Journal on Internet of Things
DOI:10.32604/jiot.2021.017943
Article

Security and Privacy in 5G Internet of Vehicles (IoV) Environment

Benjamin Kwapong Osibo[1], Chengbo Zhang[1], Changsen Xia[1], Guanzhe Zhao[2] and Zilong Jin[1,3,*]

[1]School of Computer Science, Nanjing University of Information Science and Technology, Nanjing, 210044, China
[2]Huihua College of Hebei Normal University, Shijiazhuang, 050091, China
[3]Jiangsu Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET), Nanjing University of Information Science and Technology, Nanjing, 210044, China
[*]Corresponding Author: Zilong Jin. Email: zljin@nuist.edu.cn
Received: 07 January 2021; Accepted: 11 April 2021

Abstract: Modern vehicles are equipped with sensors, communication, and computation units that make them capable of providing monitoring services and analysis of real-time traffic information to improve road safety. The main aim of communication in vehicular networks is to achieve an autonomous driving environment that is accident-free alongside increasing road use quality. However, the demanding specifications such as high data rate, low latency, and high reliability in vehicular networks make 5G an emerging solution for addressing the current vehicular network challenges. In the 5G IoV environment, various technologies and models are deployed, making the environment open to attacks such as Sybil, Denial of Service (DoS) and jamming. This paper presents the security and privacy challenges in an IoV 5G environment. Different categories of vehicular network attacks and possible solutions are presented from the technical point of view.

Keywords: 5G Internet of Vehicles; privacy; security; vehicular networks

1 Introduction

IoV is a distributed network environment consisting of vehicles communicating with other vehicles and systems such as roadside infrastructure, pedestrian mobile devices, and public networks. With the advantages of 5G, IoV will support five types of network communication; Intra-vehicular, Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Vehicle to Cloud (V2C) and Vehicle to Pedestrian (V2P) communications. Data sharing within the electronic control units (ECUs) of vehicles is facilitated by Intra-vehicular communication, whereas V2V supports data sharing within nearby vehicles [1–2]. Vehicle-to-everything (V2X) communications today, make it possible for vehicles and roadside units to be communicating nodes, providing each other with information, such as safety warnings, traffic congestion, etc. V2V communication makes it possible for vehicles in a network to send messages to each other, usually concerning their location, travel direction, etc. This technology uses dedicated short-range communications (DSRC), a standard set forth by bodies like the Federal Communications Commission (FCC) and International Organization for Standardization (ISO).

5G network offer low latency (reduces delay), high bandwidth, high data rate and improved overall network performance. Edge Computing coupled with 5G will allow a large range of connected technologies to be used simultaneously without incurring network outages. Vehicles can quickly join or leave the communication network even with their high mobility and irregular distribution. Vehicles usually broadcast information on their locations, speed, navigations, etc., at fixed time intervals within the network. Transmitted data is very important and must follow their optimum route without any unnecessary loss or drop. The number of vehicles on our roads has seen a rapid increase in recent years, likewise the rate of accidents and vehicular attacks, particularly in urban areas. IoV is then emerging to

improve the traffic conditions in cities and also improve road safety. The emergence of IoV and V2X makes it possible for vehicles to learn and share information about road conditions and the surrounding environment [3].

Modern vehicles are built with cameras, sensors, and other intelligent devices to monitor, transmit, and receive vehicle information [3]. These vehicles have the potential of storing personal data such as contact numbers, messages and financial information. Attackers find this stored information vulnerable and try to steal through remote access [4]. According to [4], cyberattacks on automated vehicles have risen by more than 50%. Vulnerabilities in connected vehicles that attackers target includes; Bluetooth, Tire Pressure Monitoring System (TPMS), On-board Diagnostics (OBD), Steering and Braking ECU, remote key and then infotainment application [4].

