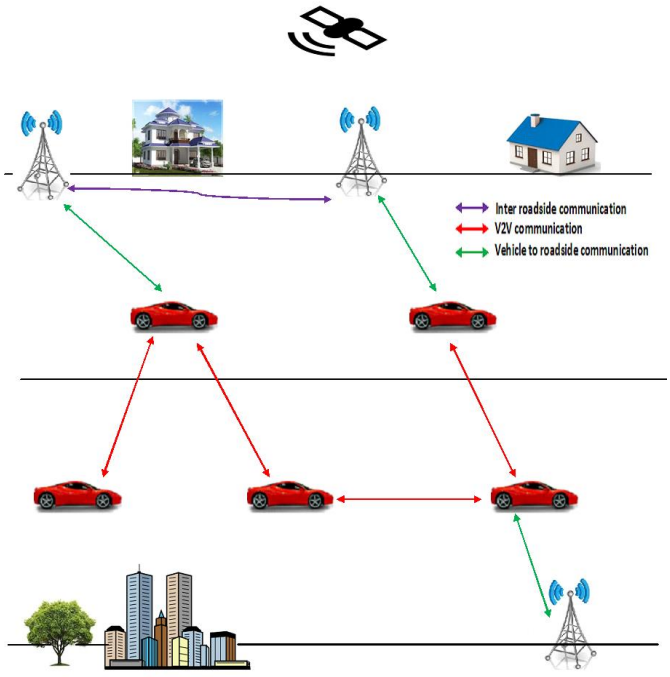

Figure 1: Vehicular Ad hoc Network

There are various kinds of possible attacks on Vehicular Ad hoc Networks [10, 11]. This one is critical in which Vehicular Ad hoc Network security should be skilled of maintaining each of the single kind of attack [12,13]. By Sybil attack is one of the serious attacks that has been discovered these days. Sybil attack is a type of security risk when a hub in a system confirms several features [16]. Most systems, same as a shared system, depend on considerations of personality, where each PC speaks to one character [14]. A Sybil attack occurs when an Unreliable PC is caught to claim various characters. Challenges reveal when a reputation system, (for instance, a record sharing reputation on a system) is betrayed into believing that an attacking PC has a disproportionally wide effect [15]. Correspondingly, an attacker with different personalities can use them to behave maliciously, by either taking data or interfering correspondence. Sybil attacks have showed up in various

conditions, with wide uses for well being, security and trust. For example, a web survey can be static using many IP locations to represent countless. Some organizations have likewise used Sybil attack to enhance better appreciations.
In this paper, Sybil attack prevention has been suggested utilizing genetic algorithm. The remaining paper is presented as Section 2 provides the detailed description of Sybil attack prevention in VANET. Section 3 consist the results and formulation in MATLAB and at last Section 4 consist conclusion and future scope.

II. RELATED WORK

[1] In this paper the author detects Sybil attack through cryptographic system. In this method a fixed key infrastructure is used for identifying Sybil attack. For reviewing the results of this study a Mat lab simulator is used. There is very less delay in detecting Sybil attack in this method, as almost all operations are implemented in Certification Authority, so the proposed method is an efficient method for identifying Sybil attack. The only problem in this proposed method is that, when nodes prompt to other region the method does not work properly. **[2]** Fake messages and forge nodes are identified by observing their actions afterward of their sending out the messages by using the concept of data-centric Misbehavior Detection Schemes (MDS). In the data-centric MDS, Whether the received information is correct or not is decided by each node and it is made on the basis of consistency of recent received messages. There is no need of Voting or majority decisions, which makes MDS more reliable to detect Sybil attack. Once the attack is identified, Irrespective of revealing all the hidden ID of suspicious nodes, fine is imposed on those nodes and thus de-motivating them to act selfishly. Thus the computation and communication costs that were indulged in revealing all the hidden ID of suspicious nodes are reduced by this approach and the same is shown in the results**. [3]** In this a new timestamp series approach is suggested which is based on road side infrastructure. No special infrastructure or public key infrastructure is required in this approach. The case that two vehicles passes multiple RSUs simultaneously is uncommon, thus considering this assumption and impermanent relation between vehicles and RSU, two messages having identical timestamp series by same RSU will be taken as a Sybil attack by that vehicle.

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. 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, 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.

