Sybil Attack in Vehicular Ad Hoc Network (VANET): A Review

Harsimrat Kaur, Preeti Bansal
Chandigarh engineering collage, Mohali, Punjab, India

Abstract **-** Vehicular Ad Hoc Networks are receiving great interest and research efforts in modern time due to the various enhanced safety and travel comfort they are providing to the Vanet users. VANETs are being increasingly recommended for traffic control, avoidance of accidents, managements of parking lots and public areas. The two concerns in Vanet are Security and Privacy. Unfortunately services provided by Vehicular Ad Hoc Networks are vulnerable to Sybil Attacks, whereby a malicious user claim multiple identities at the same time. Exchange of safety information enables life critical applications, such as alert messaging during intersection transversing and emerging of lanes. Presence of such attacks can cause a great loss to life. This paper surveys the previous researches done in this area and the various drawbacks they are having.

Keywords - Vehicular Ad Hoc Network, Sybil attack, Security, Vehicular Communication, Routing.

I. INTRODUCTION

Wireless network is the network of mobile computer nodes or stations that are not physically wired [1]. The main advantage of this network is one can communicate with the world while moving at any place any time. The disadvantage is their limited bandwidth, memory, processing capabilities and open medium. Two basic system models are fixed backbone wireless system and Wireless Mobile Ad hoc Network (MANET) [1]. An ad hoc network is defined as the collection of nodes that do not depend on a predefined infrastructure to keep the network connected. With the rapid increase in the number of vehicles on the streets, vehicle manufacturers are looking for value-added services for providing their customers with increased safety and information. Towards this goal, Vehicular Communication (VC) is likely to play a major role. VC involves the use of short-range radios in each vehicle, which would allow various vehicles to communicate with each other and with road-side infrastructure [3]. These vehicles would then form an ad hoc networks in vehicles, popularly known as Vehicular Ad Hoc Networks (VANETs).

II. SYBIL ATTACK

Sybil attack, first discussed by Douseur [2], is a serious threat as it hinders the functionality of VANETs. In this attack, an attacker node sends messages with numerous identities to other nodes in the network. The attacker replicates several nodes in the network. The node that spoofed the identities of other nodes is called malicious node/Sybil attacker, and the nodes whose identities are spoofed are called Sybil nodes[5]. In the presence of Sybil attack many others attacks can be launched. One possibility could be an misconception of a traffic jam or accident so that other vehicles change their routing path or leave the road for the benefit of the attacker. Sybil attacker can also introduce false information in the networks via some fabricated non existing nodes. For example, in the case of an highway accident, the first vehicle observing the accident is sending change route/deceleration warning message to all the following vehicles. Receivers may forward this warning message to the followers, if any. This forwarding process can be disrupted by Sybil vehicles by not forwarding the warning message or by adding some false information. This may put the life of passengers in danger [3].

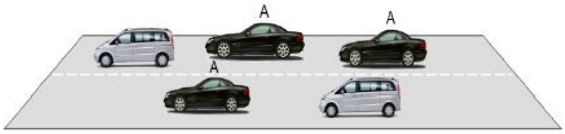

Fig.1: Sybil Attack

A. Different forms of Sybil Attack

i. ***Direct/Indirect Communication***

When an honest node sends a radio message to a Sybil node, one among the malicious nodes listens to the message. In the same way, messages sent from Sybil nodes are actually sent from one of the malicious devices. Communication to/from Sybil nodes can be direct or indirect. In a direct mode, all the Sybil nodes created by malicious node communicate with legitimate nodes. In an indirect communication, legitimate nodes reach the Sybil nodes through a malicious node [5].

ii. Fabricated Stolen Identities

In a Sybil attack, an attacker creates a new Sybil identity. This identity can be a random 32-bit integer (fabricated identity) or an attacker can spoof legitimate identity of one of its neighbours (stolen identity).

iii. Simultaneous /Non Simultaneous Participation

Multiple Sybil identities created by malicious nodes can simultaneously participate in the attack or the attacker can

present these Sybil identities one by one. A particular identity may leave or join the network many times, that is, one identity is used at a time. The number of identities the attacker uses is equal to or less than the number of physical identities [3].