Fig. 1 illustrates a general 5G IoV environment with Vehicles, RSUs, Cloud Service, and a pedestrian. The existence of V2P makes it possible for communication to happen between vehicles and pedestrians through DSRC, cellular networks, Wi-Fi, and other wireless technologies. V2P communication helps avoid potential crashes or collision between drivers and pedestrians by making them aware of each other. In an autonomous vehicle scenario, vehicles can also transport passengers from one location to another after passengers have made a request via a mobile application [5]. On the road, V2V communication facilitates the sharing of information related to emergency brake lights, collision warnings, navigation lights warnings, and blind-spot warnings among vehicles on the road [6]. In getting the full benefit of this dynamic environment, RSUs contribute to carrying and sharing information about happenings on roads and other conditions such as weather to road users (pedestrians and vehicles). IoV can be considered as a form of Internet of Things (IoT) network, which is very mobile and is improving rapidly [7].

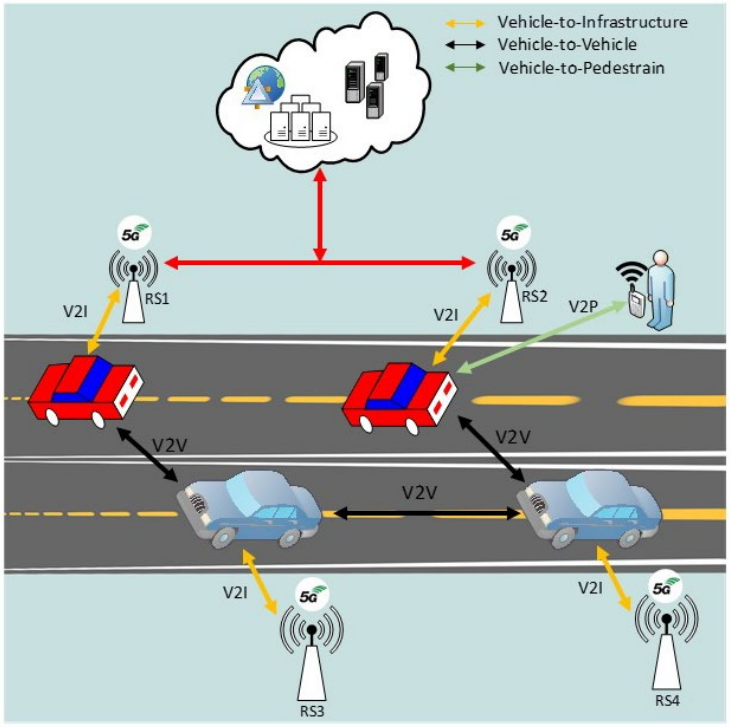

Figure 1: Illustration of 5G-enabled IoV environment

The paper's structure is as follows: Firstly, Section 1 presents the introduction, whereas Section 2 presents security requirements in IoV. Cyberattacks in the IoV environment are introduced in Section 3, then in Section 4 some proposed solutions to these attacks are provided. Finally, the conclusion is presented in Section 5.

2 Security and Privacy Requirement in IoV

2.1 Security Requirement

Owing to the direct impact on human life, privacy and security are critical concerns for IoV networks and as such, autonomous vehicles require a very robust security structure [5]. Like other networks, IoV involves the use of several communication systems and models, which makes it open to highly dangerous attacks [5–8]. In ensuring safe driving in an IoV environment, vehicles and other road users needs to be protected against radio jamming, data diddling, eavesdropping, DoS, and distributed denial of service (DDoS) [5–9]. Security in IoV depends massively on the medium through which communication takes place. Also, delays in the delivery of information may result in several security issues [10]. The fast movement and change in location of vehicles coupled with the strict Low latency requirement in vehicular networks mean the current security algorithm for vehicular networks and IoV needs to be improved accordingly.

2.1.1 Hardware Requirement

Hardware security refers to protecting hardware components against possible attacks in an IoV network due to device vulnerabilities. These devices consist of several communication units such as chips, sensors, and buses that work together in the network [11]. Besides chips and buses, devices also have firmware which is a target for many attackers. The main focus is to ensure that the various hardware components in IoV networks are implemented and configured appropriately. Also, device firmware needs to be updated in time to discourage hackers from exploiting them. While talking about hardware security, the physical protection of hardware components in an IoV environment can't be ignored. Assuming RSU1 and RSU2 in Fig. 1 are physically tampered with or damaged, the entire environment will be affected, leading to some serious consequences. The physical accessibility and availability of IoV devices cannot be ignored. Devices need to be kept in a restricted or secured area to prevent unauthorized access. Cybercriminals can implant malicious hardware or software into IoV devices if they can reach them. It is necessary to know the infrastructure in the environment and also advisable to dispose of old infrastructures that aren’t needed.

