# Security in V2X Communications: A Comparative Analysis of Simulation/Emulation Tools

João Silva[1(✉)], Luís Barreto[1,2], and Sérgio Ivan Lopes[1,2]

[1] ADiT-LAB, Instituto Politécnico de Viana do Castelo, Rua Escola Industrial e Comercial Nun'Álvares, 4900-347 Viana do Castelo, Portugal
jemanuelsilva@ipvc.pt, lbarreto@esce.ipvc.pt, sil@estg.ipvc.pt

[2] IT - Instituto de Telecomunicações, Campus de Santiago, 3810-193 Aveiro, Portugal

**Abstract.** Autonomous driving is becoming a reality and cars are getting connected with everything (traffic lights, roads, bicycles, other cars, people, infrastructure, etc.) being Vehicle-to-Everything (V2X) communications a critical factor in the success of autonomous cars. It is, thus, important to understand and study the main security vulnerabilities of V2X communication standards in the specific application context concerning future Intelligent Transportation Systems (ITS) and contribute with a comparison between existent simulation/emulation tools for security analysis in V2X communications with a focus on the ITS application domain. In that sense, this paper presents ta baseline study of different simulation/emulation tools that can be used to study those vulnerabilities. This study has shown that VENTOS is the simulator more suited for the truck platoon application scenario, and the Eclipse Mosaic is the best choice for simulation in the Cooperative Collision Avoidance application case.

**Keywords:** Security · V2X communication · ITS · Truck platoon · Intersection collision avoidance · Simulation · Emulation

## 1 Introduction

In recent years, there has been a significant growth and a rapid expansion of Intelligent Transportation Systems (ITS), mainly in metropolitan areas, and consequently an increase in cars circulating in the interior of those areas and on motorways. Due to this increase, the different types of transportation systems face several problems, such as a general growth in traffic and, as a consequence, a rise in accidents and environmental pollution, impacting the overall sustainable development of the urban ecosystem. These factors impose serious socio-economical problems, thus motivating countless efforts to improve the entire transportation process to become more secure and sustainable. Having this into consideration, policymakers have been joining forces to put forward initiatives such as the "CAR 2 CAR Communication Consortium" [1]—composed of some


S. Paiva et al. (Eds.): SmartCity360° 2021, LNICST 442, pp. 408–421, 2022.
https://doi.org/10.1007/978-3-031-06371-8_27

of the largest car manufacturers—which is becoming a hot topic, not only due to standardization but also in research and academia.

The idea of autonomous vehicles has also boosted the implementation of Intelligent Transportation Systems (ITS), especially within the industry. Typically, ITS present a set of characteristics, such as the measuring of distances between vehicles, the computing capacity of these data, and the ability to communicate with different subjects, that allow vehicles to have some or total independence or just support to driving.

There are several benefits of having autonomous vehicles, such as an improvement in road safety since 94% of serious accidents are due to human error. An autonomous vehicle has the potential to remove this factor, helping to protect passengers from vehicles, bicycles, or pedestrians [2]. Autonomous vehicles can also bring economical and social benefits, given that high amounts of financial resources are annually spent due to high accident rates—and everything that they involve—such as the expenses directly related to the accidents, the reduction in productivity, the loss of lives, and consequently, the loss of quality of life and the increase of government expenditure in the health service. Efficiency and convenience will also improve because ITS is beneficial in the sense of smoothing and making traffic constant, thus reducing the number of hours people spent on mobility-related tasks, directly enhancing their quality of life. On the other hand, reducing fuel consumption and reducing gas emissions present a major goal towards environmental sustainability. Another important benefit is related to the type of vehicles that provide mobility improvements to more people in society, such as older people with limitations to perform safe driving, thus raising its level of independence and improving its social inclusion.

According to [3], vehicle automation can be classified into four different categories: i) Systems that assist driving (driving support systems), which calculate better routes taking into account traffic and distance, fuel/energy consumption, and gas emissions; or ii) Systems that inform the driver of hazards, having no autonomous aspect, e.g., forward-collision warning, blind-spot warning or pedestrian detection and warning; iii) Systems that have partial control of the vehicle, both for driver support and emergency interventions, such as during driver monitoring if it is found that the driver is not in a position to drive or is showing unstable behavior, the system takes control of the vehicle to take it to a safe state; iv) Systems that include total vehicle control such as speed and trajectory, which have the resources, intelligence, and means of communication necessary to be autonomous.

