International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 345-351 www.ijaem.net ISSN: 2395-5252

VANET Security Attack Services on Traffic Management: Survey

Haider K. Hoomod, Mohammed Mahdi
Mustansiriyah university- college of education- computer dept. Baghdad- Iraq

Submitted: 01-06-2022 Revised: 05-06-2022 Accepted: 08-06-2022

ABSTRACT: In the previous couple of years, various types of researchers concentrate on Vehicular Ad-hoc networks (VANET) field due to various facilities it provides. VANET a subgroup of mobile ad-hoc network (MANET), refers to a group of intelligent nodes i.e. (vehicles) on the road. These intelligent vehicles interact with one other or with the road side unit (RSU) for providing safer roads and a more efficient driving experience and providing security against attackers. In VANET messages are conveyed in an open wireless channels Security is therefore the most concerning issue in VANET. In this paper several types of the security issues, requirements, attacks, attackers in VANET have been described and some recent solutions to solve the security problems with their advantages and disadvantages have been discussed.

I. INTRODUCTION:

In today's digital environment, intelligent transportation systems (ITS) play a critical role in making residents' lives easier in every way possible. By reducing traffic congestion and mitigating unpleasant incidents, ITS attempts to improve traffic efficiency. In terms of providing road and traffic safety, reducing traffic congestion and enhancing traffic flow, and delivering entertainment services on vehicles, ITS provides ubiquitous and robust services. [1]. The automotive sector recognizes the importance of connecting vehicles to IT systems; for example, vehicle communication improves traffic safety and streamlines traffic flow [2]. It is carried out to satisfy the demands and to broaden the recognition event of cars, which sensors cannot do [2]. The elements of traffic flow, driver behavior, and driving conditions can all be recognized and communicated with nearby vehicles. Vehicular ad hoc networks (VANETs) have been established to share this information and improve the efficiency of vehicle communication [3].(vanet) have been introduced [3].

The goal of the ITS is to improve traffic flow and provide traffic safety. The registration method, roadside units (RSUs), and onboard units (OBUs) are all used in VANET, which is a kind of MANET with road routes [4]. The OBUs are the radios that are installed in every car as a transmitter to communicate with other vehicles, and the RSUs are the network devices that are installed along the street. RSUs are used to communicate with infrastructure and to house dedicated short-range communication (DSRC) network devices [5]. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications are the two types of VANETs [6].

II. BASIC OVERVIEW OF VANETS

VANETs, which are ad hoc network infrastructures in which vehicles are connected by wireless communication, have been rapidly growing since 1980 [7]. VANETs have recently been employed to improve traffic safety, improve traffic flow, reduce traffic congestion, and provide driver guidance [8].

the VANETs basic model diagram, illustrating how vehicle communication can be divided into V2V and V2I communication, road side units (RSUs), and onboard units (OBUs). We'll go through these factors first, then describe the unique qualities and benefits of VANETs over MANETs in terms of network structure, bandwidth, and dependability, among other things. As previously stated, VANETs are made up of three components: OBUs, RSUs, and trusted authority (TA); these factors are addressed more below.

2.1. Architecture of a VANET. In most cases, automobiles and RSUs communicate via wireless technology, which is referred to as wireless access in the vehicular context (WAVE).

The WAVE architecture specifies how security messages are sent [1], and WAVE communication assures passenger safety by updating vehicle information and traffic flow. This application

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 345-351 www.ijaem.net ISSN: 2395-5252

increases the traffic flow and efficiency of the traffic management system while also ensuring pedestrian and driver safety. the VANETs are made up of several components such as OBUs, RSUs, and TAs. The RSU often houses an application that allows it to interface with other network devices, whereas the OBU is put on each vehicle and collects data such as speed, acceleration, and fuel consumption. These data are relayed to neighboring vehicles in then. These data are forwarded to the nearby vehicles through wireless

2.2. Interaction In VANETs: there are a variety of methods. ITS is dedicated to providing secure communication in order to improve traffic flow and road safety while also overcoming obstacles. Different networking solutions, such as MANETs and VANETs, can be used to alleviate traffic congestion. In the ITS, V2X communications play a critical role. help make traffic more efficient, safer, and easier to drive by providing real-time and highly trustworthy information such as collision warnings, road bottlenecks, traffic congestion warnings, and emergency circumstances, users can have better experiences.
with other modes of conveyance [9]. Communication between two devices (V2X) as indicated in Figure 1, information can be exchanged between V2V, V2I, and vehicle to pedestrians (V2P). The transmission medium in V2V communication is the transmission rate is high, and the latency is short.

