Analysis of Possible Security Attacks and Security Challenges Facing Vehicular-Ad Hoc Networks

Ibraheem Abdelazeem Ibraheem, Weibin Zhang*, Abdeldime M.S. Abdelgader and Feng Shu

***Abstract*—Vehicular Ad-Hoc Network (VANET) is a technology that has been recently designed as one of the emerging future communications systems, a critical specialist used to support Intelligent Transportation Systems (ITS) by implementing a wide range of automotive applications and services. The primary objectives of VANET are to improve road safety and driving conditions. In addition, it supply many services including toll payment services, navigation, warning messages, congestion avoidance, alarm signals, and convenient internet access. The vehicle networks facing many different challenges and attacks due to lack of permanent infrastructure and high mobility. To maintain the network carefully against attackers, the security design of VANET must ensure integrity, authentication and confidentiality services. Moreover, as that network is very dynamic, making it a unique type of network, it is important to consider how this affects network security. Hence, this paper discusses the components and characteristics of vehicular networks. It has also presents survey of security challenges facing vehicle networks and security requirements. Moreover, it summarizes and analyses the possible attacks and a set of security weaknesses exist in VANET.**

I. Introduction

Vehicular Ad-Hoc network (VANET) is a technology that combines the capabilities of new wireless networks with vehicles [1]. VANET creates a strong network between moving vehicles and roadside units(RSU) [2], [3], [4]. It is a type of mobile Ad-Hoc networks (MANETs) that establishe communication between adjacent vehicles and nearby fixed devices, which is generally described as a side by (RSU)[5]. VANET can makes an important connection between the dynamic node by using different network equipment such as the IEEE 802.11 b / g wife, WiMAX IEEE 802.10, bucktooth and IRA[6].

The idea of the network is designed to provide a wide range of applications proposed by the group of engineers from (Delphi Delco) Electronics and IBM in 1998 [2], [3]. With the development in wireless communications technology, the concept of network vehicles has attracted interests all over the world. The goal of VANET is to allow communication between vehicles, and access to acceptable road safety and transport sector management. VANET connections are also subject to much faster fermentation, multi-path delay propagation and more Doppler frequency propagation than other wireless systems. Applications supported by VANET includes life safety applications, safety warning applications, electronic fee packages, internet access, group communications, and online service finders [7], [8].

In recent years, many new projects has been started and targeted to realize the dream of car networks and effective implementation of vehicle networks[5]. The vehicles are connected to each other (V2V) or with the Road Side Unit (V2R) by single hop or multiple protocols over the vehicle network of the contract. The probe is a small, low-cost, low-power device capable of sensing the environment, distributing data, and wirelessly communicating with certain base stations or end users. These contacts are qualified for various applications to enhance road safety and effective transportation [9], [10], [11].

Since VANET is a technology that create a mobile network, it converts every contributing moving cars as nodes in a network to the car into a wireless router or node, permits cars approximately 100 to 300 meters of each other to connect therefore, introducing a wide-ranging network. As vehicles

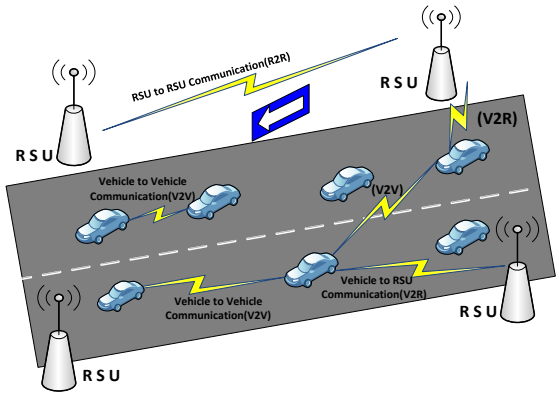

Fig. 1: VANET Components

Manuscript received June 12, 2019; revised July 14, 2019.

Ibraheem Abdelazeem Ibraheem, Weibin Zhang and Feng Shu are with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing 210094 e-mail:ibrahem2k19@gmail.com, Weibin email:13829668@qq.com.

Abdeldime M.S. Abdelgader is with Karary University, Khartoum, 12304, Sudan. Email: abdeldime@hotmail.com

step aside of the signal range and fall off the network, other vehicles can link in, connecting vehicles to one another consequently generates mobile internet [12]. The (RSU) is tasked as a router between vehicles on the road and linked to other network devices [6]. Each vehicle can connect with other cars using the Dedicated Short Range Communication (DSRC) short radio signals (5.9 GHz), and can reach the range of one kilometer. This connection is a dedicated connection, that meaning each connected node can move generously, without the dial to the wires. Each vehicle has an onboard unit (OBU), and this unit links the car with the RSU by DSRC radios, and another device called Tamper Proof Device (TPD) , wich is a device that fields the vehicle confidences, all the information about the vehicle like keys, drivers identity, trip details, speed, and rout.