In [4], a quantitative scale maps the systems previously introduced in a 5 level scale:

- Level 0: when there is no automation;
- Level 1: when just driver assistance is considered;
- Level 2: when it uses partial automation;
- Level 3: when there is enough automation and the driver is not necessary to monitor the environment;

– Level 4: includes high automation but still allows the driver to control the vehicle;
– Level 5: for full automation, no need for human intervention.

These systems are dependent on factors that directly relate to other subsystems, such as computing power and decision making, communications between the different network elements. Moreover, all decisions rely on shared information, which is more effective if the reliability and speed of communication are guaranteed. Due to this, several improvements in all types of communication technologies—such as DSRC, C- V2X (LTE/5G), WI-FI, Bluetooth, among others—have been put forward due to the demand of several ITS application domains.

Recently, several V2X communications simulators for different environments have emerged, becoming accessible to more people and without the need to spend high resources, allowing a wider community to focus on its study, i.e. academia and industry. This work will also present an analysis of different V2X communications simulators that are the most suitable for Truck Platoon and Cooperative Collision Avoidance application domains.

The remainder of this document is organized as follows: Sect. 2 introduces the ITS domains under the scope of this work; Sect. 3 presents the general architecture of V2X systems in the ITS application domain; Sect. 4 presents an overview of existent simulation/emulation tools for V2X communications in the ITS application domain and puts forward a discussion regarding the main findings; and in Sect. 6 the conclusions are presented.

## 2 Related Work/ITS Domains

The ITS application domains can be classified into four general categories: 1) Mobility, 2) Safety, 3) Environmental, and 4) Comfort.

These systems, when applied to mobility, are responsible for traffic management, thus supporting users with information on where the most traffic or hazards are. This results in different actions such as calculating the route, making it shorter or faster, taking into account different factors (distance, energy, traffic, time, weather, etc.), speed management, or cooperative navigation [5]. This information is collected by vehicles or RSU's (Road Side Units) and transmitted to vehicles directly or indirectly. When applied to the context of public transport, Advanced Traveler Information Systems (ATIS), provide users the detailed transport information allowing them to plan their trip, being able to understand the transport schedule, the duration of the trip and the distance the transport is at the location. Traffic Demand Estimation/Traffic Management are applications of ITS with a focus on mobility that aim to manage traffic both in urban centers and on highways, avoiding congestion that can increase accidents, increase pollution and make users spend unnecessary time on the road. Traffic Accurate Position Estimation, which can be applied to the vehicle itself, provides important information about the route and possible changes to the driver

and public transport allowing greater ease when the user prepares the trip and the service provider to show the real position of your vehicle. Roadside Service Finder, provides information about nearby petrol stations or hotels, for example, and Cooperative Adaptive Cruise Control (CACC) allows vehicles to be driven in a platoon [6].

Regarding the safety domain, ITS plays a fundamental role contributing to the reduction of traffic accidents, as a consequence of the increase in information and alerts that it presents to the driver about potential hazards that are not yet visible to him, such as speed reduction warning when approaching a tight curve or road in poor conditions. This domain includes different applications such as the "Vehicle Safety Application", which consists of vehicle and driver monitoring, and "Emergency Trajectory Alignment" [7,8]. Collision Warning and Obstacle Warning [9] are capable of informing the driver in advance about the possibility of collision or objects on the route, based on the information shared between the different vehicles and the infrastructure, the same applies to autonomous vehicles. Intelligent Speed Adaptation/Speed Limit informs about the appropriate speed or can adapt it according to the limit indicated on that road, while Incident Detection [10]/Pedestrian Crossing informs drivers/vehicles about accidents or pedestrians crossing the road, in routes where they circulate, respectively. Traffic Lights and Approaching of Emergency Vehicles are also some examples of ITS other applications.

ITS systems also bring environmental benefits, allowing the reduction of harmful gases emissions and fuel consumption. The information shared by the different surroundings in a given location regarding the state of the traffic (congested, free, accident) allows the driver to change its route, reschedule it and even change the trajectory habit, allowing a significant reduction in daily fuel consumption. CACC or Vehicle Platooning are other ITS applications with a great impact on the environment, consisting of one vehicle guiding remaining vehicles and thus controlling different factors of the trip such as (speed, braking, trajectory, etc.), then reducing consumption and consequently the emission of harmful gases. Since this applies mainly to business fleets, it also allows the reduction of the number of drivers. Calculating the route taking into account different factors, or the possibility of route recalculation when there is traffic or an accident also has a high impact on fuel reduction and gas emissions.