2.1.2 Software Requirement

In IoV, devices gather highly accurate and detailed data from the environment and vehicles, this collected data is important for the proper functioning of the IoV network. However, if the data is not properly secured or protected, attackers can take advantage and compromise the network. All collected and stored data should be accounted for. Also, messages that are circulated in the IoV environment should be mapped appropriately. Infotainment systems in modern vehicles also pose some risk to the IoV environment. Unknowing vehicle users can install malicious software onto their network’s programs through these infotainment systems. In such a scenario, attackers could spy, interrupt, or steal sensitive information from users and in some cases cause severe attacks such as DoS or DDoS. DDoS is one of the most common attacks in the last few years, where attackers try to interrupt IoV servers or networks by flooding them with internet traffics. Internet traffic by itself may not be malicious, but the attack disrupts the IoV ecosystem.

2.1.3 Radio Requirement

The intelligence of modern vehicles, smart mobile devices (SMDs), and smart infrastructures like the traffic lights make the IoV environment smart. These devices in the environment collect and send information to the cloud or edge servers via communication mediums such as Wi-Fi, ZigBee, Bluetooth, etc. As mentioned earlier, these communication channels establish connection among IoV components and therefore needs strong security since they can be exploited and used to launch attacks in the IoV network. They also require protocols to make them susceptible to known attacks.

5G in IoV will have the ability to send more data at much faster rates and support many devices at the same time unlike the small number of devices 4G supports. High speed, huge bandwidth, and ultralow latency are the advantages of a 5G IoV environment. Considering the 5G spectrum, it comprises small cells and millimeter waves which span from 30–300 GHz [12]; also other technologies such as massive multiple-input multiple-output (MIMO), network slicing, and function visualization all contribute to achieving the required performance of the 5G network [13]. The various integrated technologies in 5G make it open to numerous security challenges and as such policies and measures are needed to protect the network. Fig. 2 shows the forecast for mobile 5G subscriptions worldwide from 2021 to 2025 [14].

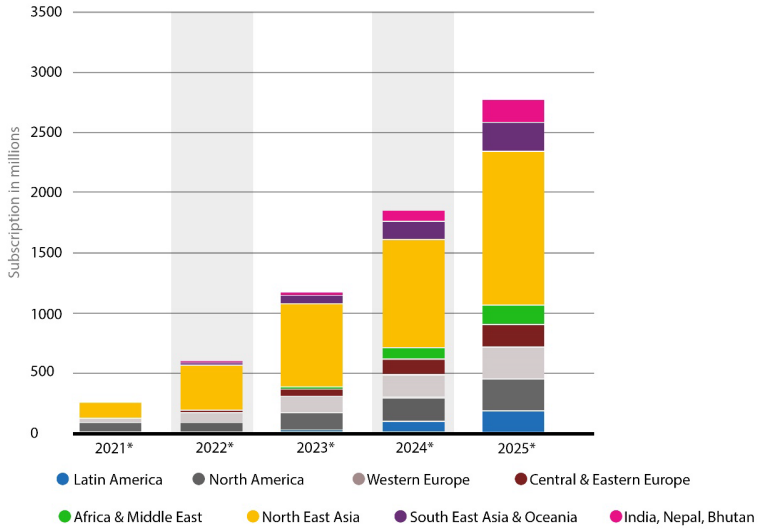

Figure 2: Forecast for 5G subscriptions worldwide [14]

2.2 Privacy Requirement

In Vehicular networks, different attacks on information privacy are possible. Attackers can target information such as the vehicle's speed, health condition and location. Also, the personal information of vehicle users or owners that are stored in infotainment systems can be a target for attackers. Below [15] are some outlined areas of concern regarding privacy in an IoV environment.

2.2.1 Vehicular Information Privacy

Vehicular information such as vehicle's health condition, registration information, and data generated and distributed by vehicles needs appropriate protection. Usually, during application offloading, data is transferred from vehicles to more powerful units for processing, all these offloaded data needs adequate privacy to prevent attackers from intercepting them.

