AMSE Association for the Advancement of Modelling & Simulation Techniques in Enterprises
IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Advances in Modelling and Analysis B
Vol. 62, No. 2-4, December, 2019, pp. 48-52
Journal homepage: http://iieta.org/journals/ama_b

A Detailed Case Study on VANET Security Requirements, Attacks and Challenges

Ravula Prathap Kumar[1*], Munisamy Shanmugam[2]

[1] Department of Computer Science & Engineering, Vadlamudi, Guntur, India
[2] Vignan's Foundation for Science, Technology & Research (Deemed to be University), Vadlamudi, Guntur, India

Corresponding Author Email: prathapkumar.r2008@gmail.com

https://doi.org/10.18280/ama_b.622-403

Received: 10 October 2018
Accepted: 13 June 2019

Keywords:
VANETs, MANETs, malicious nodes, OBUs, RSUs, security

ABSTRACT

VANETs specially appointed systems is a sub category of MANETs. It alludes to an arrangement of smart vehicles travelled on the road. These can furnish communication with another using OBU or with RSU based on WLAN innovations. The primary favorable position of them are that they improve Information privacy and vehicle safety by shielding vehicle drivers/passengers protection from attackers. Security is a champion among the most fundamental issues associated with VANETs since the data delivered is disseminated in a spread out condition. They confront numerous difficulties. In this study, we talk about the security requirements, different attacks of VANETs and challenges.

1. INTRODUCTION

A Vehicular Ad hoc Network (VANET) is a ceaselessly self-designing, infrastructure less system of cell phones associated remotely. These can furnish communication with another using OBU or with RSU based on WLAN innovations. In this kind of system, vehicles are considered as communication nodes that can be long to a self-sorting out system without earlier information of other's essence. Two classifications of nodes are: On-Board Units (OBUs) and Road Side Units (RSUs). OBUs are fixed inside the vehicle and they are communicating with other vehicles. while RSUs are used for reliably routing the packets in VANETSs. OBUs can interface the vehicle to RSUs with Dedicated Short Range Communication (DSRC) radios. VANETs contrast from MANETs in various ways: high node versatility, extensive size of networks, a geo-graphically compelled topology i.e profoundly unique, strict continuous due date, inconsistent channel conditions, unavoidably moderate deployment, sporadic availability between nodes, driver conduct and successive network discontinuity. The reason for utilizing VANETs is to permit communication amongst vehicles and amongst vehicles and road infrastructure. Keeping in mind the end goal to be an essential part of a VANET and to convey productively, nodes require certain highlights that will help them to assemble data, to illuminate their neighbors and to settle on choices by thinking about the majority of the gathered data. Such highlights are sensors, cameras, on-board PCs, GPS, EDR and omnidirectional antennas.

VANET innovation displays certain preferences, for example, a decrease in the quantity of road collisions, a more agreeable driving and travelling knowledge with rearrangements of certain toll payment processes, stopping, fuel, and so forth. These innovations need information communication between vehicless. The content of the information can affect drivers conduct. It can alter the system topology and security ought to be undermined if a malicious client modifies information [1]. Very few conceivable attacks would aim congested driving conditions, spread counterfeit data, cheat the situating data, disclose IDs, replay, masquerade or then again fashion information, disregard security or cause wormholes, DoS attacks as well as hardware altering [1].

Figure 1. Vehicular Ad-hoc network

2. SECURITY REQUIREMENTS OF VANETS

2.1 Data authentication and integrity

The authorization levels of vehicles are controlled by authentication [1]. Authentication means verifying user's permissions of two vehicles. It ensures that the message transfer between two vehicles is appropriate only when they are authenticated. Integrity protects the data from unauthorized users that cannot alter or corrupt the messages. It ensures that the correct delivery of message to the receiver from the sender [1].

2.2 Data confidentiality

It ensures that the data transmission between vehicles and remote stations secretly using encryption techniques [2]. The message should not be revealed to outsiders from gaining the drivers information. Confidentiality to ensure secure communications using encryption algorithms [1]. Any vehicle information such as vehicle speed, time to travel, round trip

travel route and violation ought to be stored in a TPD and it should be extracted by any authorized authority person [1, 3].

