Engineering Universe for scientific Research and management
ISSN (Online): 2319-3069
Vol. XIII Issue IX
September 2021

A REVIEW ON EFFICIENT AGAINST DOS ATTACKS IN VEHICULAR AD-HOC NETWORK

Vivek Kumar[1], Prof. Chetan Agarwal[2], Prof. Vijendra Palash[3]
[1,2,3] Department of Computer Science Engineering RITS, Bhopal, (MP), India
viveksrist@gmaill.com

ABSTRACT Recently, vehicular ad hoc networks (VANETs) got much popularity and are now being considered as integral parts of the automobile industry. As a subclass of MANETs, the VANETs are being used in the intelligent transport system (ITS) to support passengers, vehicles, and facilities like road protection, including misadventure warnings and driver succor, along with other infotainment services. The advantages and comforts of VANETs are obvious; however, with the continuous progression in autonomous automobile technologies, VANETs are facing numerous security challenges including DoS, Sybil, impersonation, replay, and related attacks. This paper discusses the characteristics and security issues including attacks and threats at different protocol layers of the VANETs architecture. Moreover, the paper also surveys different countermeasures.

KEYWORDS: vehicular ad hoc networks, intelligent transport system, different protocol layers, support passengers.

INTRODUCTION

Aiming at ensuring the safety and facilitating the passengers and driver, the VANETs are getting much popularity and attention from the researchers VANETs are the networks of vehicles communication and road infrastructures to extend road safety and infotainment The wireless sensors are fitted within vehicles, accompanied with positioning devices and maps. Through On-Board Unit (OBU), the vehicles are connected with road-side units (RSUs) to share intervehicle and vehicle to RSU, the safety related and otherwise information The VANETs consist of short-range communication infrastructure. Therefore, the source and destination share information through intermediate nodes. Like OBU, RSU, the trusted authority (TA) is also an entity of the VANETs architecture and is responsible for controlling and supervising the whole network.

OVERVIEW OF VANETs

The VANETs architecture contains the OBU, RSU, and TA. There are two types of communication technologies in VANETs architecture, i.e., (1) vehicle to vehicle (V2V) and (2) vehicle to infrastructure (V2I) communication as shown in Figure 1. V2V contact vehicles converse with one another and exchange the traffic-related information inside the wireless network range In such networks, when any unforeseen incident happens, such as accident or traffic blockage on the road, instantly a vehicle sends an alert signal to the other nodes or vehicles in the network suggesting to avoid that particular road or area. The vehicle, employing V2I communication, shares the information with RSU which is part of infrastructure installed on the road. The V2I-based communication notifies the driver about traffic and weather updates to keep an eye on the nearby environment. RSU and OBU are registered by a trusted authority, which is used to keep up and

supervise the VANETs system. The road-side unit positions itself on the road for authentication and communication between TA and OBU. With the use of dedicated short-range communication (DSRC) [6], the OBU fitted in each vehicle can transmit traffic information to nearby vehicles and RSU.

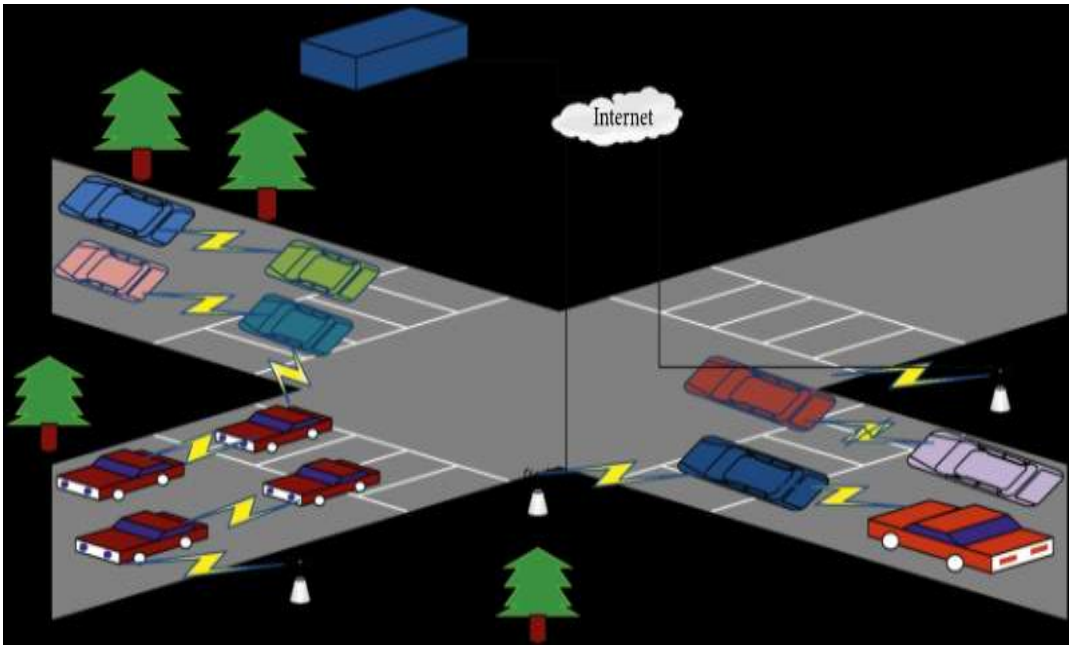

Fig.1: VANETs architectures.