The Intelligent Transport System (ITS) supported the operation of information exchange in dedicated networks around the vehicle from V2V or with its proximity to the base station (RSU). The nature of the open access medium in VANET makes it vulnerable to many attacks. However, security is the significant requirement in VANET [13], [14], [15]. To fortification VANET parts from attacks with methods such as denial of service attacks (DOS), many insurance methods are proposed. There are many Constraints in VANET they are listed in the following points.

- **Security Requirements**
  Make sure that the authorized user creates the connection. Denial of service attack (DOS) can cause the network to be dropped. Failure to report indicates that the nodes cannot be undone because the user does not forward a message, choosing the correct sequence is necessary, and it is requisite to complete structured data to eliminate counterfeit messages [9].
- **Attacks in VANET**
  Tapping is a public attack on secrecy, and routing attacks are attacks that destroy the network layer routing protocol node vulnerability to hijack a session only after the connection is established. Usually, the driver himself is the owner of the vehicle, so obtaining the owner's identity can threaten privacy [13].
- **Attackers on VANET**
  Predictable attacks are characterized by their unique and passive use: Active attackers create signals or packets while passive attackers perceive the network only, wicked and rational malicious attackers have no personal advantage after the attack, they damage the network operation . Inside and Out: Insiders are real members of the system while outsiders are hackers, thus an incomplete number of attacks [14].
- **Technical Problem**
  It is difficult to manage the network and control overcrowding in the network, in VANET electromagnetic waves are used to communicate, and this environment is affected [15]. As network topology and channel condition change rapidly, and due to high transportability, the environmental impact must be taken into account in VANET.

This paper presented the components and characteristics of vehicular network and discussed the security challenges facing vehicle network that raise many problems and provided comprehensive information on VANET various security requirements. In addition to detailing security requirements and potential attacks and classifying them. The rest of the paper is organized as.
Section II represents structure and characteristics of VANET. The VANET security requirements are presented in section III. Section IV summarizes the different attack classifications on VANET. Finally, section V concludes the paper and future direction of the action plan.

II. Structure and Characteristics of VANET

A. Component of VANET

VANET is a self-organization wireless network, hence the building of vehicular ad hoc network included several hardware and software components. In this section, the characteristics and environment under which vehicular network is designed are described. The user is the prime component of the vehicular network, and this network aims to avail and serve the right information around the road to the user [7]. VANET contains the following structures:

1) Vehicles
   Vehicles are the nodes of the vehicular networks. VANET produces the wireless communication between vehicles (V2V) and between vehicles and infrastructure arrival point (V2I).
2) Infrastructure
   Infrastructure in relation to the outside environments contains the roadside base stations. Which are the roadside units and they are situated at a devoted location like a cross or near parking spaces Their primary functions are to increase the communication zone of the ad hoc network by re-stretch the information to others and to work safety applications like low bridge warning, accident warning, etc .
3) Communication Channels
   Radio waves are the shape of electromagnetic radiation that plays an active role in protocol performance to limit the number of nodes within a single conflict range with wavelengths in the electromagnetic spectrum longer than the infrared light. Radio waves have frequencies of 190 GHz to 3 kHz [16].

B. VANET Characteristics

1) High Mobility and Rapidly Changing Network
   The vehicles move on the expressway at high velocity and change their position, instantly. It is challenging to presage the condition and therefore, produce privacy problems. Fast cars also make the network changeable. The VANET topology rely on the street infrastructure and parking, as displayed in figure 1, each vehicle is armed with a unit on board or OBU that connect with other OBU or RSU [17].

ISBN: 978-988-14048-7-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

2) Unbounded Network Size
Network size in VANET has no geographical limit, it can consist of towns, cities, or even countries. Information exchange in this quick network is much repeated because it gets signals from other vehicles as well as RSUs [2]. Careful and timely transferred information can only minimize the hazard on the road. VANET supplies such standards enabling a driver to get information on time and avert accidents [18].

3) Wireless Communication
Nodes are wirelessly connected and exchange their information

4) High Computability Ability
The computational capacity of the node is increased, due to computational funds and sensors [16].