2.3 Vehicle privacy and anonymity

It ensures that the personal and private information of drivers and vehicles can not be disclosed to unauthorized access. The information like an identity and driving behaviour of driver, the previous and current locations of the vehicle should be private and drivers want to disclose it [1]. Temporary (anonymous) keys are used to achieve the privacy and these keys will be changed frequently as each key could be utilized once and expires immediatley and all the keys ought to store.

2.4 Access control

It ensures that the role of determining rights and privileges to all nodes in the network. Hence all the nodes in the network perform their functions according to the roles and privileges authorized to them. There are two kinds of tickets: TGT and TGS. The TGT enables the customer to get TGSs while TGSs give benefit access to the customers. Subsequently, customers should first acquire a TGT before they ask for a TGS for each dministration they need to utilize. Henceforth, the entrance control prepares another guarantee which stops unapproved individual from getting to the administrations for which they don't approach rights [1, 3, 4].

2.5 Data non-repudiation

It ensures that identify the attackers even after the crash happened using the information of a vehicle which was stored in TPD. The information such as route trip, speed of the vehicle, time, etc. Only specific authorities are allowed to retrieve the data.

2.6 Vehicle ID traceability

It ensures that the ability to disclose actual identities of message senders in order to protect the true information when there is any dispute [2]. Only authorities can reveal this.

2.7 Scalability

There might be an extensive number of verification requests send to the confirmation server during traffic congestion. The system may then be cut down, and to guarantee the correspondence amongst vehicles and vehicles to infrastructures without disruption, an elective channel ought to be given [5].

2.8 Efficiency and Robustness

It ensures that the transferred messages have less overhead, computation, and processing delays. Also, VANET has the ability to deliver services under different attacks [2].

2.9 Forgery

Vehicles injects large volumes of wrong messages or wrong emergency warnings which can leads to abnormal conditions in the system [2, 6].

2.10 Availability

It ensures that the availability of information to the legitimate users even there are awful situations or wrong occasions. It guarantees that the accessibility of data to the honest to goodness clients even there are awful conditions or false occasions. Likewise, the capacity of system to confront diverse sorts of attacks and still gives its administration [2]. To overcome the loss of communication between the nodes and the controller, availability in wireless channel is always issued. To overcome that the software defined VANET adds a recovery setup that restores the system's functionality. Moreover, each SDN (Software Defined Node) node contains an intelligent system that deals with such type of problems [7].

3. CAPTION

3.1 Attackers on vehicular ADHOC network

Attacker is one who modifies or delete the vital information. To secure the VANET, first we need to know different attackers, their temperament, and ability to harm the network. Based on it the attackers might be categorized into three kinds.

3.1.1 Insider and outsider

The validated individuals of network are insiders while Outsiders are the non-authenticated members of the networks and henceforth, they have restricted ability to attack the network. Outsiders performs eavesdrop attack and Dos attack. An attacker can surge or stick the system with sham messages, despite the fact that he doesn't belong to the network, a few vehicles in system might get these messages and system will be goes down hence [1, 6, 7].

3.1.2 Malicious and rational

The main aim of Malicious attackers is cutting down or hurting the system. They have no specific target [1, 6, 7]. The main aim of Rational attackers has particular target. They can be high perilous [1, 6, 7].

• **Active and Passive**: Active attackers produce signals or packet. Active aattackers are thosewho are residing inside the network [1, 6, 7]. Passive attackers are those who are outside the network and they have only sensed the network [1, 6, 7].

3.2 Attacks in VANETs

Several attacks that can influence execution of acitvity in VANETs. A portion of them are inside and other ones are outside attacks.

3.2.1 Attack on identification and authentication

Impersonation Attack: The malicious node can destroy the proper functioning of the network by inserting false information into it. Impersonation attacks mainly depends on authentication and confidentiality. A unique network ID is assigned to each and every vehicle. The ID is important when the accident happened. In this type, the attacker gets an ID of sender, modified the message and passes it to receiver. This leads authentication proecess violation. Hence malicious message is like originated from the sender [8-10].

Sybil Attack: Multiple fake identities are created by attacker. He acts as a few nodes to take part in the network. He sends the traffic jam messages or false messages to other

vehicles. The purpose is to direct vehicles on road to go away from other route for the favor of attacker [11-14].

3.2.2 Attack on privacy

It is related to the illegally obtaining sensitive information of the vehicles in the network. Taken care is needed to do not accessing the private information of the vehicle drivers and vehicles by unauthorized users [15]. Personal informtaion of a driver is ID, driving license, age, name etc. or belongs to car's trip path, speed etc [16].