VANETs is a dynamic ad hoc network that enables the vehicles converse with one another using fixed and mobile nodes offering numerous services, however with narrow access to the network's infrastructure. Compared to the MANETs, the VANETs have high mobility features and normally vary in topology. In VANETs, vehicles or nodes move arbitrarily in the network, and their movement transforms the network topology. VANETs topology is complex and dynamic because of the strong mobility factor of nodes . The features of VANETs are mentioned below. Because of the high mobility, the VANETs have good versatility relative to MANETs, and they play a significant role in modelling VANETs protocol. In VANETs, every node moves quickly; thus, vehicles' mobility minimizes the communication time in the network The VANETs might get better driver protection, improve traveller console, and support a better flow of traffic. The core benefit of VANETs is that nodes communicate straight to everyone In VANETs; the topology design is vibrant because the vehicle speed of mobility is very high. Therefore, the forecast of node position is very tough to compute. The high speed of vehicle networks is extra weak to attacks, and it is incredibly complicated to identify intruders and vehicles if something is wrong in a network Due to high-speed mobility vehicles, traffic congestion or even lousy weather, the network may experience freq Eavesdropping assault is a type of passive assault and is done in the privacy of the network. Assailant collects the secret information, and the attacker secretly monitors the traffic flow of the network or the existing location and actions of a specific vehicle. This type of assault cannot be detected easily because the attacker performs its activity without any kind of reaction. Figure 2 shows that Car C regularly monitors ATM's cash van's facts and leaks such information to the intruder. ID revelation assault is a subcategory of eavesdropping where the assailant exposes the identity vehicle and uses it to track the under-attack vehicle. In this situation, the nodes may receive proper guidance from the V2I infrastructure

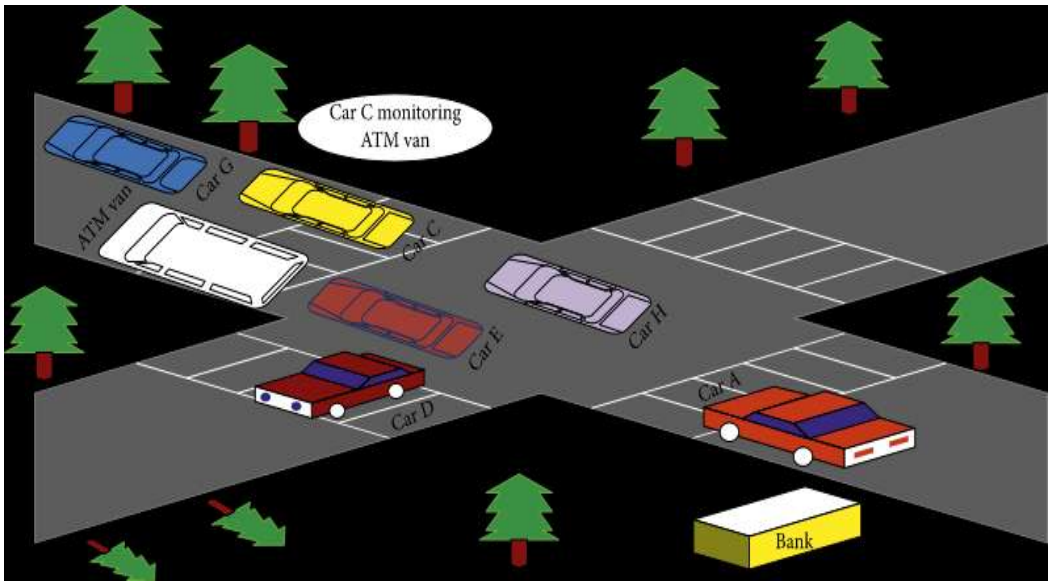

Fig.2: Eavesdropping assault.