The fourth and final domain of ITS is related to "Comfort and Infotainment Applications" and its main objective is to increase the comfort and convenience that the vehicle provides to users, such as providing different applications that users can take advantage of such as VoIP, video, GPS [11], thus allowing you to search for a gas station, the nearest restaurant or hotel, and their prices, to provide internet so that passengers can continue their work, receive and send messages or play an online game.

### 2.1 Trucks Platoon

Platooning is an application of ITS that allows a group of vehicles to travel together, to define the speed and distance at which they travel among them-

selves, thus avoiding unexpected behavior by the different autonomous driving vehicles in the group [7]. The platoon is composed of a Platoon Leader (PL) who controls the platoon in distinct aspects—speed, distance, number of vehicles and which vehicles are allowed to enter or leave the platoon—and the Platoon Members (PMs) that follow these guidelines and report their status to the PL. Platooning integrates several technologies, such as Adaptive Cruise Control (ACC) systems, Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication systems, different sensing technologies such as Radio Detection and Ranging (RADAR) or Light Detection and Ranging (LIDAR), and visible light cameras which can measure the distance between vehicles and inform the ACC system through the vehicle's internal network. In turn, the ACC System sends control messages to the engine and brake modules and steering to control the vehicle's speed and direction. CACC is the most used concept in platooning and consists of adding V2V communications to ACC, either through cellular networks, WiFi, or Bluetooth, allowing vehicles not only to depend on sensor data, but also to exchange information between vehicles or RSU's [12]. The data reaches the ACC system through the in-vehicle network protocols such as Controller Area Network (CAN) and Local Interconnected Network (LIN), which typically do not use encryption, thus being a security breach that can be exploited [13]. CACC allows vehicles to quickly share information, resulting in considerable accuracy and safety improvement when traveling, particularly when braking or accelerating synchronously and cooperatively. Trucks Platooning makes it possible to improve traffic management and road performance as vehicles travel with a reduced distance from each other, as well as safety since the speed variation at which they travel is small reducing the impact speed in the event of a collision [14]. Fuel consumption and consequent pollutant gas emissions [15], can also be reduced as the air resistance to which vehicles are subject [2], decreases. This approach also applies to autonomous or partially autonomous driving vehicles, allowing the reduction of the number of effective drivers [7], thus decreasing operational costs.

### 2.2 Cooperative Collision Avoidance

Due to the increasing number of vehicles and consequently, traffic accidents, particularly on intersections, there is a need to improve collision avoidance systems. There has been an increase in research in academia and car manufacturing companies, leading to the current state in which the vehicle contains several sensors and cameras that cooperate with each other to reduce risks. However, these sensors have limitations, such as the need for line-of-sight (LoS), crucial for object detection [17]. In urban conditions, LoS is difficult to guarantee since vehicles may be behind buildings until the last moment, i.e. close to the intersection. One way to overcome this limitation can be the inclusion of isotropic wireless communications that cover all the vehicle environment, allowing it to communicate with neighboring vehicles and with RSUs [18]. The communication between vehicles and between vehicle and infrastructure elements improves the performance of these collision avoidance systems since it allows predicting the accident

and informing the driver, or in the case of autonomous vehicles, allowing preventive measures to be considered [19]. Communication on these systems is based mainly on IEEE 802.11p, known in Europe as European Telecommunication Standards Institute's (ETSI ITS-G5) or in the USA as Dedicated Short Range Communications (DSRC). In this way, vehicles communicate with the RSUs and exchange important information such as speed, intersection status, and vehicle position, using the GPS signal, and these, in turn, inform other vehicles. Whenever possible, vehicles communicate directly with each other since these types of communication suffer from decreased performance in urban environments with buildings as an obstacle to communication and with when a high density of vehicles occurs. To overcome these difficulties, there are already numerous advances in the application of C-V2X (LTE/5G) technology [20].