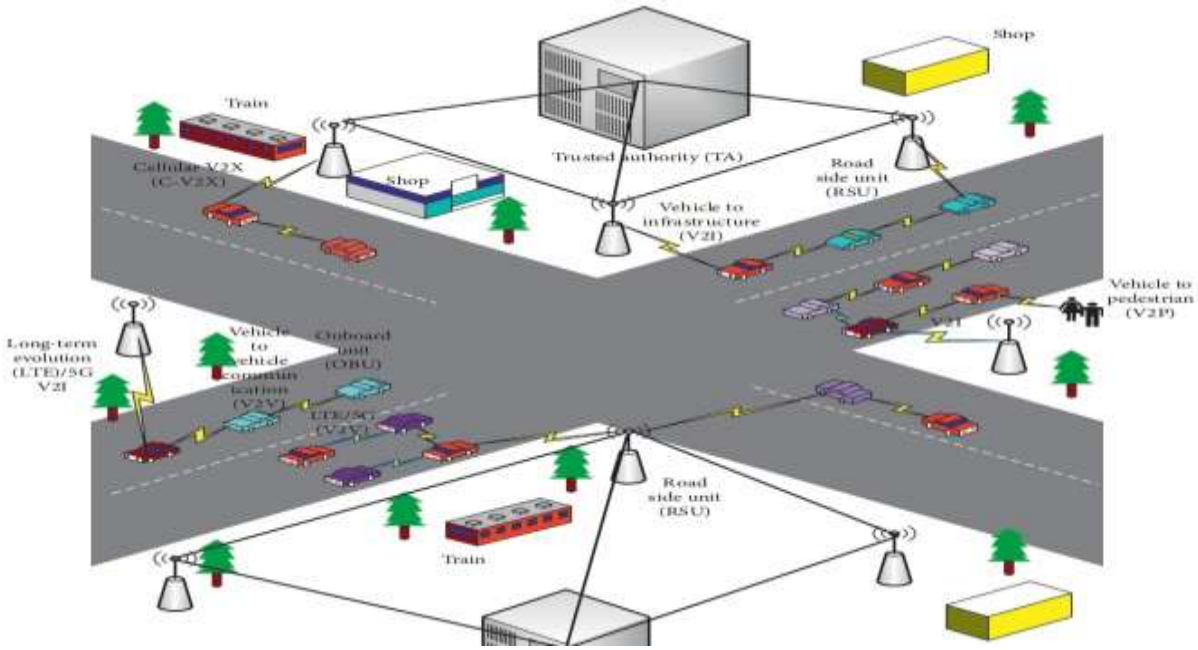

Figure 1: VANET model diagram

2.3. Standards for the VANET: The VANET communication protocol specifies the complete set of requirements for implementing this policy. The VANET standardization has an impact on all layers of the open system interconnection (OSI) model, which is utilized as a communication tool and comprises all of the layers' necessary capabilities.
[10]. dedicated short-range communication (DSRC) ,WAVE stands for wireless access in a vehicle environment, and IEEE stands for The comprehensive standard of communication protocol for dealing with VANETs is designated as 802.11p.

III. VANET SECURITY AND CHALLENGES

MANETs have recently introduced a new security threat that is viewed as a critical issue for researchers to address, such as a lack of central points, mobility, poor wireless connectivity, and driver issues [45]. VANET security ensures that intruders do not inject or change the sent messages. In addition, the driver is accountable for accurately conveying the traffic conditions within the time constraints. Because of their unique qualities, VANETs are more vulnerable to attacks. Security concerns, in particular, must be adequately

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 345-351 www.ijaem.net ISSN: 2395-5252

handled; otherwise, secure communication in VANETs will be severely limited [4].

In terms of VANET security, it is vital to state that the system must be in compliance with the acceptable network operation. Failure to meet these conditions could result in a potential threat or attack in VANETs. The five major security domains are availability, secrecy, authenticity, data integrity, and nonrepudiation [2, 26]. depicts the security services, as well as the dangers and attacks that they face, which will be described in more detail in the coming sections.

3.1. **Availability**: Availability is the most important aspect of security services that needs to be addressed because it is linked to all safety applications. The main responsibility of availability is to manage functionality, and its security must ensure that the network and other applications continue to function in the event of a failure or malicious attack [12]. If VANETs are more vulnerable to attacks, then availability is more important than any other security factor [13].