Session hijacking: Attacker hijack and take the control of the session after connection is established [6].

Identity revealing: The Private information of the owner can be stolen by the vehicles driver. Hence identity of the owner can be put the privacy at risk [17]. The attacker observes the target vehicle and sends harmful message to it. When it is overwhelmed with virus will take ID of the vehicle [9].

Location Tracking: The system connects with WiFi access point and tracking the location of a client within the access point range. System tracks the information of a driver and pass it to the navigator server for the period of time. The attacker observes the target vehicle and sends harmful message to it. When it is overwhelmed with virus will take location of the vehicle and route of the vehicle in time constraint [9, 14, 18].

3.2.3 Attack on availability

The system and applications ought to stay operational even within the sight of issues or malicious conditions [1].

Network Denial of Service: DOS attack objective is to make the network down to make network resources and services unavailable to the legitimate vehicles from accessing. It is either by blocking the physical channel or by "Sleep Deprivation".DoS attacks can be carried out in following ways. First one is to consume bandwidth of communication medium. Seconde one is to prevent vehicles to access to network services [16]. For example, an attacker may continually broadcast a several false messages to flood the network aiming to bring down the transmission channel so that vehicles cannot exchange messages safely [15, 17].

Distributed DoS attack: DDOS attack is more dangerous than DOS attack as it is distributed in manner. In this, several attackers attack the real client from getting to the victim node from accessing the service. In this attacker utilizes distinctive area to dispatch the attack.The fundamental target is to bringing down the system so the system won't be accessible to the clients [2, 13].

3.2.4 Routing attack

In this type of attack, the malicious node may fall down the packet or interrupt the routing process. Possible routing attacks are as follows.

Black Hole attack: In this, the malicious node entirely utilized the routing protocol and it drops the packets instead of delivering them to the destination node. Before dropping the packets it atracts the nodes by sending malicious route reply continually [2, 16, 18].

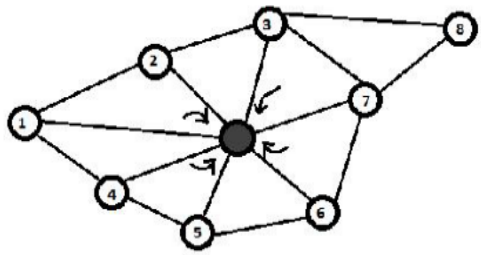

Figure 2. Blackhole attack

Worm Hole attack: The malicious node interrupts routing process by capturing the packets form one place and transmits them to another distant place. Packets are locally distributed. Wormhole attack is launched by malicious node easily without having any knowledge of the network or cryptographic mechanisms [18].

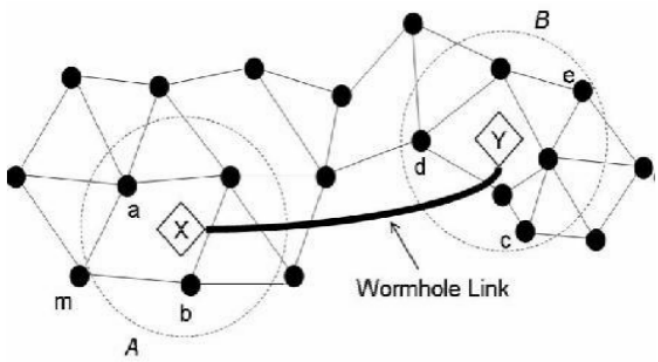

Figure 3. Wormhole attack

A high speed connection is created among two remote nodes as depicted in Figure 3 Legitimate vehicles in transmission range of this two remote nodes (X and Y) use this connection for transferring their data. An attacker can drop the data over the connection [16].

3.2.5 Attack on confidentiality

Eavesdropping: This attack is used against the confidentiality. The main object of this attack is to retrieve the confidential data such as a phone calls, SMS, Video calls or fax etc. In this attack, the attacker must be resided in a vehicle or near RSU and then traps the related data. Message encryption techniques can be used to prevent eavesdropping attacks [1, 8, 16, 17].

