IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

REVIEW PAPER OF VEHICULAR AD HOC NETWORK (VANETS)

Pawandeep Kaur*, Er. Aayushi Chadha
* Research Scholar, Universal Group of Institutes Lalru, Punjab, India
Assistant Professor, Universal Group of Institutes Lalru, Punjab, India

DOI: 10.5281/zenodo.573534

ABSTRACT

MANET stands for Mobile Ad hoc Network. It is a robust infrastructure less wireless network. malicious vehicles can degrade the network performance by triggering some security attack. VANET are self-configuring networks composed of a collection of vehicles and elements of roadside structure linked with each other without requiring any infrastructure, sending and receiving information of current traffic situation. These are used for the communication among the mobile vehicles. It has some security issues like attacks, authentication etc. In this work, a novel technique has been proposed to detect malicious vehicles and isolate Sybil attack from the network. This will help to improve network performance.

KEYWORDS: VANET, GPS, RSU, DSRC, GPSR, GLS

INTRODUCTION

Vehicular adhoc networks (VANETs) are classified as an application of mobile adhoc network (MANET) the main benefits of VANETs are the potential in providing travellers comfort & they enhance road safety and vehicle security while protecting driver's privacy from attacks perpetrated by adversaries. Recently VANETs have emerged to turn the attention of researchers in the field of wireless and mobile communications.Vehicular adhoc network are wireless networks where all the vehicles from the nodes of the network. It is for the driver comfort and road safety, the inter-vehicle communication provide them. Vehicular ad-hoc network is subclass of mobile ad hoc networks which provides a distinguished approach for intelligent transport system. It is autonomous and self-organizing wireless communication network, where all the nodes in VANET involve themselves as servers or client for exchanging and sharing information. The network architecture of VANET can be classified into three categories pure cellular, pure ad-hoc and hybrid. Currently, DSRC (Dedicated Short-Range Communication) has been proposed as the communications standard specifically for VANETs, it is a short medium range communications service that offers very low latency and high data rate.

APPLICATIONS

Safety applications: Safety applications are most important factor to decrease the road accident and loss of life of the occupants of vehicles. There are so many accident happened due to the collision of vehicles.

Car speed warning: With help of these protocols use a combination of GPS and digital maps are used to judge threat level for driver approaching a curve quickly.

Traffic signal violation warning: It is also designed to send a warning message when driver detects the vehicle is in risk of running the traffic signal. The decision to send a message is made on the basis of traffic signal status and timing the vehicle position and speed.

Collision risk warning*:* in this system vehicle and RSU detect chances of collision between multiple vehicles are not able to communicate amongst themselves. The system will collect data about vehicles that are coming in opposite direction and are approaching towards the destination.

Lane change warning: In this application vehicle monitor the position of vehicle within a roadway lane and warn a driver if it is unsafe to change lanes.

Sybil Attack in VANET

It consists of sending multiple messages from one node with multiple identities. Sybil attack is always possible except the extreme conditions and assumptions of the possibility of resource parity and coordination among entities. When any node creates multiple copies of itself then it creates confusion in the network. Claim all the illegal and fake ID's and Authority. It can create collision in the network. This type of situation is known as Sybil attack in the network. This system can attack both internally and externally in which external attacks can be restricted by authentication but not internal attacks. As there is one to one mapping between identity and entity in the network.

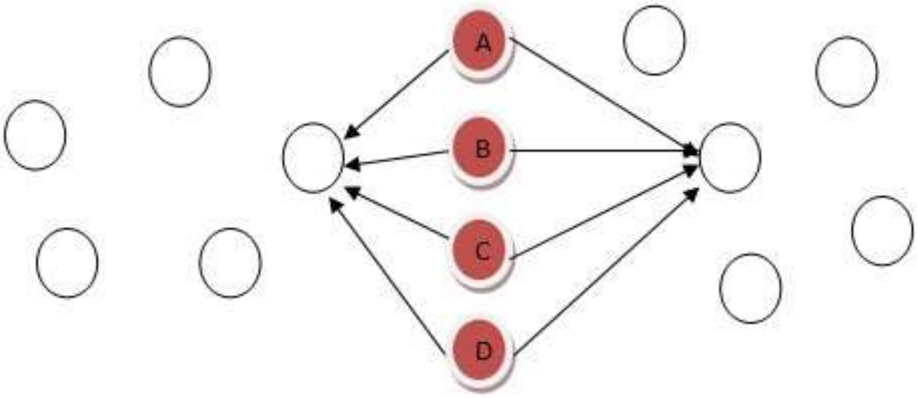

Figure 1.1: Sybil Attack

A, B, C ,D nodes are Sybil nodes which create fake or similar identity in the network and collapse the network.