3.2. Confidentiality. Confidentiality ensures that only the designated receiver has access to the data, while outside nodes may not be able to access the data until the secret data has been received by the designated user.

3.3. Authentication. In VANETs, authentication is critical. It protects VANETs from potential threats in the network. It is critical to contain the necessary transmission mode information, such as user identification and sender address. Authentication provides the authority to govern vehicle permission levels and can also protect against Sybil attacks by assigning a unique identity to each vehicle [11].

3.4. Integrity of data. It ensures that the message's content isn't tampered with during transmission. It can be ensured in VANETs by leveraging public key infrastructure and the cryptography revocation process [14].

3.5 Nonrepudiation. It assures that the sender and receiver of the message do not refuse to engage in transmission and reception in the event of a disagreement [29, 15].

IV. SECURITY ATTACKS AND THREATS IN VANETS

We'll talk about the attacks and threats in this part .service of security .

4.1. Availability on Availability. The availability of information is a critical component of the VANET system, and its absence may result in a decline in the efficiency of VANETs [15]. We'll go over the dangers and assaults in VANETs in this part.

(i) DOS (Distributed Denial-of-Service) Attacks DOS is one of the most common attacks in VANETs, and it's produced by internal or external vehicles attacking the network [13]. The +e attacker disrupts vehicle communication, effectively blocking all options for action. +A distributed denial of service (DDoS) assault can be carried out by a large number of attackers at the same time [26].

(ii) Attack of the Jamming. In this assault, the attacker uses a high-powered signal with an equivalent frequency to disrupt the communication channel in VANETs [27]. Because it did not follow the proper safety notice, this is the most serious attack for safety applications. In any effective jamming attempt, the jammer can jam the valuable signal by taking an action at the same time as the occurrence of an event.

(iii) Malware Attack. Through the software components that operate the OBUs and RSUs, the attack can be penetrated into the VANET system [16, 17]. If a malware assault occurs in VANETs, the other components of the VANET system will malfunction.

(iv) Broadcast tampering is a type of cyber-attack. Untrustworthy vehicles can reproduce the same messages in the VANETs by changing the message or by generating and inserting a new message while acting as a transmit node for inter vehicle communication in this assault [18]. As a result, the correct safety signals may be hidden from dedicated users, potentially resulting in dangerous mishaps.

(v) Blackhole Attack This is the principal threat that attacks ad hoc network availability and also exists in VANETs. A registered VANET user is usually the source of this assault. Although the suspected node gets packets from the network, it refuses to participate in the networking process. Due to the malicious node, which claims to contribute to the nonpractical event, this may disturb the routing table and prevent the crucial message from reaching its intended recipients [1, 13,29].

(vi) Grayhole Attack It's a type of blackhole attack in which untrustworthy vehicles pick and choose which data packets to forward while dropping the others without being traced. [19].

(vii) Greedy Behavior Attack. This attack usually targets the message authentication code (MAC) capability, in which the malicious

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 345-351 www.ijaem.net ISSN: 2395-5252

vehicle abuses the MAC protocol to consume a huge amount of bandwidth at the expense of other users. This resulted in an overflow of traffic and a collision on the transmission channel, causing delays in the registered user's legitimate services [20].

(viii) Spamming Attack. The attacker introduced a large number of spam messages, such as advertisements, into the VANET system, causing a collision by consuming additional bandwidth [13, 21].

4.2. Attack on Confidentiality in VANETs .Invasion of VANET Confidentiality Confidentiality assurances can be encrypted using certificates and sharing public keys for all exchange messages, with only designated vehicles having access. As a result, vehicles outside of the nodes are unable to grasp private and secret information shared among the vehicles. The cryptographic solutions ensure that information is kept private. The following are some of the most typical challenges to secrecy that will be explored in this section:

(i) Eavesdropping Attack. Attack on Eavesdropping In wireless communication technology, such as MANETs and VANETs, eavesdropping is fairly frequent. the The goal of this attack is to extract confidential data from protected data. As a result of this attack, nonregistered users may be exposed to sensitive information such as user identification and data location that might be used to track vehicles.

(ii) Traffic Analysis Attack. One of the most hazardous assaults that threatens secrecy is the Traffic Analysis Attack. After listening to the message transmission, the attacker examines its frequency and attempts to extract and acquire as much relevant information as possible.

(iii) Attack on the Man-in-the-Middle. This attack occurs in the middle of a V2V transmission to inspect and change the messages. The attacker has access to and control over the full V2V communication, yet the communication entities believe they can interact privately with each other [22].