Vehicular Ad hoc Network (VANET) is a development of Mobile Ad Hoc Network (MANET), VANET is a combination of vehicles equipped with wireless devices. Communication occurs on the highway between vehicles with other vehicles, vehicles with infrastructure, namely the Road Side Unit (RSU). Communication between vehicles and RSU is referred to as the Intelligent Transport System (ITS). The aim of VANET is to help people avoid vehicle accidents, according to the US Department of Transportation (USDOT). It is intended to describe how vehicles can be connected to overcome some problems such as safety and the environment. VANET has several possible attacks, Sybil attacks, timing attacks, replay attacks, routing attacks, DOS attacks are a few examples. This can be seen from the motives of the perpetrators, as well as the use of security holes in accordance with the security requirements that are targeted.

Vehicular Ad-Hoc Networks (VANET) are a proper subset of mobile wireless networks, where nodes are revulsive, the vehicles are armed with special electronic devices on the motherboard OBU (On Board Unit) which enables them to transmit and receive messages from other vehicles in the VANET. Furthermore the communication between the vehicles, the VANET interface is donated by the contact points with road infrastructure. VANET is a subgroup of MANETs. Unlike the MANETs nodes, VANET nodes are moving very fast. Impound a permanent route for the dissemination of emergency messages and alerts from a danger zone is a very challenging task. Therefore, routing plays a significant duty in VANETs. Decreasing network overhead, avoiding network congestion, increasing traffic congestion and packet delivery ratio are the most important issues associated with routing in VANETs. In addition, VANET network is subject to various security attacks. In base VANET systems, an algorithm is used to discover attacks at the time of confirmation in which overhead delay occurs. This paper proposes (P-Secure) approach which is used for the detection of DoS attacks before the confirmation time. This reduces the overhead delays for processing and increasing the security in VANETs. Simulation results show that the P-Secure approach, is more efficient than OBU model VANET approach in terms of PDR, e2e_delay, throughput and drop packet rate. ANETs applications and requirements There are two main types of applications in VANETs which are comfort (information/entertainment) applications, safety applications, and transport efficiency applications Comfort applications are related with providing suitable convenience means for passengers like traffic information system, weather information, and locations of some centres of services such as gas stations and restaurants. Safety applications are related with enhancing the safety of passengers (vehicles) along the road; and this type of applications depends deeply on a trust negotiation between vehicles and

remote base stations (IVC). Examples of safety applications such as receiving warning messages about emergency case (flood of water crosses a road at a specific space) at a certain distance in the road or an accident happened and vehicles traffic has to be changed to another direction. Transport efficiency applications aim to achieve an ideal use of road traffic, and also minimize vehicles collisions and traffic load. An example for the previous application is an advisory system delivered by vehicles through the road by trusted base stations to tell them about the optimal speed to arrive at the green phase of a traffic system.

VANETs exhibits special characteristics where communicating vehicles move with various accelerations and the established successful communication channels among vehicles depend on trust interactions between vehicles. For the previous reasons, some requirements should be found to achieve success for VANETs applications such as increasing the ratio of vehicles equipped with VANET tools to other vehicles which have not. In addition some technical aspects are important such as required message size, frequency, latency constraints, communication ranges, and security levels [13]. Moreover, besides the last mentioned requirements, there is a dominant factor in achieving success in VANETs applications which is establishing secure Reputation Management Systems (RMS). This system can build strong relationship between vehicles, assign, and isolate the malicious and selfish vehicles from the network.

CONCLUSION

From the research that has been done, it can be concluded that based on the security requirements and types of attacks that can occur in VANET, network availability is the first and most important thing because it is related to network services, if not available, users will lose the benefits of safety and non-safety applications. In order to be used properly, network services must be available at all times, but attacks on DoS that are carried out can result in availability being disrupted. This attack is categorized as the first class because it diverts services from the start and prevents sending information between nodes and infrastructure. In this paper, we describe the VANET architecture, attack type, type of attack, several methods and models to cancel and reduce the risk of attacks, not only DoS also includes DDoS. The most important thing
is to maintain availability on the network, messages generated by VANET services

REFERENCES

[1] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, “Vehicular Ad Hoc Networks (VANETs): Status, Results, and Challenges”, in Telecommunication Systems, Volume 50, Issue 4, pp 217-241, 2017.

[2] Irshad Ahmed Sumra, Iftikhar Ahmad, Halabi Hasbullah, Jamalul-lail bin Ab Manan, “Classes of attacks in VANET”, in Tenth International Conference on Wireless and Optical Communications Networks (WOCN), pp 1 - 5, 2013.

[3] Al-kahtani, Salman bin Abdulaziz, Al Kharj, “Survey on security attacks in Vehicular Ad hoc Networks (VANETs)”, in 6th International Conference on Signal Processing and Communication Systems (ICSPCS), pp 1 - 9, 2012.