When compared to the previously mentioned protocols, the LTE protocol presents as main advantages easy implementation and low cost, since LTE cellular network infrastructure already exists, unlike IEEE802.11p which demands higher investment. LTE-V presents even better coverage, capacity and is a better choice for high mobility environments, using the same frequency spectrum of 3G and 4G. The major disadvantage of LTE-V is related to the transmission bite rate, which is considerably lower when compared with 3G and 4G [57].

Regarding the 5G communication protocol, this is the most promising one since it intends to eliminate most of the existing limitations in the current standards (3G, 4G/LTE), such as dynamic mobility and high relative velocities, extremely low-latency, ultra-high rate, high capacity for high message volume and high availability and reliability. There are still several challenges to guarantee the mentioned topics and make 5G the standard for communication in ITS [58].

## 3 Network Architecture

Both application cases mentioned in the previous sections share the same network architecture that can be divided into five communication types, as it is possible to observe in Fig. 1. The first type is related to the V2I communication since vehicles have to communicate directly with the RSU units. The second type refers to V2V, where the On Board Unit (OBU) of each vehicle communicates directly with neighboring vehicles. The third type concerns to Vehicle-to-Network (V2N) communications where vehicles communicate with the network, in this communication is normally used by cellular networks C-V2X (LTE, 5G) and they can provide services with support for wide-area coverage being beneficial to applications like traffic management and for infotainment applications [36,37]. The fourth type consists of Vehicle-to-People (V2P) communications which consist of communication between vehicles and pedestrians and should be taken into consideration when studying the cooperative Collision Avoidance context. Lastly, the fifth type concerns in In-Vehicle (IV) communications, the vehicle's internal network that allows communication between its functional components such as ECUs, AUs, Sensors (Radar/Lidar, Camera and Global Positioning System (GPS)) [21].

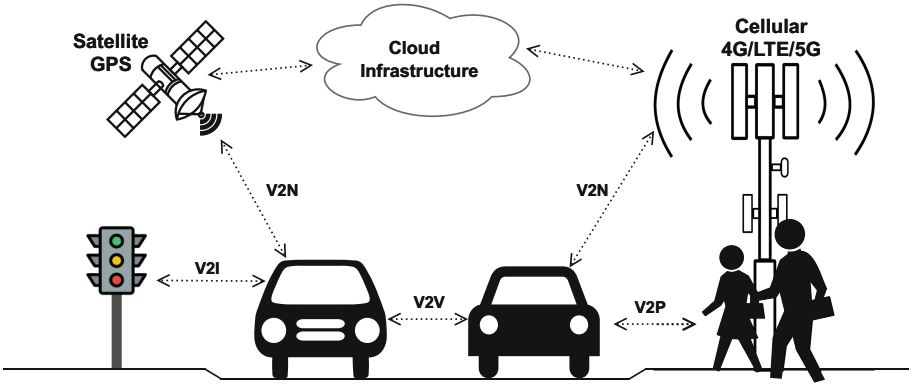


**Fig. 1.** V2X Network Architecture.

Existing communication technologies for V2I and V2V are supported by wireless technology and available in the 5.9 GHz band (5.85–5.925 GHz) [16]. This communication is based on the DSRC Protocol (Dedicated Short Range Communications), which evolved from IEEE 802.11p protocol, and was developed from IEEE802.11 to meet all V2X communications requirements. It is through this DSRC protocol that vehicles are able to communicate with their neighboring vehicles, share relevant information—such as speed, location, or acceleration several times per second, with a communication range of a few hundred meters—with the RSUs allowing to inform the state of the signs or the existence of hazards, e.g. the approach of an intersection, or the proximity to an emergency vehicle. At the In-Vehicle domain level, communications between the ACC system and the different ECUs are made using the CAN and LIN protocols, with the disadvantages being the fact that they do not encrypt communications, which is an important threat because it is possible to take complete control of the vehicle since an ECU with outward-facing interfaces can be compromised. These and all the other vulnerabilities related to communication between vehicles which may refer to communication protocols like DSRC, LTE, or 5G need to be avoided to autonomous driving vehicles become reliable for users. Bearing in mind that a failure in the communication between these autonomous or semi-autonomous transport systems can lead, in the best case, to a warning to a driver, which is not effective and an advantage, and, in the worse case, to a catastrophic loss of human lives. Therefore, it is necessary to develop safe and stable systems that are more reliable and trusted by the users. The exchange of information in these systems takes place mainly between V2I, V2V and IV, as for example the data of the different sensors to help autonomous driving or exchange data with other vehicles [22]. The entities used in V2I and V2V communications are vulnerable to attacks from wireless networks, and when an attack is successful a vehicle can be compromised and can trigger false warnings that in turn also impact the vehicles that are connected to each other in the communications stream. Likewise, attackers can create messages with the intention of deceiving other

vehicles on the network [59]. These examples show the importance of creating and implementing security requirements in V2X communications that guarantee the needs of users with regard to security, privacy, reliability, and integrity. Below, are presented the critical requirements that have been defined for these type of systems:

1. Authentication - Guarantees the recipient that the sender is trustworthy [23].
2. System and Communications Integrity - ensures that the content of messages is not modified during transmission and reliability and accuracy of message communication can be guaranteed at the destination [24,25].
3. Access Control - serves for granting access to specific services for the various network entities. The property of access control authorizes a node for performing allowed actions in the network, e.g., the network protocols that the node can execute [26].
4. System and Communications Confidentiality - guarantees non-disclosure of certain resources to unauthorized users without access rights.
5. Availability - services and protocols should remain functional even if faults occur. Therefore, the availability requirement guarantees secure, fault-tolerant and protocols that are able to re-stabilize themselves after the exclusion of the fault [27].
6. Privacy and Anonymity - systems should ensure for protecting the privacy of network users. Therefore, in the context of a broader area, privacy refers to information/data hiding, while anonymity is considered as a subset of privacy in vehicular networks.
7. Non-repudiation - Ensures that when a recipient identifies the source of message, the source takes complete responsibility and cannot deny later of its role [28].

## 4 Simulation/Emulation Tools

With the need to evaluate the problems identified in the previous section, design new solutions, or validate research studies, several simulators/emulators have been developed in recent years. The use of simulators allows to digitally replicate several real-world scenarios easier, without the need for having costly equipment, such as vehicles or infrastructure. There are several scenarios where these tools prove to be an advantage because they were developed according to the requirements and characteristics of VANET's, allowing to simulate distinct scenarios and network architectures in the ITS application domain, e.g. intersections or traffic jams, where the density of vehicles is high and can overload the network [29]. Moreover, they enable the simulation of the characteristics of high mobility vehicles with rapidly changing network topologies [30], which brings great difficulties for data transmission and routing [31], and requires low latency and high reliability for the V2X communications [32]. Another important aspect is related to the study of security aspects related to the communication between the different actors. The use of simulation tools allows more people to study vulnerabilities in the C-ITS communication protocols and therefore to improve the progress of these technologies.

### 4.1 Comparative Analysis

There are two different types of simulators, traffic simulators and network simulators. It is possible to integrate different traffic simulators with network simulators to replicate situations with different vehicles such as intersections and communication between vehicles and/or infrastructure elements. This study only considers simulators that already contain both traffic and network simulators integrated. However, to understand which is the best and most appropriate we will study the characteristics of the used traffic and network simulators.

With regard to traffic simulators, the main criteria that will be evaluated are: 1) type of communications it supports, 2) language/interface in which it is developed, 3) if it allows modeling obstacles, and 4) if it allows speed control and Multi-lane. On the other hand, in network protocols, the main criteria that will be used in evaluation will be: 1) type of communication it supports and 2) scalability.

**Table 1.** V2X simulators/emulators comparison.

| Simulators | Traffic software | Network software | License | References |
|---|---|---|---|---|
| VENTOS | SUMO | OMNet++ | Public, OpenSource | [35,47] |
| ITETRIS | SUMO | Proprietary software | Public | [48,53] |
| Tectos | SUMO | NetSim | Private | [41,49] |
| Artery | SUMO | OMNeT++ | Public, OpenSource | [33,38,50] |
| VEINS | SUMO | OMNeT++ | Public, OpenSource | [51,52] |
| Eclipse Mosaic | Eclipse SUMO | OMNeT++/NS-3 /SNS/Cell | Public/Private | [46,54] |
| VNS | Divert 2.0 | NS-3/OMNeT++ | Public | [56] |
| EstiNet11 | Proprietary software | Proprietary software | Private | [55] |

Most of the simulators in Table 1 are based on Sumo traffic simulator software [3,35]—developed in C++—because it is one of the most used and complete in the ITS application domain, as it allows V2X communications, allows speed control, multi-line simulation, and presents as a major drawback, not having obstacle modeling. However, obstacle modeling can be added using external tools. Moreover, it also allows the integration of other important tools to study different scenarios such as platooning [34], among others. There are other possibilities using proprietary software and Divert 2.0 solutions, but there is little information available about their characteristics and functionalities. In [33], El-Rewini et al. present a detailed assessment of several simulators.