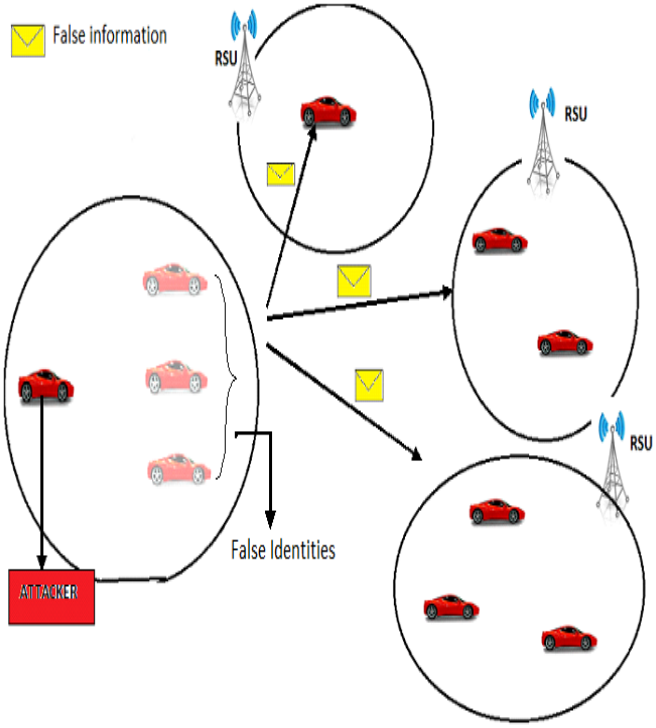

Fig. 2 Sybil Attack

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. 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

IV. DETECTION OF SYBIL ATTACK USING GENETIC ALGORITHM

This is the mechanism for detection of Sybil attack explained by the framework flow chart:

Step 1: Start
Step 2: obtain the network parameters from the provided VANET system. Every chromosome is then formulated for a fitness function by taking the different network parameters.
Step 3: Compute threshold T1= average (NPi). Then the threshold is evaluated by computing the mean of the individual network parameters. Then the fitness criterion for each and every network parameter is evaluated
Where, T1 = First Threshold
NPi = Network Parameter i.e. network throughput, delay for I = 1, 2, 3….N. N= Total no of nodes in the network.
Step 4 : Encode chromosomes depending on threshold formulated.
Step 5 : Then Shortlist chromosomes depending on fitness, *(NPi<=T1) then {NPiop =1} else {NPi =0}.*
Step 6 : Now, evaluate T2 as the weighted mean of the network parameters. Then the living Sybil nodes are the ones with the value of all the optimal parameters to be zero. Hence these nodes are found and plotted versus their node identification number.
Step 7 : Stop.
Below flowchart is the suggested mechanism to prevent network Sybil attack. The very first phase is the network parameters collection i.e. no. of rounds, no. of nodes, network width, and network length. After that network deployment happens that presents the data packets transmission from source to destination. After Sybil nodes detection takes place in the network. After this parameter formulation in Sybil attack takes place. Then employ genetic algorithm to examine these parameters so that Sybil attack prevention takes place. At last again parameter formulation has been done while examining with genetic algorithm. Optimization has been performed utilizing combination of fitness function and thresholding.

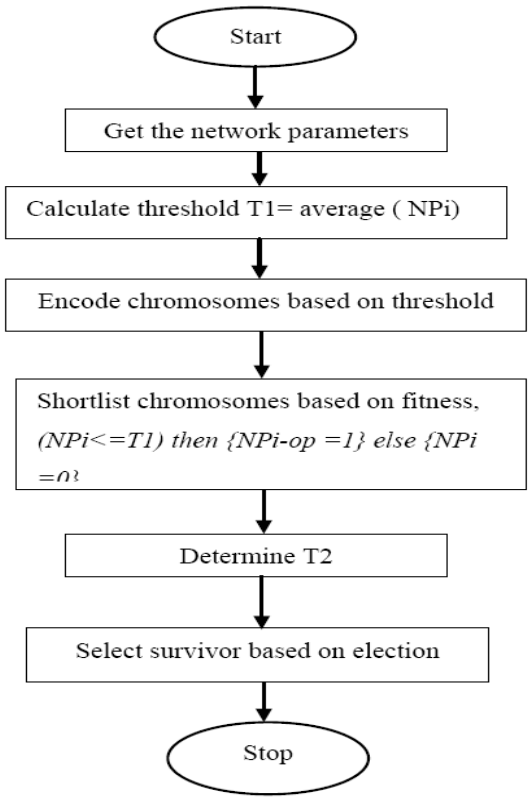

Fig. 3: Flowchart of GA

V. Conclusion

VANETs is quiet not secure as well as susceptible to various attacks so there is requirement of a proficient, dependable as well as a secured protocol which can be capable to rapidly organized and also use dynamic routing mechanism. Peer-to-peer systems play an ever-increasingly significant role of our daily life. Since, mostly peer-to-peer systems are susceptible to Sybil attacks. For designing more effective and practical Sybil defenses, we suggested an implementation depending on Genetic algorithm. In this paper, the challenges concerned to security i.e. Sybil attack has been studied. Then an Intrusion Detection System (IDS) particularly for Sybil attacks is implemented employing Genetic Algorithm, and then examined with networks of distributed node configurations.

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