(iv) Social Attack: This tactic is meant to divert the driver's focus away from the road. The attacker sends the drivers messages that are immoral and unethical. the attackers' goal is to see how drivers respond after receiving such immoral messages, so impacting the driving experience and vehicle performance in the VANET system [30]. Social Attack: This tactic is meant to divert the driver's focus away from the road. The attacker gives the drivers messages that are immoral and unethical. The attackers' goal is to see how drivers respond after receiving such immoral messages, so impacting the driving experience and vehicle performance in the VANET system [30].

4.3. Attack on Authentication in VANETs Attack on Authentication in VANETs. Authentication is a term used to describe the process of verifying a crucial component of the VANET system that protects against assaults caused by rogue nodes accessing the network. VANETs are protected from both internal and external assaults through authentication [31].

(i) Attack of Sybil [32] was the first to mention the Sybil attack. This is the most deadly attack, in which the 'node' contains numerous phony identities and broadcasts various messages to disrupt the VANETs' normal functioning. Other vehicle behaviors can be manipulated by the attacker, and the recipient vehicle believes the signals are coming from multiple vehicles. As a result, they may believe there is traffic on the road, so they were forced to change their routes and leave the road clean.

(ii) An attack on the tunnels. The wormhole assault [13] is comparable to this technique. The attacker utilizes the same network to start the secret chat, and he used an extra communication channel called tunnel to connect two VANETs that were far apart. As a result, even the farthest nodes can communicate as neighbors .There is no traffic on the road.

(iii) GPS spoofing is a method of deceiving GPS receivers The position and location of the node are critical in the VANET, and they must be precise and legitimate. The log file, which contains the GPS satellite's location table, is kept. In this attack, the attacker used a method to fabricate bogus GPS location information and did not reveal the true location in order to avoid vehicles thinking it was available somewhere else [33].

(iv) Node Impersonation Attack: This attack is carried out by obtaining the user's legitimate ID and transferring it to another authorized user on the VANETs [28].

(v) Free-Riding Attack. This attack is fairly prevalent, and it's started by a rogue user who makes fraudulent authentication attempts while using cooperative messaging authentication. In this type of attack, the malicious user takes advantage of other users' authentication

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 345-351 www.ijaem.net ISSN: 2395-5252

contributions without providing its own, which is referred to as a freeriding attack. This exploit could put cooperative message authentication in jeopardy [35].

(vi) Replay Attack. Replay Attack. This attack, also known as a playback attack, happens when genuine data is fraudulently transferred or causes a delay in order to produce an unauthorized and malevolent impact. To counter this attack, the VANET will need enough time sources with higher cache memory, which will be used to compare received messages.

4.4. Attack on Data Integrity in VANETs .Data Integrity Attack in VANETs. In this section, we'll go through some of the most common risks to integrity, which are listed below:

(i) Masquerading is a type of attack that disguises itself as something else. By using registered user IDs and passwords, the attacker gains access to the VANET system and attempts to broadcast fraudulent messages that appear to emanate from the registered node [36].

(ii) Replay Attack. The attacker's goal is to falsely repeat or delay transmissions by using genuine data and continuously inject beacon messages that were previously received on VANETs, making it impossible for traffic authorities to identify vehicles in the event of an emergency [36, 37].

(iii) Message Tampering Attack . As the name implies, this attack happens when an attacker updates or alters recent message data that is about to be broadcast [38]. For example, if the route is congested, the attacker modifies the data to clear the road, causing users to change their driving plans.

(iv) Illusion Attack. This exploit collected malicious data from sensors and received data from antennas to construct traffic warning signals based on the current road state, which may deceive surrounding motorists [39]. Vehicle accidents and traffic congestion can trigger illusion attacks, which reduce the performance of the VANET system by consuming unwanted bandwidth.

4.5. Attack on Nonrepudiation: It assures that in the event of a disagreement, the sender and recipient of communications cannot deny the transmitted and received messages.

(i) Repudiation Attack. In the event of a dispute, this assault happens when an attacker denies partaking in the action of sending and receiving communications [22].

All security attacks in VANETs are summarized in Table 1. It pinpointed each attack, as well as any compromised security services and potential responses.