Regarding network simulators, we noticed that the most used ones are OMNet++, which allows only V2V communications and supports graphical interface and high scalability, and NS-3 which allows V2X communications but does not support graphical interface and has reduced scalability (approx. 500 nodes). There are still others like NETSIM [41,42] which is a commercial software, and SNS and Cell [46] with a focus on cellular networks.

## 5 Discussion

In general, we can see that most of the simulators presented in Table 1 are based on the SUMO software [34] and that it allows the integration with different external tools, which makes it possible to eliminate any limitation that it has when compared to other traffic simulators, thus making it a good choice for the study of any scenario. Regarding network simulators, we noticed that there are significant differences in the two most used, i.e. the chosen simulators and the community adoption. OMNeT++ is presented as a software that allows high scalability but is exclusively dedicated to V2V communications [33,38–40] and NS3 as software whose greatest advantage is to allow the study of V2X communications, however, with less scalability [43–45]. In this way, it is already possible to recognize that the best choice is a public domain solution since they are based on the previously mentioned software. Considering the simulators comparison in the context of studying security vulnerabilities in two distinct application contexts, such as truck platoon and cooperative collision avoidance, VENTOS [35] and Eclipse Mosaic [46], are the simulators that better fill the requirements previously introduced. Besides, the iTETRIS [48] simulator is also a good option for the study of these application domains because it uses SUMO, i.e. its network simulator allows V2X communications, and the main advantage is that iTETRIS's modules are standard compliant with European Telecommunication Standards Institute's (ETSI's)) architecture for ITS Communication, which allows this simulation platform to produce realistic and large-scale ITS system modeling, however, a more detailed comparison is planned as future research. In the case of the Truck Platoon application context, the simulator that best fits the requirements is VENTOS, which is a simulator focused on collaborative driving, such as ACC, CACC, platoon management protocol, and also due to the fact that its stack is developed to study security attacks in collaborative driving situations [35]. In the specific case of the CACC application scenario, the simulator most suitable is the Eclipse Mosaic, since it also uses SUMO as traffic software and allows users to choose between different network simulators, such as OMNet ++ NS3 and the simulator of cellular networks called "Cell".

## 6 Conclusion

Vehicle-to-Everything (V2X) communication technologies are a critical success factor in autonomous driving, as cars are becoming more and more connected with everything (traffic lights, roads, bicycles, other cars, people, infrastructure,

etc.). This work introduced two relevant ITS application domains, i.e. Trucks Platoon and Cooperative Collision Avoidance, and referred its main security vulnerabilities. The main contribution of this work is the presented comparison between existent simulation/emulation tools for the security analysis in V2X communications. The evaluation performed allows to understand which are best adapted to the study of security related problems in the introduced application domains, with focus on important criteria, such as traffic and networking software, licence type and other core technical characteristics. Based on this study, we concluded that VENTOS is the simulator more suited for the truck platoon application domain, and the Eclipse Mosaic is the best choice for simulation in the Cooperative Collision Avoidance application domain.

Future work involves assessing vulnerabilities in the previously mentioned contexts, using the simulators/emulators that proved to be the most suitable.

**Acknowledgment.** This contribution is a result of ongoing research, in the scope of a dissertation work of the M.Sc. in Cybersecurity, in collaboration with the Applied Digital Transformation Laboratory (ADiT-Lab), and funded by the Polytechnic Institute of Viana do Castelo.