2.2.2 Personal Information Privacy

In the Vehicular Network, Personal information of vehicle owners or drivers such as their names and driving license details should not be disclosed. Also, drivers should be mindful of the kind of information they store in their infotainment system. Messages and Contacts are common details stored in a vehicle's systems that attackers can exploit when not protected well.

2.2.3 Location Privacy

Destination routes and location information of vehicles in the environment should be kept safe to prevent possible attacks [15].

3 Attacks in IoV

In an environment where many components and devices are connected to the internet, there are always concerns about security and privacy. One major concern in IoV today is the assurance of security and privacy of users. How will the entire environment and customer data be protected? Due to the wireless medium in IoV, Vehicles and other parties in the network are open to various attacks. Fig. 3 demonstrates DDoS, jamming, Man-in-the-middle attack, and eavesdropping attacks in wireless networks which also applies to the 5G IoV environment [5–13].

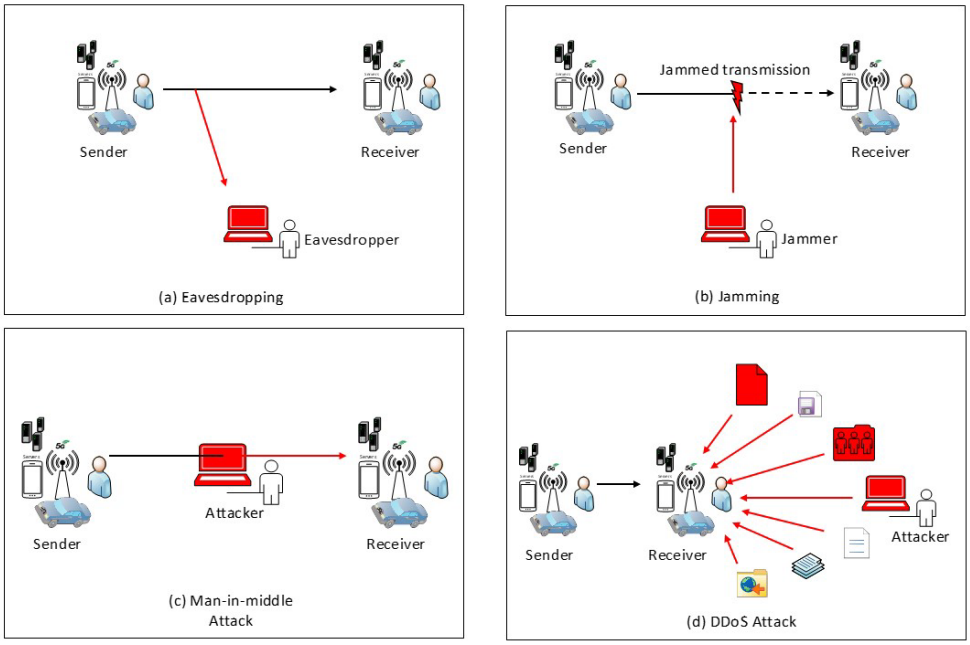

Figure 3: Illustration of attacks in Wireless 5G Networks (a) Eavesdropping (b) Jamming (c) Man-in-the-middle attack (d) DDoS attack

3.1 Eavesdropping Attacks

Eavesdropping occurs when attackers gain unauthorized access to vehicular messages or communication [16]. In eavesdropping, attackers usually take advantage of vehicular networks that are not properly secured and then intercept data sent or received. Besides vehicles, RSUs in the IoV environment are sometimes targets for attacks due to their roles in transferring traffic information. Eavesdropping in some cases, is referred to as snooping or sniffing attack. Data or information is usually not disturbed or altered; the attackers mostly aim to secretly gain access to information. Eavesdropping is a passive kind of attack and detecting it can be very tough. Fig. 3(a) illustrates eavesdropping in vehicular networks.

3.2 Jamming

Jamming is one of the numerous exploits that attackers use to compromise vehicular networks in an IoV environment. Jamming is considered a type of DoS attack because attackers deny services to authorized systems by overwhelming systems with traffics, keeping communication medium busy. As illustrated in Fig. 3(b) the attacker deliberately jams the transmission medium between the sender and receiver, in this instance, the receiver may be denied from receiving vital information.

