IJCSN International Journal of Computer Science and Network, Volume 4, Issue 3, June 2015
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 0.417

Different Methods Used in VANET to Avoid Attack

Riya Baby

Department of Electronics and Communication,
Mar Baselios Institute of Technology and science,
Nellimattom, Kerala, India

Abstract - VANETs are the promising approach to provide safety and other applications to the drivers as well as passengers. It needs security to implement the wireless environment and serves users with safety and non safety applications. In this paper, we propose different classes of attacks and every class is expected to provide better solution for the VANET attack.

Keywords - *Vehicular Ad-hoc Network, DOS, Sybil Attack, Security.*

1. Introduction

Million people are killed each year on the road accidents. Road traffic safety is the challenging issue in traffic management. One method is to overcome this situation by exchanging the information of traffic environment among the vehicles. VANET is self organized network that can be formed by connecting vehicle, to improve driving safety and traffic management with internet access by drivers. VANET represents a challenging class of MANET that enables vehicle to vehicle communication and vehicle to roadside unit communication. VANETs are playing an important role in accident avoidance, traffic control, and management of parking vehicle in public area. To develop a cooperation based system, give more importance to security and privacy.

To secure the VANET, first we have to discover who are the attacker, their capacity, and nature to damage the system. On the basis of capacity these attackers may be three types. Insiders are the authenticated members of n/w and Outsiders are the intruders and hence limited capacity to attack. These types of attackers are an authentic user of the network and have detail knowledge of network. Malicious attackers have not any personal benefit to attack; they just harm the functionality of the network. Rational attackers have the personal profit hence they are predictable. Active attackers generate signals or packet whereas passive attackers only sense the network.

2. Different Methods

There are different type of attack is occurring in the VANET. Attacks and their solution are given in below.

In the case of DENIAL OF SERVICE (DOS) ATTACK, their major task to avoid the communication between the nodes. For this, they make the node continuously busy or jam the communication channel. To overcome this problem the Processing Unit will suggest to the On Board Unit to switch technology, channel or to use frequency hopping technique.

Whenever attackers jam any one of the channels, there is an option to move to others channels. and also there are different technologies that work with VANET, such as UMTS's Terrestrial Radio Access -Time Division Duplex (UTRA-TDD), Wi-MAX ,Wi-Fi, and Zig-Bee. Whenever attacker launches attack, we can select other techniques.

In spread spectrum communication, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) are used. FHSS changes the communication channel using some regular interval and follow some pseudo-random sequences. it will more difficult in attacker to introduce DOS attack.

Sender and receiver nodes already know the sequence of the hopping and they can exchange the safety messages to each other's. It's making difficult for attackers to launch any attack when the channels/frequencies are rapidly changed. It is also possible for the OBU to have multiple transceivers for sending and receiving messages. If there any case of DOS attacks, the system will have the option

to move from one transceiver to another. This will eliminate the chance for total n/w collapse. As a result, part of the network remains in operation, allowing users to access the network and send/receive critical life information between nodes.

Announce false message:-If the false message can be sign by certified pseudonyms, this attack can be identified by a majority voting method if there are more benign vehicle than attacker. If two or more malicious vehicle reports a fake event, we are using threshold scheme. The number of event reporting vehicle is less than threshold; we consider it as a fake event. The threshold value is depending on the number of vehicle on the road. Node Impersonation is an attempt by a node to send a modified version of a message received from the real originator by doing any accident. To overcome this problem, a unique identifier is assigned to each vehicle node in VANET, which will be used to verify the real message originator.

Sybil attack:-one vehicle will sent multiple message to other vehicle and each message contain different pseudonyms. If multiple vehicle sent message have same coarse grained pseudonyms then it is called false alarm.

To overcome this problem we introduce fine and coarse grained pseudonyms. Coarse grained pseudonyms given to the RSU for find malicious vehicle. After that it is same, we check the position in different time. From this we can find the false alarm. If it is not the false alarm then we check the fine grained pseudonyms present in the DMV. From this we can say it as a Sybil attack and we can avoid this message.

3. Conclusions

VANET will become world largest ad-hoc network. So we want to give more importance to improve the safety. In this paper we discus about different attacks and there solution. To avoid DOS attack we have option to switch the channel and technology. To improve the safety and avoid Sybil attack, we introduce fine and coarse grained pseudonyms. Finding the direction and position we can conclude it is a false alarm. Using voting scheme we can avoid false message.

Acknowledgments

The author would like to thank teachers and friends in Mar Baselios Institute of Technology.

References

[1] P. Golle GREENE D.et STADDON J. “Detecting and Correcting Malicious Data in VANETs ” VANET ’04, 1 Octobre 2004

[2] F. Doetzer, “Privacy issues in vehicular ad hoc networks”, Privacy Enhancing Technologies, Lecture Notes in Computer Science, Springer 2005, pp. 197–209

[3] Tim Leinmuller, Elmar Schoch, and Christian Maihofer, “Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks”, Proceedings of Forth Annual Conference on Wireless on Demand Network Systems and Services Oberguyrgl,pp.84-91, 2007

[4] Halabi Hasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan,"Denial of Service (DOS) Attack and Its Possible Solutions in VANET",World Academy of Science, Engineering and Technology, pp.411-415,Volume-65, 2010

[5] G. Guette,B.Ducourthial,"On the sybil attack detection in VANET",Laboratoire Heudiasyc UMR CNRS 6599,France.

RIYA BABY received the B-Tech. degree in electronics and communication engineering from Mahatma Gandhi University, Kottayam, Kerala, in 2013, and currently pursuing the M-Tech degree in Advanced communication and information system. Her current project interests include vehicular ad hoc networks, mobile cloud computing, and network security.