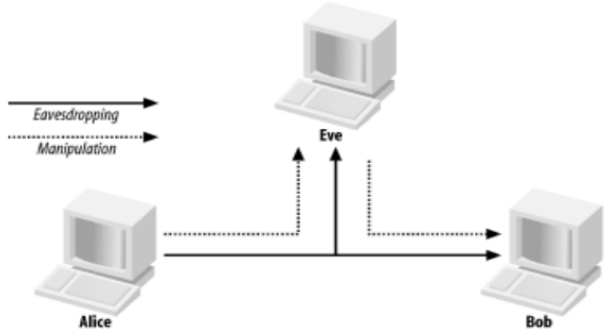

Figure 4. Eavesdropping

Table 1. Comparision of different attacks

Attack type	Security requirements	Application area	Layer	Reference
Impersonation Attack	Identification and Authentication	Traffic efficiency	Application /Transport	[14, 16]
Sybil	Identification and Authentication	Traffic safety Traffic efficiency	Network	[6, 17, 18]
Session hijacking	Privacy	Traffic safety	Transport	[6, 16]
Identity revealing	Privacy	Traffic safety	Physical	[16]
Location tracking	Privacy	Traffic safety	Network	[7]
DOS	Availability	Traffic safety	Network	[6, 16, 18, 19]
DDOS	Availability	Traffic efficiency	Network	[6, 16, 18, 19]
Blackhole	Routing	Traffic safety Traffic efficiency	Network	[11, 18]
Wormhole	Routing	Traffic safety Traffic efficiency	Physical	[11]
Eavesdropping	confidentiality	Traffic safety	Physical	[6]

4. CHALLENGES

Many challenges be tended to by the research group and the business. A portion of them as follows:

4.1 Time constraints

VANET is time basic where messages identified with safety ought to be sent with in the length of the time restrict. So, to achieve continuous requirement, fast cryptographic calculation ought to be utilized. Message and vehicles confirmation would be difficult [1, 8]. For example, all emergency service apllications include this for delivering the information. The client has adequate time to respond after receiving the warning message. The consequences may be catastrophic if the arrival due time is met [1].

4.2 The scale of the network

VANET is the greatest specially appointed system on the planet. The quantity of nodes in the system is growing day by day in huge amount [1]. This may influence their capacities if there is no vigorous private system which can circulate cryptographic keys for that huge quantity of nodes. As a result of that, an examinined framework ought to be designed before sending VANETs to make certain of its scalability for any adjustments in vehicular communication [1, 8].

4.3 The high mobility of nodes

Nodes in VANETs generally change topology at rapid speed. Hence predicting a vehicles location and making the vehicle privacy is much more difficult. It is difficult to apply traditional verification mechanisms for vehicles and information due to the vehicles mobility is high [1, 8].

4.4 Network volatility

The connection among two vehicles can be temporary due to high mobility of vehicles in the network. Hence connections will be lost frequently [1]. Furthermore, the connected vehicles could even travel in opposite directions. Applying securing approaches relying upon checking identities is hard [1, 8].

4.5 Incentives

These incentives could be lessen the quantity of vehicle hazards and enhance the passengers safety. Drivers have to be cautioned before 2 seconds of collision, the accident rate will be enormously reduced [1]. Numerous vehicle collisions ought to be encountered crossing points. Hence driving at crossing points is one of the important challenges to the drivers [1, 8].

5. CONCLUSION AND FUTURE WORK

Vehicle drivers need privacy and security of information and they need safety when they are travelling on the road in future and it might be conceivable by actualizing secure and passengers safe VANET applications which is a rising innovation. This innovation is a rich region for attackers who attempt to modify the vehicles information with their malicious attacks. In this paper we showed some Security requirements, Challenges and some conceivable attacks furthermore, their comparisons. In future we plan to build up the network for identifying the critical attacks and confirming it through simulation by applying our original thought on the method to secure the messages in vehicular communication.

REFERENCES

[1] Engoulou, R.G., Bellaïche, M., Pierre, S., Quintero, A. (2014). VANET security surveys. Computer Communications, 44: 1-13. https://doi.org/10.1016/j.comcom.2014.02.020

[2] Mokhtar, B., Azab, M. (2015). Survey on security issues in vehicular ad hoc networks. Alexandria engineering journal, 54(4): 1115-1126. https://doi.org/10.1016/j.aej.2015.07.011

[3] Bernardinia, C., Asgharb, M.R., Crispoc, B. (2017). Department of Computer Science, Aalto University, Finland Department of Computer Science, The University of Auckland, New Zealand Department of Computer Science, KU Leuven, Belgium Department of Information Engineering and Computer Science, University of Trento, Italy, Security and privacy in vehicular communications: Challenges and opportunities.