## References

1. Kiela, K., et al.: Review of V2X–IoT standards and frameworks for ITS applications. Appl. Sci. **10**(12), 4314 (2020). https://doi.org/10.3390/app10124314
2. Automated Vehicles for Safety (February 2018). https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety
3. Bishop, R.: Intelligent vehicle applications worldwide. IEEE Intell. Syst. Appl. **15**, 78–81 (2000)
4. NHTSA. https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety
5. Karagiannis, G., et al.: Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions. IEEE Commun. Surv. Tut. **13**(4), 584–616 (2011)
6. Singh, P.K., Nandi, S.K., Nandi, S.: A tutorial survey on vehicular communication state of the art, and future research directions. Veh. Commun. **18**, 100164 (2019)
7. Bian, K., Zhang, G., Song, L.: Security in use cases of vehicle-to-everything communications. In: IEEE Vehicular Technology Conference, September 2017, pp. 1–5 (2018)
8. Chowdhury, M., Apon, A., Dey, K.: Data Analytics for Intelligent Transportation Systems, pp. 1–316 (2017)
9. Nkoro, A.B., Vershinin, Y.A.: Current and future trends in applications of Intelligent Transport Systems on cars and infrastructure. In: 17th IEEE International Conference on Intelligent Transportation Systems, ITSC 2014, October 2014, pp. 514–519 (2014)
10. Al-Sultan, S., Al-Doori, M.M., Al-Bayatti, A.H., Zedan, H.: A comprehensive survey on vehicular Ad Hoc network. J. Netw. Comput. Appl. **37**, 380–392 (2014)
11. Araniti, G., Campolo, C., Condoluci, M., Iera, A., Molinaro, A.: LTE for vehicular networking: a survey. IEEE Commun. Mag. **51**(5), 148–157 (2013)

12. Singh, P.K., Tabjul, G.S., Imran, M., Nandi, S.K., Nandi, S.: Impact of security attacks on cooperative driving. In: 2018 IEEE Region 10 Conference, TENCON 2018, October 2018, pp. 138–143 (2018)
13. Valasek, C., Miller, C.: "Adventures in Automotive Networks and Control Units," Technical White Paper, p. 99 (2013)
14. Amoozadeh, M., Deng, H., Chuah, C.N., Zhang, H.M., Ghosal, D.: Platoon management with cooperative adaptive cruise control enabled by VANET. Veh. Commun. **2**, 110–123 (2015)
15. Veldhuizen, R., Van Raemdonck, G.M.R., van der Krieke, J.P.: Fuel economy improvement by means of two European tractor semi-trailer combinations in a platooning formation. J. Wind Eng. Ind. Aerodyn. **188**, 217–234 (2019)
16. Dadras, S.: Security of Vehicular Platooning (2019)
17. Rashdan, I., Schmidhammer, M., De Ponte Müller, F., Sand, S.: Performance evaluation of vehicle-to-vehicle communication for cooperative collision avoidance at urban intersections. In: IEEE Vehicular Technology Conference, pp. 1–5 (2018)
18. Thomas, L., Panicker, S.T., Jerry Daniel, J., Tony, T.: DSRC based collision warning for vehicles at intersections. In: 3rd International Conference on Advanced Computing and Communication Systems: Bringing to the Table, Futuristic Technologies from Around the Globe, ICACCS 2016 (2016)
19. Rawashdeh, Z.Y., Mahmud, S.M.: Intersection collision avoidance system architecture. In: 2008 5th IEEE Consumer Communications and Networking Conference, CCNC 2008, pp. 493–494 (2008)
20. Gharba, M., et al.: 5G enabled cooperative collision avoidance: system design and field test. In: 18th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2017 - Conference (2017)
21. Hamida, E., Noura, H., Znaidi, W.: Security of cooperative intelligent transport systems: standards, threats analysis and cryptographic countermeasures. Electronics **4**(384), 380–423 (2015)
22. Ghosal, A., Conti, M.: Security issues and challenges in V2X: a survey. Comput. Netw. **169**, 107093 (2020)
23. Heijden, R.V.D.: Security architectures in V2V and V2I communication. In: Proceedings of the 20th Student Conference on IT, University of Twente, Netherlands, pp. 1–10 (2010)
24. Dak, A.Y., Yahya, S., Kassim, M.: A literature survey on security challenges in VANETs. Int. J. Comput. Theor. Eng. **4**, 1007–1010 (2012)
25. Samara, G., Al-Salihy, W.A., Sures, R.: Security analysis of vehicular ad hoc networks (VANET). In: Proceedings of the International Conference on Network Applications Protocols and Services, pp. 55–60. IEEE (2010)
26. Sakib, R.K.: Security issues in VANET, Department of Electronics and Communication Engineering, BRAC University, Ph.D. thesis (2010)
27. Mejri, M.N., Ben-Othman, J., Hamdi, M.: Survey on VANET security challenges and possible cryptographic solutions. Veh. Commun. **1**(2), 53–66 (2014)
28. Hasrouny, H., Samhat, A.E., Bassil, C., Laouiti, A.: VANET security challenges and solutions: a survey. Veh. Commun. **7**, 7–20 (2017)
29. Wang, J., Shao, Y., Ge, Y., Yu, R.: A survey of vehicle to everything (V2X) testing. Sensors **19**(2), 334 (2019)
30. Oluoch, J.: VANETs: security challenges and future directions. World. Acad. Sci. Eng. Technol. Int. J. Comput. Electr. Autom. Control Inf. Eng. **10**, 1033–1037 (2016)