5) Hard Delay Constraints
Safety messages are the aim of VANET. Therefore, safety messages should be given high priority and must be transferred on time [19].

The above unique characteristics breed new challenges that need to be resolved in the vehicular network environments. The main problems of the vehicular network can be abbreviated, as follows:

- The signal strength difference received causes an intermittent connection.
- High mobility causes repeated neighborhood fluctuation.
- Hidden or exposed peripheral problems occur as a concern of packet loss.
- Mounting channel load (High-intensity environment).

To solve these problems, a number of efforts have been made. The literature contains a significant amount of studies classifying these challenges in all parts. The studies research to address all layers related issues ranging from lower layers (physical and MAC layers) enhancement to upper layers application developments.

III. SECURITY REQUIREMENTS FOR VANET

In VANET, security is required as VANET packets hold dangerous life information and it is fundamental that these packets must come to the drivers without any modification or admission of data. Similarly, the accountability of drivers should also be recognized [9]. That they notify the traffic setting appropriately and within time. However, VANET must content following security requirements.

- **Availability**
Vehicular networks will provide requisite real-time for many purposes so they must be available all the time. These applications need an immediate reaction from sensor networks or Ad-Hoc if there is some delay in seconds for different forms network, the annihilation of the result can occur,or the message can become in utile [16].
- **Authentication**
Authentication includes the process of checking the transmitter identity, and setting if he has the rights to connect through the network, meaning to be able to send and receive messages through the network VANET, It is important that the data which propagates in the organism must be correct and created by an authentic client because in VANET nodes respond access, to the data established from the other end [7], [11].

- **Privacy**
Personal information about vehicles and drivers must be safe and confined such as real identity, destination, and speed from unauthorized access [8]. The requirement of privacy is necessary in group communications, as this security requirement is the warranty that data will only be read by confirmed users where hardly group members are unable to understand such data.

- **Integrity**
All messages that are sent and received through the network must be secure against modification attacks in order, to trust messages contents. In a vehicular network, data integrity is one of the most critical security aims, and it must be maintained while communicating $V2V$ or vehicle to roadside unit $V2R$ [11]. Message content should not be modified during it goes from sender to receiver, if the source is an authentic user of the network but message contents has been changed then there is no necessity to check the authenticity of the source user. The message meaning is very vital while connecting in safety and no safety applications of the vehicular network.

- **Non-Repudiation (NR)**
Particular authority is assured for sender identification, the vehicle could be specified from the documented messages it sends. In this security based system, a sender can be set easily. This averts deception from rejecting their crimes because even if the attack happens, (NR) will smooth the ability to observe the attacker[18].

IV. CATEGORIZE ATTACKS AND THREATS:

Attacks on VANET impact in his modality, to cure with these attacks, many researchers classify these attacks [18], it can be in general classified into three major groups, those that pose a threat to availability, a threat to authenticity, a threat to driver confidentiality, and diversity. Confidentiality, integrity and availability (CIA) are the main modules of security aims. The increasing research attention, potential applications, and security problem in VANET prime to the requirements to appraise the attacks on security goals. This section, as shown in Figure 2 presents the survey of attacks on security objectives and labels in particulars the nature of attacks and the behavior of attackers through different scenarios in the network [9].

It is requisite to classify the VANET threats because it has a unique nature outcome, in unique vulnerabilities and several types of attacks that entail important computing. Researchers classified these attacks with different classifications, such as

ISBN: 978-988-14048-7-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

TABLE I: Classifications of Attacks.

Attack Name	Attack Type	Attack Effects
Timing Attack	Insider Attack, malicious	Integrity
Man-in-the-Middle	Insider Attack	Confidentiality, Privacy, and Integrity
Bogus Information	Insider Attack	Authentication
Black Hole	Outsider, passive Attack	Availability
Malware	Insider Attack, malicious	Availability
Monitoring Attack	Monitors Road Activity	Authenticity and Privacy
Sybil Attack	Insider, network Attack	Authentication and Privacy
Spamming	Insider Attack, malicious	Availability
Wormhole/Tunneling	Outsider, malicious, monitoring Attack	Authentication and Confidentiality
Dos	Malicious, active, insider, network Attack	Availability