[4] Kadam Megha V, “Security Analysis in VANETs: A Survey”, in International Journal of Engineering Research and Technology (IJERT), Vol. 1 Issue 8, October - 2012.

[5] Mahmoud Al-Qutayri, Chan Yeun and Faisal Al-Hawi, “Security and Privacy of Intelligent VANETs”, in Computational Intelligence and Modern Heuristics, book edited by Al-Dahoud Ali, 2010.

[6] J.T. Isaac, S. Zeadally, and J.S. Cmara, “Security attacks and solutions for vehicular ad hoc networks”, in IET Communications, pp. 894-903, 2009.

[7] Xiaodong Lin, Rongxing Lu, Chenxi Zhang, Haojin Zhu, Pin-Han Ho, and Xuemin (Sherman) Shen, “Security in Vehicular Ad Hoc Networks ”, in IEEE Communications Magazine , pp. 88-95, 2008.

[8] M. Raya, J. Pierre Hubaux, “Securing vehicular ad hoc Networks”, in Journal of Computer Security, vol.15, January 2007, pp. 39-68.

[9] I.Ahmed Soomro, H.B.Hasbullah, J.lb.Ab Manan, “Denial of Service (DOS) Attack and Its Possible Solutions in VANET”, in WASET, issue 65, 2010 ISSN 2070-3724.

[10] I.Chen Chen, Xin Wang, Weili Han, and Binyu Zang, “A Robust Detection of the Sybil Attack in Urban VANETs ”, in Distributed Computing Systems Workshop, ICDCS Workshops ’09. 29th IEEE International Conference, 2009, pp. 270-276, 2009.

[11] Chim Tat Wing, “Secure and Privacy-preserving Protocols for VANETs”, in PhD thesis at The University of Hong Kong, August 2011.
[12] Lei Zhang, “Research on Security and Privacy in Vehicular Ad Hoc Networks”, in PhD thesis at Universitat Rovira i Virgili, June 2010.
[13] J.Douceur, “The Sybil Attack”, in First International Workshop on Peer-to-Peer Systems, 2002, pp. 251-260.
[14] J.Newsome, E.Shi, D.Song and A.Perrig, “Loc & Defenses”, in International symposium on information processing in sensor networks, 2004, pp. 259-268.
[15] Gilles Guette, Bertrand Ducourthial, “On the Sybil attack detection in VANET ”, in IEEE International Conference on Mobile Ad hoc and Sensor Systems, 2007, pp. 1-6.
[16] Bin Xiao, Bo Yu, Chuanshan Gao, “Detection and localization of Sybil nodes in VANETs”, in DIWANS ’06, pp. 1-8.
[17] S. S. Manvi, M. S. Kakkasageri, D. G. Adiga, “Message Authentication in Vehicular Ad hoc Networks: ECDSA Based Approach”, in International Conference on Future Computer and Communication, 2009, pp. 16-20.
[18] Jinyuan Sun, Yuguang Fang, “A defense technique against misbehavior in VANETs based on threshold authentication”, in Military Communications Conference MILCOM 2008. IEEE, 2008, pp. 1-7.
[19] Tat Wing Chim, S.M. Yiu, L.C.K. Hui and V.O.K Li, “Security and Privacy Issues for Inter-vehicle Communications in VANETs”, in Sensor, Mesh and Ad Hoc Communications and Networks Workshops, 2009, pp. 1-3.
[20] T.W. Chima, S.M. Yiu, Lucas C.K. Hui, Victor O.K. Li, “SPECS: Secure and privacy enhancing communications schemes for VANETs”, in Journal of Ad Hoc Networks 9, 2011, pp. 189-203.
[21] Chenxi Zhang, Rongxing Lu, Xiaodong Lin, Pin-Han Ho, and Xuemin (Sherman) Shen, “An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks”, in IEEE INFOCOM 2008 proceedings, 2008, pp. 816-824.
[22] Y.C. Hu, A. Perrig and D.B Johnson, “Packet leashes: a defense against wormhole attacks in wireless networks”, in INFOCOM. Twenty- Second Annual Joint Conferences of the IEEE Computer and Communications, 2003, pp. 1976-1986.
[23] Nai-Wei Lo, Hsiao-Chien Tsa, “Illusion Attack on VANET Applications - A Message Plausibility Problem”, in Globecom Workshops, 2007, pp. 1-8.
[24] Soyoung Park, B. Aslam, D. Turgut and C.C. Zou, “Defense against Sybil attack in vehicular ad hoc network based on roadside unit support”, in Military Communications Conference, MILCOM, 2009, pp. 1-7.
[25] B. Parno and A. Perrig, “Challenges in Securing Vehicular Networks”, in Hot Topics in Networks (HotNets-IV), 2005