RELATED WORK

The introduction of IEEE 802.11 along with advanced wireless ad-hoc networks and location-based routing algorithms makes vehicle-to-vehicle communication viable/possible. Applications for inter-vehicle communication include intelligent cruise control, lane access and emergency warning systems among others. The Vehicular systems employ wireless ad-hoc Networks and GPS to determine and maintain the inter-vehicular separation necessary to ensure the one hop and multi hop communications needed to maintain spacing between vehicles. Location based routing algorithms are flexible and efficient enough with regards inter-vehicular communication so, they form the basis of any VANET (R. A. Santos et al.). Some of location-based algorithms are Greedy Perimeter Stateless Routing (GPSR), Grid Location Service (GLS), Location Aided Routing (LAR) and Distance Routing Effect Algorithm for Mobility (DREAM). Location-Based Routing Algorithm with Cluster-Based Flooding (LORA-CBF) is an option for present and future automotive applications. A vehicle to vehicle communication for cooperative collision warning as proposed by Xue Yang et al. (2004) provides such facilities to a large extend but the wireless communication used is unreliable due to channel fading, packet collisions, and communication obstacles, can prevent messages from being correctly delivered in time. The necessary condition for the support of message differentiation is that underlying MAC protocol should provide service differentiation among different classes of messages. The 802.11e EDCF (Enhanced Distributed Coordinated Function), an extension to IEEE 802.11 provides such a function (G. Chesson et al., 2002). In 802.11e EDCF, different levels of channel access priorities can be provided through different choices of Inter Frame Space (IFS) and contention window (CW) sizes. Corresponding to different delay requirements, three classes of messages are defined, where class 1 messages have the highest priority to be transmitted and class 3 messages have the lowest priority. The VANET is the self configuring type of network, in which the vehicles can move freely in the network. In such type of network, there are more chances that malicious vehicles can join the network and trigger some type of attack. Among the possible attacks Sybil attack is the most harmful attack which is possible in the network. This attack will reduce the network performance. In this work, we will work on to detect malicious vehicles in the network which is responsible to trigger such type of attacks.

CONCLUSION

The vehicular adhoc network is the self-configuring type of network in which vehicles can move freely on the roads. The vehicle adhoc network is the decentralized type of network in which vehicles can join or leave the network when they want. Due to such type of network nature many malicious nodes may join the network which are responsible to trigger various type of security attacks. The Sybil attack is most common type of attack in which malicious nodes can change its identification time to time. In this work, it is been concluded that Sybil attack reduced network performance in terms of throughput, delay and packet loss. In this work, technique will be proposed which will be based on network information and monitor mode technique. The simulation is performed in NS2 and it has been analyzed that proposed technique will detect malicious nodes from the network in minimum amount of time. In future proposed technique will be applied for the detection of wormhole attack in the network.

REFERENCES

[1] Raya, M., & Hubaux, J. P. “Securing vehicular ad hoc networks”, Journal of Computer Security, 15(1), pp.39-68, 2007.

[2] Iqbal, S., Chowdhury, S. R., Hyder, C. S., Vasilakos, A. V., & Wang, C. X. “ Vehicular communication: protocol design, test bed implementation and performance analysis”, In Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly , pp. 410-415, 2009.

[3] Xiao, B., Yu, B., & Gao, C. “Detection and localization of sybil nodes in VANETs”, In Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks pp. 1-8,2006.

[4] Hao, Y., Tang, J., & Cheng, Y. “Cooperative sybil attack detection for position based applications in privacy preserved VANETs” IEEE In Global Telecommunications Conference (GLOBECOM 2011), IEEE pp. 1-5, 2011

[5] Chang, S., Qi, Y., Zhu, H., Zhao, J., & Shen, X. “Footprint: Detecting sybil attacks in urban vehicular networks”, IEEE sponsored Parallel and Distributed Systems, IEEE Transactions on, 23(6), pp.1103-1114, 2011.

[6] Chang, S., Qi, Y., Zhu, H., Zhao, J., & Shen, X. “Footprint: Detecting sybil attacks in urban vehicular networks”, IEEE sponsored Parallel and Distributed Systems, IEEE Transactions on, 23(6), pp.1103-1114, 2011.

[7] Lee, B., Jeong, E., & Jung, I. “A DTSA (Detection Technique against a Sybil Attack) Protocol using SKC (Session Key based Certificate) on VANET”, International Journal of Security & Its Applications, 7(3), pp.1-10, 2013.

[8] Li, M., Xiong, Y., Wu, X., Zhou, X., Sun, Y., Chen, S., & Zhu, X.” A Regional Statistics Detection Scheme against Sybil Attacks in WSNs”, IEEE Sponsored In Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on pp. 285-291, 2013.

[9] Ganan, C., Munoz, J. L., Esparza, O., Mata-Diaz, J., & Alins, J.”PPREM: privacy preserving revocation mechanism for vehicular ad hoc networks”, Computer Standards & Interfaces, 36(3), pp-513-523, 2014.

[10] Balamahalakshmi D., & Shankar M. K. V., “Sybil Attack Detection with Reduced Bandwidth Overhead in Urban Vehicular Networks”, International Journal of Engine ring Trends and Technology (IJETT) – Volume 12, pp. 578 – 584, 2014.

CITE AN ARTICLE

Kaur, P., & Chadha, A., Er. (2017). REVIEW PAPER OF VEHICULAR AD HOC NETWORK (VANETS). *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, 6*(5), 296-298. doi:10.5281/zenodo.573534