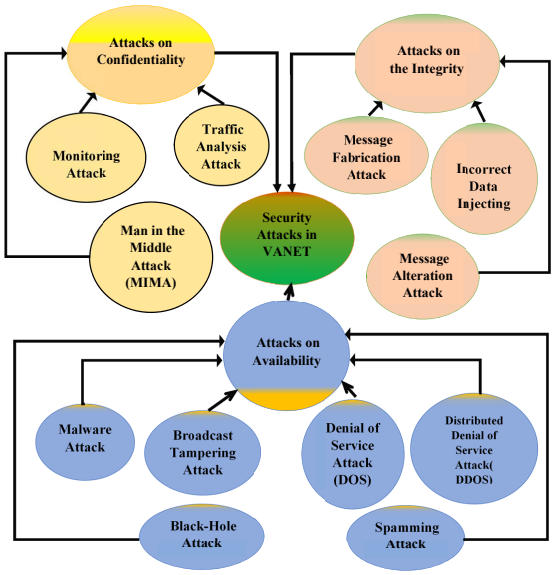

Fig. 2: Possible Attacks on Security Requirements

in [19]. Categorized attacks there are treated to requirements VANET (authenticity, confidentiality,and availability). While researchers in [20]. Categorized attackers into three classes: Selfish Driver, malicious attacker, and pranksters. Also, there are different calcification suggested by researchers in [21]. They distributed attacks as Network Attack NA,Social attack (SA), monitoring aAttack (MA), timing attack (TA), social attack (SA), and application attack. Another classification indicated in [22]. Attacks were described in three categories: Active vs Passive, insider vs outsider, and malicious. Rational vs Each category defines different types of attacks. In this section, we discuss some of these attacks.

A. *Attacks on Confidentiality*

One of the important issues for vehicle users is not to disclose the identity and privacy of the site, which includes blocking the exact location in time and space to protect the users by hiding the request of the user and it cannot be distinguished from the requests of other users [19]. Another part of confidentiality is to analyze the traffic flow from $V2V$ or from vehicle to RSU communication, in which attackers are just saved and monitored on the communication between vehicles and the needed information is collected. Possible attacks concerning to confidentiality are offered, below through different scenarios [8].

1) Monitoring Attack: In this form of attack, the total network is checked, and the attacker listens to all communications in the $V2V$ and the car to a roadside unit $(V2R)$ [23]. When any data relevant to its needs are heard, this data is directed to the person mind. For instance, in the case of a policy process, the police planned an operation against a certain criminal in a specific area. To transport the process, the police must connect with each other to pass details, such as precise location and run time. The attackers snoop on all communications and inform the criminals about the next police operation.

2) Traffic Analysis Attack: This attack is considered to be a severe level hazard against the privacy of the user in VANET, the attacker make analyses on the traffic packets between the $V2V$ or $V2R$ [23], and uses these packets which contains position, Vehicle ID, and the traveling path of the car which may be helpful to read out the wanted information

ISBN: 978-988-14048-7-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

for its desired objective.

3) Man in the Middle Attack $(MIMA)$: In the MIMA the attacker is after listening to the contact between the vehicles and carries out the wrong or changed message insertion between vehicles. Valid vehicles think they are directly connected with each other and that the attacker protests traffic and controls all communication between them [13], [24].

B. Attacks on the Integrity

The integrity of communication guarantee that the message is not changed in transit and that the messages the driver receives are not deceptive [25]. In a vehicular networks, data integrity is one of the key security goals, and it must be looked after while communicating $V2V$ or vehicle to RSU $V2R$. If the source is the original user of the system but message contents are varied then there is no requirement to check the authenticity of the source user. Message content is very significant while communicating in safety and no safety requests of the vehicular network [10], [19]. Potential safety related attacks are listed below.

1) Message Alteration Attack: This type of attack contains both modifying the authentic content of messages and sent data, delaying the transmission of information messages, or repeating messages previously transmitted [13].

2) Message Fabrication Attack: Here, attackers transmit false data in a network, these kinds of attacks begin by selfish drivers. They manufacture messages using propagation methods and then initiate an attack by sending these messages to the network it can be fabricated in two forms [19]. In order to be competent to drive more quickly, the attacker (the selfish driver) appears to be an emergency car. The other option is that untrue information around the attacker's identity, speed and position are directed to other vehicles or RSU.

3) Incorrect Data Injecting Attack: In this attack, the attacker (E) controls communication by inserting other data into the true message from the vehicle (A) to vehicle (B) [7]. As the message moves to many nodes, the targets of the attack is to reach many leaps, affecting the other nodes of the malicious contract and to send the message back to others [25].

C. Attacks on Availability

The network must be available every time, vehicle networks aim to help users through their possible applications, but if the network is not available for communication, the major purpose of the network becomes unavailing. Attacks related to availability are displayed below in different scenarios [2], [7], [24].