Attack	Compromised services	Countermeasures
DOS	Availability, authentication	Use the bit commitment and signature-based authentication technique
Jamming	Availability	Use frequency hopping technique, direct-sequence spread spectrum (DSSS)
Malware	Availability	Reliable hardware and digital signature of software
Broadcast tampering	Availability, integrity	Cryptographic primitives are enabled for prevention, but a nonrepudiation mechanism may exist
Blackhole, grayhole	Availability	Reliable hardware and digital signature of software
Greedy behavior	Availability	Use intrusion detection systems (IDSs)
Spamming	Availability, confidentiality	Reliable hardware and digital signature of software
Eavesdropping	Confidentiality, integrity	Exploit physical layer security protocols
Traffic analysis	Confidentiality	Use encryption techniques
Man-in-the-middle	Authentication, confidentiality, integrity	Robust authentication technique such as digital certificates
Social	Confidentiality	Use digital signatures
Sybil	Availability, authentication	Deployment of central validation authority (VA), location and position verification, and efficient allocation of transmission resources.
Tunneling	Integrity	Reliable hardware and digital signature of software and sensors
GPS spoofing	Authentication	Signature-based authentication technique with positioning system and the usage of bit commitment
Free-riding	Authentication	Use strong authentication technique
Key and/or certificate replication	Confidentiality, authentication	Use certified keys, and check the validity of certificates in real time through CRL
Message tampering	Availability, authentication	Zero-knowledge schemes for authenticate message
Masquerading	Authentication, nonrepudiation, integrity	Digital signature of software, and trusted and reliable hardware which makes impossible to change protocols
Replay	Authentication, integrity, nonrepudiation	Message authentication, using digital signature scheme
Illusion	Authentication, integrity	Software must be handled by authorized entity, sensors operation must be authenticated, and use the plausibility validation network (PVN)
Repudiation	Nonrepudiation	Identity-based signature and ID-based online/offline (IBOOS) techniques with complex managing certificates may exist

V. CONCLUSION:

This paper constitutes a comprehensive review of VANET security, after discussing characteristics, applications. Then threats or attacks to VANET and solutions to these security problems were introduced. In addition to this some issues in security such as requirements of security, attacker profiles and attacks has been pointed out and certain solution with advantages and disadvantages are highlighted.

REFERENCE

[1]. M. Nidhal, 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.

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

[3]. S. Biswas, J. Miˇsic, and V. Mi ´ ˇsic, "DDoS attack on WAVE- enabled VANET through synchronization," in Proceedings of the IEEE Global Communications Conference (GLOBECOM),pp. 1079–1084, Anaheim, CA, USA, 2012.

[4]. H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: a survey," Vehicular Communications, vol. 7, pp. 7–20, 2017.

[5]. M. Smita and N. Pathak, "Secured communication in real time VANET," in Proceedings of the International Conference on Emerging Trends in Engineering and Technology (ICETET), pp. 1151–1155, Nagpur, India, 2009.

[6]. A. Dua, N. Kumar, and S. Bawa, "A systematic review on routing protocols for vehicular ad hoc networks," Vehicular Communications, vol. 1, no. 1, pp. 33–52, 2014.

[7]. A. Stampoulis and Z. Chai, "A survey of security in vehicular networks," Project CPSC, vol. 534, 2007.

[8]. G. Jyoti and M. S. Gaur, Security of Self-Organizing Networks MANET, WSN, WMN, VANET, CRC Press, London,UK, 2010.

[9]. Y. Wang and F. Li, Vehicular Ad Hoc Networks, Springer,London, UK, 2009.

[10]. H. Hartenstein and K. P. Laberteaux, "A Tutorial survey on vehicular ad hoc networks," IEEE Communications Magazine, vol. 46, no. 6, pp. 164–171, 2008.

[11]. R. G. Engoulou, M. Bella¨ıche, S. Pierre, and A. Quintero, "VANET security surveys," Computer Communications,ol. 44, pp. 1–13, 2014.

[12]. L. Zhang, "Key management scheme for secure channel Establishment in fog computing," IEEE Transactions on Cloud Computing, 2019.

[13]. S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," Telecommunication Systems, vol. 50, no. 4,pp. 217–241, 2012.

[14]. F. Qu, Z. Wu, F. Wang, and W. Cho, "A security and privacy review of VANETs," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985–2996, 2015.

[15]. R. Mishra, A. Singh, and R. Kumar, "VANET security: issues, challenges and solutions," in Proceedings of the International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 1050–1055, Chennai, India, March 2016.

[16]. J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, "An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks," IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 5, pp. 1621–1632,2019.

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

[18]. K. Bylykbashi, D. Elmazi, K. Matsuo, M. Ikeda, and L. Barolli, "Effect of security and trustworthiness for a fuzzy cluster management system in VANETs," Cognitive Systems Research, vol. 55, pp. 153–163, 2019.