3.3 Man-in-the-Middle Attacks

With this concept, attackers or hackers seek to breach and intercept communications between two separate parties, such as V2V, V2I, I2I, or even V2P networks. This can be a dangerous attack in the IoV

environment because being in the middle, the attacker secretly monitors, captures, and effectively controls communication between the two systems. As illustrated in Fig. 3(c) after a successful interception of the original communication, the attacker can then trick vehicles or other receiving parties leading them to act on messages from the attacker instead of the true sender.

3.4 DoS and DDoS Attacks

A DoS attack occurs when a service or system that usually works is unavailable for some time due to capacity overload or exhausted network resources. DoS is a serious attack that can partially or totally destroy vehicular networks, making infrastructures and services unavailable to users in an IoV environment. The DDoS attack, on the other hand, is a complex version of DoS. In DDoS, hackers use a larger number of compromised systems to attack one targeted system, making it harder and difficult to detect and defend as compared to the less complex DoS. Unlike cyber-attacks such as eavesdropping and man-in-the-middle attacks discussed earlier in this section, with DoS and DDoS, attackers usually do not try to steal or modify information. However, the cost of unavailability of services on the side of victim systems makes this cyber-attack the most famous in terms of taking down a whole network system [17]. Fig. 3(d) illustrates DoS and DDoS attacks in a 5G wireless network which can be also be applied to IoV. The attacker floods the receiving vehicle or node with several dummy messages just to overload the channel so that by the time-critical information is sent to the vehicle, the channel would have been too busy to process or receive the information.

3.5 Sybil Attacks

Sybil is a severe attack in which attackers maliciously use multiple fake identities or nodes in an attempt to control vehicles in an IoV environment [18]. To the victim nodes or vehicles, these fake identities appear to be unique users, however, it is a single attacker who controls the fake nodes all at once. Fig. 4(a) shows an IoV environment with one Sybil attacker, one victim node, and two Sybil nodes [19]. The Sybil attacker in the red vehicle controls the two Sybil nodes (yellow vehicles) all at the same time, while traveling on the road, the victim node acts on information received from the Sybil nodes without knowing that the information is deliberately sent from an attacker. The attacker can then send wrong information about the condition or happenings on road just to lure the victim node to change its direction.

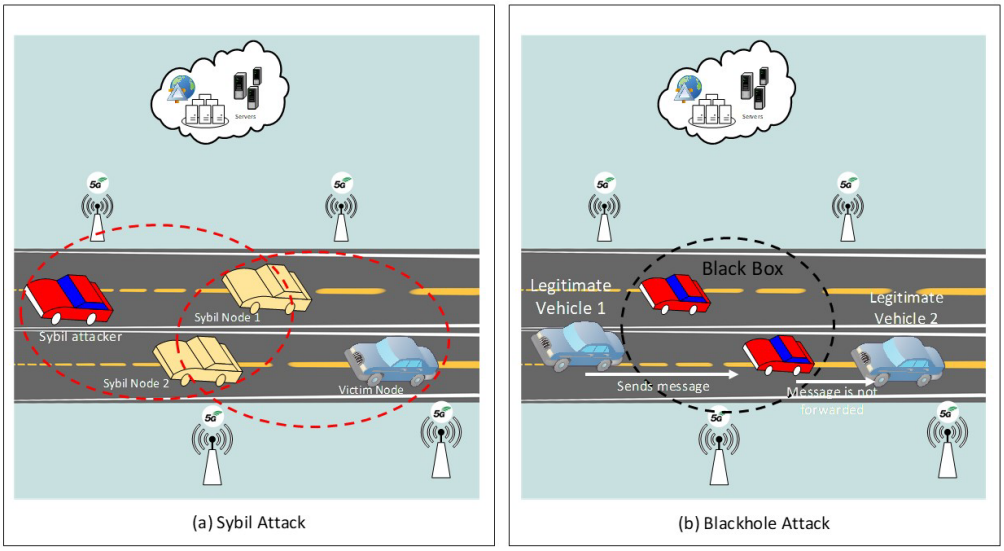

Figure 4: Sybil attacks (a) and blackhole attacks (b) in a 5G IoV environment

3.5 Blackhole Attacks

Blackhole attack is a well-known security threat in vehicular networks, where attackers try to take advantage of the loopholes to carry out malicious activities or specifically redirect network packets. In Blackhole attacks, intruders aim to interrupt network packets to either insect false information or cause the packets to be lost. Fig. 4(b) illustrates a black hole attack formed by two malicious red vehicles or nodes, which refuses to forward messages received from legitimate vehicle 1 to legitimate vehicle 2 [20].