1) Denial of Service Attack (DOS): In DOS the attack is one of the highest attacks in connection to the availability of the network [25]. Its target is to stop the original vehicles from accessing the networks services, and this is achieved by jamming the channel in the wireless environment, so that the attacker can benefit from the network, resources, the entire network and create problems sending high-frequency signals, which does not allow the vehicles to send and receive messages of peace or lack of safety on the network. In vehicular networks, DOS attack has three various forms [24].

- Channel communication division:
  Where the attacker benefits from the limited current limited capacity of the wave standard, thus interrupting the connection between vehicles.
- The attacker consumes the vehicles:
  Resources and therefore it is unable to perform other tasks because it is always preoccupied.
- The attacker can hinder the messages and drop it.

2) Distributed Denial of Service Attack: The Distributed Denial of Service(DDoS) attack is more severe than the DOS attack in a vehicle environment because the attack technicality is in a distributed fashion. In this issue attackers prefaced attacks from many places. may use different time periods to launch attacks [26]. The nature of the attack and the time slots of $V2V$ may vary for this particular attacker.

3) Malware Attack: In this event, attackers are usually malicious insiders before an outsider. Malware attacks are just like viruses as viruses in VANET obstruct the average employment of the network. When there are software updates in VANET elements or RSU VANET becomes infectious by these attacks frequently [27].

4) Black-Hole Attack: Here attack, the attackers car is a black hole in the net, they often create and break the connection by rejecting the multiple node redirection [24]. The black-hole attack is a different kind of attacks, and can be found in the vehicle networks in two different forms. One user starts communication with other users of the system and it is suddenly dropped out of the connection. And another case where other users refuse to share a new user or connect to the system [7].

5) Spamming Attack: To expend the bandwidth of network and to raise the transmission latency, the attacker sends spam messages in the network due to the rareness of needful infrastructure and centralized management. Controlling of this kind is difficult. In this attack, the attacker distributes spam messages to a group of users Those messages are of no concern to the user just like announcement messages [28].

6) Broadcast Tampering Attack: The nature of this attack is to reason road accidents or change the flow of traffic on some specific route [29]. Safety messages are transmitted in the network and inform other users about current safety conditions of any particular area. In this situation, an attacker

ISBN: 978-988-14048-7-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

plays with the broadcast safety message and probably inserts false safety messages.

The authors in [30]. Were inspected and discussed concerning VANET vulnerabilities where attacks were categorized into several categories. It has been noted that this classification depends on insiders, slander, strangers and surveillance attacks. This classification is summarized in the tableI.

V. CONCLUSION

This paper presented the components and characteristics of VANET, the security challenges it faced and provided comprehensive information on the various potential attacks and their classification. Vehicle networks are fertile ground for attackers who try to intercept the network with their malicious attacks. Security in VANET and the level of guaranteed implementation seriously affect the safety of persons and proprieties. Recently, many researchers examined security attacks and tried to find solutions. Others try to define security in the wireless connection nodes that are connected, and data is changed over wireless channels. Thus, the requirement for reliable connections. In order to make the development of VANET systems worth the effort, it must meet the various security requirements and conditions. In future work, many solutions can be propose that can improve the security of VANET by using the properties of the physical layer and the random wireless channels in the process of creating and distributing the encryption key.

ACKNOWLEDGMENT

This work is supported by the National Key R & D Program of China (No. 2018YFB1601101 of 2018YFB1601100).

REFERENCES

[1] P. Tyagi and D. Dembla, "Investigating the security threats in vehicular ad hoc networks (vanets): towards security engineering for safer on-road transportation," in *Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on*. IEEE, 2014, pp. 2084–2090.

[2] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE communications surveys & tutorials*, vol. 13, no. 4, pp. 584–616, 2011.

[3] R. Lind, R. Schumacher, R. Reger, R. Olney, H. Yen, M. Laur, and R. Freeman, "The network vehicle-a glimpse into the future of mobile multi-media," SAE Technical Paper, Tech. Rep., 1998.

[4] R. S. Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for vanet," *International Journal of Network Security & Its Applications*, vol. 5, no. 5, p. 95, 2013.

[5] J. Blum and A. Eskandarian, "The threat of intelligent collisions," *IT professional*, vol. 6, no. 1, pp. 24–29, 2004.

[6] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on vanet security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[7] I. A. Sumra, H. B. Hasbullah, and J.-l. B. AbManan, "Attacks on security goals (confidentiality, integrity, availability) in vanet: a survey," in *Vehicular Ad-Hoc Networks for Smart Cities*. Springer, 2015, pp. 51–61.