[19]. J. P. Hubaux, S. Capkun, and J. Jun Luo, "the security and privacy of smart vehicles," IEEE Security & Privacy Magazine, vol. 2, no. 3, pp. 49–55, 2004.

[20]. S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular Ad Hoc network," Journal of Network and Computer Applications, vol. 37, pp. 380–392, 2014.

[21]. B. T. Sharef, R. A. Alsaqour, and M. Ismail, "Vehicular communication ad hoc routing protocols: a survey," Journal of Network and Computer Applications, vol. 40, pp. 363–396,2014.

[22]. M. Azees, L. Jegatha Deborah, and P. Vijayakumar, "Comprehensive survey on security services in vehicular adhoc networks," IET Intelligent Transport Systems, vol. 10, no. 6, pp. 379–388, 2016.
[23]. Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," IEEE Transactions on Intelligent Transportation Systems, vol. 20,no. 2, pp. 760–776, 2019.
[24]. S. Sharma and A. Kaul, "A survey on intrusion detection systems and honeypot based proactive security mechanisms in VANETs and VANET Cloud," Vehicular Communications, vol. 12, pp. 138–164, 2018.
[25]. A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 770–790, 2018.
[26]. I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): a survey,"Vehicular Communications, vol. 16, pp. 45–61, 2019.
[27]. X. Liang, T. Yan, J. Lee, and G. Wang, "A distributed intersection anagement protocol for safety, efficiency, and driver's comfort," IEEE Internet of Eings Journal, vol. 5,no. 3, pp. 1924–1935, 2018.
[28]. T. Neudecker, N. An, T. Gaugel, and J. Mittag, "Feasibility of virtual traffic lights in non-line-of-sight environments," in Proceedings of the Ninth ACM International Workshop on Vehicular Inter-Networking, Systems, and Applications—VANET'12, pp. 103–105, Lake District, UK, June 2012.
[29]. Draft guide for wireless access in vehicular environment (WAVE) architecture 2012, http://ieeexplore.ieee.org/servlet/ opac?punumber-6320593.
[30]. M. Ghosh, A. Varghese, A. A. Kherani, and A. Gupta,"Distributed misbehavior detection in VANETs," in Proceedings of the IIEEE Wireless Communications and Networking Conference (WCNC), Budapest, Hungary, April 2009.
[31]. X. Cheng, C. Chen, W. Zhang, and Y. Yang, "5G-Enabled cooperative intelligent vehicular (5GenCIV) framework: when benz meets marconi," IEEE Intelligent Systems, vol. 32,no. 3, pp. 53–59, 2017.
[32]. S. S. Kaushik, "Review of different aproaches for privacy," International Journal of Advanced Engineering and Technology, vol. 5, no. 2, pp. 356–363, 2013.
[33]. M. Gonzalez-Martin, M. Sepulcre, R. Molina-Masegosa, and J. Gozalvez, "Analytical models of the performance of C-V2X mode 4 vehicular communications," IEEE Transactions on Vehicular Technology, vol. 68, no. 2, pp. 1155–1166, 2019.
[34]. H. Chen, R. Zhang, W. Zhai, X. Liang, and G. Song, "Interference-free pilot design and channel estimation using ZCZ sequences for MIMO-OFDM-based C-V2X communications," China Communications, vol. 15, no. 7, pp. 47–54,2018.
[35]. Cellular-Vehicle-to-Everything-C-V2X,https://internetofthing sagenda.techtarget.com/definition/Cellular-Vehicle-to-Everything-C-V2X.
[36]. R. Molina-Masegosa and J. Gozalvez, "LTE-V for sidelink 5G V2X vehicular communications: a new 5G technology for short-range vehicle-to-everything communications," IEEE Vehicular Technology Magazine, vol. 12, no. 4, pp. 30–39, 2017.
[37]. S. Chen, J. Hu, Y. Shi, and L. Zhao, "LTE-V: a TD-LTE-based V2X solution for future vehicular network," IEEE Internet of Eings Journal, vol. 3, no. 6, pp. 997–1005, 2016.
[38]. J. M. de Fuentes, A. I. Gonzalez-Tablas, and A. Ribagorda, Overview of Security Issues in Vehicular Ad Hoc Networks, Hershey, Derry Township, PA, USA, 2010.
[39]. Dsrc, http://grouper.ieee.org/groups/scc32/dsrc/