III. PREVIOUS TECHNIQES USED

AUTHORS	TECHNIQUES AND ALGORITHM	ADVANTAGES	DISADVANTAGES	PARAMETRES
Mohamed salah bouassida, gilles guette, mohamed shawky, and bertrand ducourthial	Intrusion detection approach	The approach is having signal strength	Sybil attacker emitting high power	Degree illustration Having range of 120 m
Chen Chen, Xin Wang*, Weili Han, Binyu Zang	RobSAD algorithm	The approach is robust as compared to other techniques	High routing overhead because of heavy load due to Sybil nodes	Computation time is 151 sec
Jyoti Grover, Manoj Singh Gaur & Vijay Laxmi	Vehicular Ad Hoc Networks	The detection rate is high gaining high accuracy and less error rate	decrease the transmitting power for broadcasting a beacon message due to Sybil attack	Detection Rate is 40 % False Negative Rate is 90%
Yong Hao, Jin Tang, Yu Cheng	Periodically broadcasting technique	Vehicles detect and quarantine suspect Sybil nodes locally in a cooperative way	Routing overload becomes high by broadcasting fake information due to Sybil nodes	Detection time and vehicles density
Bayrem TRIKI, Slim REKHIS, Mhamed CHAMMEM, and Noureddine BOUDRIGA	Privacy Preserving. RFID	It prevents attackers from tracking the mobility of the vehicles	limitation related to computation, storage, and bandwidth	Certificate renewal ratio 0.23 Certificate revocation ratio 0.25
V. Pa1an1· samy,P. Annda ural , S. Vi1iJ1ilakshm1.	Multicast with group security Agent	The approach is having high packet delivery ratio	Resource allocation is not proper	Packet Delivery ratio is 60 % in presence of attack No. of packets sent to the receiver is 60

IV. CONCLUSION AND FUTURE SCOPE

In Vehicular ad hoc networks, attacks always degrade the service of the entire network. Sybil attack is the attack which is performed very smartly in vanet, resulting in the impairment of the network. For future, we would use the optimization algorithm (Genetic Algorithim) that would enhance the performance with the maintenances of security so that data can be securely transferred from source to destination. This paper has focused on the numerous researches done in term of Sybil attack to find an effective system which would prevent the Sybil attack as well as give better performance by enhancing various parameters.

V. REFERENCES

[1] Cai, Jiwen, et al. "An adaptive approach to detecting black and gray hole attacks in ad hoc network." Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on. IEEE, 2010.

[2] J. R. Douceur, (2002)" The Sybil attack", In Proceedings of the International Workshop on Peer to Peer Systems, pp. 251–260.
[3] Al-Sakib Khan Pathan. Security of Self Organising Neworks: MANET, WSN, WMN and VANET. Auerbach Publications, 2010.
[4] J. Newsome, E. Shi, D. Song, and A. Perrig, (2004)"The Sybil attack in sensor networks: Analysis and defences", In Proceedings of International Symposium on Information Processing in Sensor Networks, pp. 259–268.
[5] F. Anjam, P. Mouchtaris, (2007)"Security For Wireless Ad Hoc Networks", Proc. Intersience Publishing, IEEE.
[6] Wang. Yu, "Using Fuzzy Expert System based on Genetic Algorithm for Intrusion Detection System", IEEE , pp. 201-224, April 2009.
[7] Wei Li, "Using Genetic Algorithm for Network Intrusion Detection", IEEE, pp.1-8, 2010.
[8] Crosbie, Mark, and Gene Spafford. 1995. "Applying Genetic Programming to Intrusion Detection." In Proceedings of 1995 AAAI Fall Symposium on Genetic Programming, pp. 1-8. Cambridge, Massachusetts, 1995.
[9] Anup Goyal and Chetan Kumar, " GA-NIDS: A Genetic Algorithm based Intrusion Detection System", 2010.
[10] Yuteng Guo, Beizeng Wang, Xingxing Zhao, XiaobiaoXie, Lidalin and QindaZhou,"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, China.
[11] Harley Kozhushko, "Intrusion Detection: Host Based and Network-Based Intrusion Detection Systems", Independent Study, 2003.
[12] S. Capkun, J. P. Hubaux, and L. Buttyan, "Mobility helps peer-to-peer security," IEEE Trans. Mobile Comput., vol. 5, no. 1, pp. 43–51, Jan. 2006.

She is pursuing her Master's degree from Chandigarh Engineering College, Mohali, Punjab, India. She has completed her B.Tech Degree from RIEIT Railmajra, Punjab, India. Her area of Interest includes Wireless Communication.

She had completed her Master's degree from BBSBEC, Fatehgarh Sahib, Punjab, India. Currently, she is assistant professor at Chandigarh Engineering College, Mohali, India. Her area of interest includes image processing.