4 Proposed Solutions

This section presents some proposed methods by various researchers to address the attacks discussed in the previous sections. The proposed methods are categorized based on whether the attack is against availability, data integrity, confidentiality, or authentication.

4.1 Availability

Availability refers to the overall uptime for networks (V2V, V2P, V2I, etc.) and systems in the IoV environment. It will always remain an important security requirement in IoV, especially when vehicles continue to depend on traffic and other vital road information. Without service availability, an entire IoV environment can be brought to a standstill. Jamming, Dos and DDoS are all attacks against availability in vehicular networks.

In [21], the authors proposed two systems; an anti-jamming automatic gain control (AGC) and a packet detection system to detect jams in vehicular networks. When a packet arrives in the two detection systems, the packet detection module checks for signal detection in the time domain, whereas the other monitors impulse jamming. Also, Lyamin et al. [22] proposed a data-mining-based approach for detecting Jamming DoS attacks in V2V communications. Their proposed method attempts to understand why vehicles usually lose messages in a platoon. The detection is based on understanding IEEE 802.11p protocol and also past evaluation of V2V channel incidents. Jie et al. [23] also presented a dynamic defense strategy for VANETs against DoS attacks focusing on the use of port hopping mechanisms. The authors designed a dynamic defense scheme that changes port numbers depending on the scheme of time to confuse intruders. finally, in [24], the authors proposed a packet detection algorithm for DoS attacks prevention in vehicular networks. The algorithm can detect malicious nodes in vehicular networks that send irrelevant packets to jam the network.

4.2 Data Integrity

Data integrity is the assurance that distributed information in the IoV environment is uncorrupted or not modified by unauthorized persons. In simple terms, data integrity means data received should be the same as the data sent. Man-in-the-middle attack is a common attack in an IoV environment against data integrity.

Admad et al. [25] seeks to address the man-in-the-middle attack in vehicular networks with their trust model in connected vehicles. Their model can identify malicious nodes initiating attacks in the network and then revoke these malicious nodes' credentials. The authors in [26] also proposed a pseudo-identity-based scheme for vehicular networks with conditional anonymity, authentication, and data integrity. The scheme uses pseudonym in the joining process with RSUs instead of real identity and satisfies the network's security requirements. The scheme then provides conditional anonymity to reveal the true identity of malicious vehicles. Also, in [27], the authors presented a pseudo-ID-based secure communication scheme for vehicular networks using ID-based encryption techniques to provide secure communication between V2V and V2I. The proposed scheme provides security against attacks such as man-in-the-middle and impersonation. Finally, the authors in [28] introduce an integrity checking scheme with supports of RSUs for the dynamic vehicular cloud. The scheme uses hash functions and signatures to check the integrity of messages sent from vehicles to the cloud. It also provides security for application attacks and data tampering.

4.3 Confidentiality

Confidentiality in IoV means vehicle's and user's information are kept secret and not disclosed to unintended people. Unauthorized persons need to be restricted from getting access to vehicle data such as vehicles' location and routes. Eavesdropping is a common attack in IoV against data confidentiality.

Huang et al. [29] focused on a model to prevent eavesdropping in an IoV environment by generating dummy traffic packets and directing them to specified RSUs to mislead traffic statistics and protect hotspot RSUs from attackers. The authors in [30] propose a rotated-jamming-based proactive eavesdropping scheme to monitor the suspicious link between a source and destination. The scheme performs two primary functions, intercepting information and interfering with a suspicious link. Finally, in [31], a secure and privacy-preserved real-time monitoring system for road conditions through cloud servers is presented. The proposed system prevents collusion attacks and hence prevents sensitive information of vehicle users from being disclosed to attackers.