[4] Juneja, R., Sharma, M. (2014). A Study of Vanet Security Issues and Protocols, IJR 1(8).

[5] Qu, F., Wu, Z., Wang, F.Y., Cho, W. (2015). A security and privacy review of VANETs. IEEE Transactions on Intelligent Transportation Systems, 16(6): 2985-2996. https://doi.org/10.1109/TITS.2015.2439292

[6] Hasrouny, H., Samhat, A. E., Bassil, C., Laouiti, A. (2017). VANet security challenges and solutions: A survey. Vehicular Communications, 7: 7-20. https://doi.org/10.1016/j.vehcom.2017.01.002

[7] Shafiq, H., Rehman, R.A., Kim, B.S. (2018). Services and security threats in SDN based VANETs: A survey. Wireless Communications and Mobile Computing, 8631851. https://doi.org/10.1155/2018/8631851

[8] Mejri, M.N., Ben-Othman, J., Hamdi, M. (2014). Survey on VANET security challenges and possible cryptographic solutions. Vehicular Communications, 1(2): 53-66. https://doi.org/10.1016/j.vehcom.2014.05.001

[9] Al Junaid, M.A.H., Syed, A.A., Warip, M.N.M., Azir, K. N.F.K., Romli, N.H. (2018). Classification of security attacks in VANET: a review of requirements and perspectives. In MATEC Web of Conferences, 150: 06038. https://doi.org/10.1051/matecconf/201815006038

[10] Rawat, A., Sharma, S., Sushil, R. (2012). VANET: Security attacks and its possible solutions. Journal of Information and Operations Management, 3(1): 301-304.

[11] Bhattacharya, M., Mantri, M., Maity, M. (2015). Application areas, Security Issues, Attacks and layer wise solutions of Vehicular Ad Hoc Networks (VANET). International Journal of Advance Research and Innovative Ideas in Education, 1(4): 2395-4396. https://doi.org/16.0415/IJARIIE-1304

[12] Rehman, S., Khan, M. A., Zia, T. A., & Zheng, L. (2013). Vehicular ad-hoc networks (VANETs)-an overview and challenges. Journal of Wireless Networking and Communications, 3(3): 29-38. https://doi.org/10.5923/j.jwnc.20130303.02

[13] Dhamgaye, A., Chavhan, N. (2013). Survey on security challenges in VANET. International Journal of Computer Science and Network, 2(1).

[14] Mansour, M.B., Salama, C., Mohamed, H.K., Hammad, S.A. (2018). VANET security and privacy-An overview. International Journal of Network Security & Its Applications, 10(2): 1-22. https://dx.doi.org/10.2139/ssrn.3290553

[15] Samara, G., Al-Raba'nah, Y. (2017). Security issues in vehicular ad hoc networks (VANET): A survey. arXiv preprint arXiv:1712.04263.

[16] Balta, M., Ovaz, K., Ozcelik, I. (2015). Faculty of Computer and Information Sciences, Department of Computer Engineering Sakarya University, Turkey, VANET Security Review: Application Side, M.BALTA et al./ ISITES-2015 Valencia -Spain.

[17] De Fuentes, J.M., González-Tablas, A.I., Ribagorda, A. (2011). Overview of security issues in vehicular ad-hoc networks. In Handbook of research on mobility and computing: Evolving technologies and ubiquitous impacts, 4(7): 894-911. https://doi.org/10.1049/iet-com.2009.0191

[18] Balasubramani, S., Rani, S.K., Rajeswari, K.S. (2016). Review on Security Attacks and Mechanism in VANET and MANET. Artificial Intelligence and Evolutionary Computations in Engineering Systems, 655-666. https://doi.org/10.1007/978-81-322-2656-7_60

[19] Kerrache, C.A., Lakas, A., Lagraa, N., Barka, E. (2018). UAV-assisted technique for the detection of malicious and selfish nodes in VANETs. Vehicular Communications, 11: 1-11. https://doi.org/10.1016/j.vehcom.2017.12.001

[20] Rehman, S., Khan, M. A., Zia, T. A., & Zheng, L. (2013). Vehicular ad-hoc networks (VANETs)-an overview and challenges. Journal of Wireless Networking and Communications, 3(3): 29-38. https://doi.org/10.5923/j.jwnc.20130303.02