[8] M. Altayeb and I. Mahgoub, "A survey of vehicular ad hoc networks routing protocols," *International Journal of Innovation and Applied Studies*, vol. 3, no. 3, pp. 829–846, 2013.

[9] D. Chadha, "Reena,vehicular ad hoc network (vanets): A review,," *Int. J. Innov. Res. Comput. Commun. Eng*, vol. 3, no. 3, pp. 2339–2346, 2015.

[10] F. Hui, "A survey on the characterization of vehicular ad hoc networks routing solutions," in *ECS*, vol. 257, 2005, pp. 1–15.

[11] N. R. Siddiqui, K. A. Khaliq, and J. Pannek, "Vanet security analysis on the basis of attacks in authentication," in *Dynamics in Logistics*. Springer, 2017, pp. 491–502.

[12] Z. Y. Rawashdeh and S. M. Mahmud, "Communications in vehicular networks," *Mobile Ad-Hoc Networks: Applications, Cap*, vol. 2, pp. 20–40, 2011.

[13] J. M. De Fuentes, A. I. González-Tablas, and A. Ribagorda, "Overview of security issues in vehicular ad-hoc networks," in *Handbook of research on mobility and computing: Evolving technologies and ubiquitous impacts*. IGI Global, 2011, pp. 894–911.

[14] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of computer security*, vol. 15, no. 1, pp. 39–68, 2007.

[15] H. Moustafa and Y. Zhang, *Vehicular networks: techniques, standards, and applications*. Auerbach publications, 2009.

[16] I. Bhardwaj and S. Khara, "An analytic study of security solutions for vanet," *International Journal of Computer Applications*, vol. 132, no. 10, pp. 1–7, 2015.

[17] K. Plossl, T. Nowey, and C. Mletzko, "Towards a security architecture for vehicular ad hoc networks," in *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*. IEEE, 2006, pp. 8–pp.

[18] A. Kumar, M. Bansal *et al.*, "A review on vanet security attacks and their countermeasure," *Signal Processing, Computing and Control (ISPCC)*, vol. 2017, pp. 580–585, 2017.

[19] A. Rawat, S. Sharma, and R. Sushil, "Vanet: Security attacks and its possible solutions," *Journal of Information and Operations Management*, vol. 3, no. 1, p. 301, 2012.

[20] G. Samara, W. A. Al-Salihy, and R. Sures, "Security issues and challenges of vehicular ad hoc networks (vanet)," in *New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on*. IEEE, 2010, pp. 393–398.

[21] I. A. Sumra, H. Hasbullah, J. Lail, and M. Rehman, "Trust and trusted computing in vanet," *Computer Science Journal*, vol. 1, no. 1, 2011.

[22] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE wireless communications*, vol. 13, no. 5, 2006.

[23] R. Akalu, "Privacy, consent and vehicular ad hoc networks (vanets)," *Computer Law & Security Review*, vol. 34, no. 1, pp. 37–46, 2018.

[24] A. M. Abdelgader, F. Shu, W. Zhu, and K. Ayoub, "Security challenges and trends in vehicular communications," in *Systems, Process and Control (ICSPC), 2017 IEEE Conference on*. IEEE, 2017, pp. 105–110.

[25] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "Vanet security surveys," *Computer Communications*, vol. 44, pp. 1–13, 2014.

[26] H. Hasbullah, I. A. Soomro *et al.*, "Denial of service (dos) attack and its possible solutions in vanet," *World Academy of Science, Engineering and Technology, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering*, vol. 4, no. 5, pp. 813–817, 2010.

[27] F. Sabahi, "The security of vehicular adhoc networks," in *2011 Third International Conference on Computational Intelligence, Communication Systems and Networks*. IEEE, 2011, pp. 338–342.

[28] A. M. Malla and R. K. Sahu, "Security attacks with an effective solution for dos attacks in vanet," *International Journal of Computer Applications*, vol. 66, no. 22, 2013.

[29] H. Guo and G. Liu, "Research of security for vehicular ad hoc networks," in *Computer, Mechatronics, Control and Electronic Engineering (CMCE), 2010 International Conference on*, vol. 5. IEEE, 2010, pp. 144–147.

[30] P. Tyagi and D. Dembla, "Investigating the security threats in vehicular ad hoc networks (vanets): towards security engineering for safer on-road transportation," in *Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on*. IEEE, 2014, pp. 2084–2090.