4.4 Authentication

Authentication is an essential security model in IoV as it confirms the identity of users or systems in the environment. Anytime a vehicle or node enters the network, there should be an authentication system for verifying their identity. Sybil attack in IoV can be considered an attack that violates authentication because of fake identities by attackers.

The authors in [32] present a decentralized lightweight authentication scheme for V2V communications. In order to optimize the performance of the authentication mechanism for better security of legitimate users on the network, the proposed scheme adopts the principle of transitive trust. Additionally, the authors in [33] proposed a defense mechanism against Sybil attacks for anonymous location-based routing. In detecting the attack, previous message exchanges across a zone is considered, and then based on arrival angle, nodes are grouped into various zones (safe, unsafe, etc.). Finally, Hamdam et al. [18] present a hybrid algorithm to protect VANET against Sybil attacks by combining footprint and privacy-preserving detection methods.

5 Conclusion

In this paper, we explored the existing works and proposed solutions in the domain of vehicular networks and 5G. We discussed the security requirements in an IoV environment by grouping them into hardware requirements, software requirements, and radio requirements. According to these requirements, attacks in IoV environments were outlined, and countermeasures to these attacks were also presented. Attacks in IoV are generally against data integrity, confidentiality, availability or authentication; the countermeasures to these attacks were also categorized in that perspective.

Acknowledgement: This work was supported by the National Natural Science Foundation of China (Grant No. 61602252), the Natural Science Foundation of Jiangsu Province of China (Grant No. BK20160967), Project through the Priority Academic Program Development (PAPD) of Jiangsu Higher Education Institutions.

Funding Statement: The authors received fundings by the National Natural Science Foundation of China (Grant No. 61602252), the Natural Science Foundation of Jiangsu Province of China (Grant No. BK20160967), Project through the Priority Academic Program Development (PAPD) of Jiangsu Higher Education Institutions.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. Rouse and H. Matthew, Internet of Vehicles (IoV). [Online]. Available: https://whatis.techtarget.com/definition/Internet-of-Vehicles. 2020.

[2] P. Bajaj and M. Khanapurkar, Automotive networks based intra-vehicular communication applications. [Online]. Available: https://www.intechopen.com/books/new-advances-in-vehicular-technology-and-automotive-engineering/automotive-networks-based-intra-vehicular-communication-applications. 2020.

[3] X. Xu, Y. Xue, X. Li, L. Qi and S. Wan, "A computation offloading method for edge computing with Vehicle-to-Everything," *IEEE*, vol. 7, pp. 131068–131077, 2019.

[4] CISOMAG, Cyberattacks on automated vehicles rise by 99%: Report. [Online]. Available: https://cisomag.eccouncil.org/cyberattacks-on-automated-vehicles-rise-by-99-report/. 2020.

[5] T. S. Ezgi and B. Şerif, "A survey: Security and privacy in 5G vehicular networks," in *2019 4th Int. Conf. on Computer Science and Engineering (UBMK),* Samsun, Turkey, 2019.

[6] S. Ali, "Vehicle to vehicle communication," *ResearchGate*, 2019.

[7] Y. C. Sun, L. Wu, S. Z. Wu, S. P. Li, T. Zhang *et al.,* "Attacks and countermeasures in the Internet of Vehicles," Springer, pp. 283–295, 2016.

[8] S. Parkinson, P. Ward, K. Wilson and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 11, pp. 2898–2915, 2017.

[9] H. Peng, L. Liang, X. Shen and Y. L. Geoffrey, "Vehicular communications: A network layer perspective," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1064–1078, 2018.

[10] K. Rajdeep, T. P. Singh and K. Vinayak, "Security issues in vehicular Ad-Hoc network (VANET)," in *2nd Int. Conf. on Trends in Electronics and Informatics*, 2018.

[11] N. Potlapally, "Hardware security in practice: Challenges and opportunities," in *2011 IEEE Int. Sym. on Hardware-Oriented Security and Trust*, San Diego, CA, USA, 2011.

[12] D. Belghiti and A. Mabrouk, "5G-dynamic resource sharing mechanism for vehicular networks: Congestion game approach," in *2018 Int. Sym. on Advanced Electrical and Communication Technologies,* Rabat, Morocco, 2018.

[13] D. Fang, Y. Qian and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2017.

[14] S. O'Dea, Forecast number of mobile 5G subscriptions worldwide by region from 2019 to 2025, Statista, 2021 [Online]. Available: https://www.statista.com/statistics/521598/5g-mobile-subscriptions-worldwide/. 2020.

[15] M. A. Hoque and R. Hasan, "Towards an analysis of the architecture, security, and privacy issues in vehicular fog computing," in *2019 IEEE SoutheastCon,* Huntsville, AL, USA, 2019.

[16] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Elsevier*, vol. 23, 2019.

[17] S. P. Bendale and J. R. Prasad, "Security threats and challenges in future mobile wireless networks," in *2018 IEEE Global Conf. on Wireless Computing and Networking*, Lonavala, India, 2018.

[18] S. Hamdan, A. Hudaib and A. Awajan, "Detecting sybil attacks in vehicular Ad hoc networks," *International Journal of Parallel Emergent and Distributed Systems*, 2019.

[19] K. C. Kumar and C. G. Prakash, "A survey on VANETs security attacks and Sybil attack detection," *International Journal of Sensors, Wireless Communications and Control*, vol. 6, no. 1, 2016.

[20] M. S. Al-kahtani, "Survey on security attacks in Vehicular Ad Hoc Networks (VANETs)," in *2012 6th Int. Conf. on Signal Processing and Communication Systems*, Gold Coast, QLD, Australia, 2012.

[21] S. Y. Yeh, J. Y. Chu and T. Y. Hsu, "Poster: Anti-jamming automatic gain control and packet detection for vehicular receiver," in *2015 IEEE Vehicular Networking Conf.,* Kyoto, Japan, 2015.

[22] N. Lyamin, D. Kleyko, Q. Delooz and A. Vinel, "Real-time jamming DoS detection in safety-critical V2V C-ITS using data mining," *IEEE Communications Letters,* vol. 23, pp. 442–445, 2019.

[23] Y. Jie, M. Li, C. Guo and L. Chen, "Dynamic defense strategy against DoS attacks over vehicular Ad Hoc networks based on port hopping," *IEEE Access*, vol. 6, pp. 51374–51383, 2018.

[24] S. Kumar and S. M. Kulwinder, "Prevention of DoS attacks by detection of multiple malicious nodes in VANETs," in *2019 Int. Conf. on Automation, Computational and Technology Management (ICACTM),* London, UK, 2019.

[25] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain and F. Hussain, "MARINE: Man-in-the-Middle attack resistant trust model in connected vehicles," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3310–3322, 2020.

[26] M. A. Alazzawi, H. Lu, A. A. Yassin and K. Chen, "Efficient conditional anonymity with message integrity and authentication in a vehicular Ad-Hoc network," *IEEE Access*, vol. 7, pp. 71424–71435, 2019.

[27] M. Singh, T. Limbasiya and D. Das, "Pseudo-identity based secure communication scheme for vehicular Ad-hoc networks," in *2019 IEEE Int. Conf. on Advanced Networks and Telecommunications Systems (ANTS),* GOA, India, 2019.

[28] N. Hegde and S. S. Manvi, "Hash based integrity verification for vehicular cloud environment," in *2019 IEEE Int. Conf. on Cloud Computing in Emerging Markets*, Bengaluru, India, 2019.

[29] X. Huang, R. Yu, M. Pan and L. Shu, "Secure roadside unit hotspot against eavesdropping based traffic analysis in edge computing based internet of vehicles," *IEEE Access*, vol. 6, pp. 62371–62383, 2018.

[30] H. Xu and L. Sun, "Wireless surveillance via proactive eavesdropping and rotated jamming," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 10713–10727, 2019.

[31] B. Baruah and S. Dhal, "A Secure and privacy-preserved road condition monitoring system," in *2020 Int. Conf. on Communication Systems & Networks (COMSNETS),* Bengaluru, India, 2020.

[32] M. C. Chuang and J. F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular Ad-Hoc networks," *IEEE Systems Journal*, vol. 8, no. 3, pp. 749–758, 2013.

[33] S. V. Kumari and B. Paramasivan, "Defense against Sybil attacks and authentication for anonymous location-based routing in MANET," Springer, 2016.