31. Alotaibi, M.M., Mouftah, H.: High speed multi-hop data dissemination for heterogeneous transmission ranges in VANETs. In: IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB), pp. 1–7 (2015)
32. Bai, F., Krishnan, H.: Reliability analysis of DSRC wireless communication for vehicle safety applications. In: 2006 IEEE Intelligent Transportation Systems Conference, pp. 355–362 (2006)
33. El-Rewini, Z.: Cybersecurity challenges in vehicular communications. Veh. Commun. **23**, 100214 (2020)
34. Mena-Oreja, J., Gozalvez, J.: PERMIT - a SUMO simulator for platooning maneuvers in mixed traffic scenarios. In: 2018 21st International Conference on Intelligent Transportation Systems (ITSC), pp. 3445–3450 (2018)
35. Cassou-Mounat, J., Labiod, H., Khatoun, R.: Simulation of cyberattacks in ITS-G5 systems. In: Krief, F., Aniss, H., Mendiboure, L., Chaumette, S., Berbineau, M. (eds.) Communication Technologies for Vehicles: 15th International Workshop, Nets4Cars/Nets4Trains/Nets4Aircraft 2020, Bordeaux, France, November 16–17, 2020, Proceedings, pp. 3–14. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-66030-7_1
36. Sheikh, M.U., Hämäläinen, J., David Gonzalez, G., Jäntti, R., Gonsa, O.: Usability benefits and challenges in mmWave V2V communications: a case study. In: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain (2019)
37. Báguena, M., Tornell, S.M., Torres, Á., Calafate, C.T., Cano, J., Manzoni, P.: VACaMobil: VANET car mobility manager for OMNeT++. In: 2013 IEEE International Conference on Communications Workshops (ICC), Budapest, Hungary, pp. 1057–1061 (2013)
38. De Rango, F., Tropea, M., Raimondo, P., Santamaria, A.F., Fazio, P.: Bio inspired strategy for improving platoon management in the future autonomous electrical VANET environment. In: 2019 28th International Conference on Computer Communication and Networks (ICCCN), Valencia, Spain, pp. 1–7 (2019). https://doi.org/10.1109/ICCCN.2019.8847088
39. Renzler, T., Stolz, M., Watzenig, D.: Decentralized dynamic platooning architecture with V2V communication tested in Omnet++. In: 2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE), Graz, Austria, pp. 1–6 (2019). https://doi.org/10.1109/ICCVE45908.2019.8965224
40. Avino, G.: Poster: a simulation-based testbed for vehicular collision detection. In: IEEE Vehicular Networking Conference (VNC), 2017, Torino, pp. 39–40 (2017). https://doi.org/10.1109/VNC.2017.8275655
41. Malik, S., Sahu, P.K.: Study on wireless communication aspect of VANETs. In: IEEE MTT-S International Microwave and RF Conference (IMaRC), Kolkata, India, 2018, pp. 1–4 (2018). https://doi.org/10.1109/IMaRC.2018.8877354
42. Jat, S., Tomar, R.S., Sharma, M.S.P.: Traffic congestion and accident prevention analysis for connectivity in vehicular ad-hoc network. In: 2019 5th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 2019, pp. 185–190 (2019). https://doi.org/10.1109/ISPCC48220.2019.8988463
43. Liu, W., Wang, X., Zhang, W., Yang, L., Peng, C.: Coordinative simulation with SUMO and NS3 for vehicular ad hoc networks. In: 2016 22nd Asia-Pacific Conference on Communications (APCC), Yogyakarta, Indonesia, 2016, pp. 337–341 (2016). https://doi.org/10.1109/APCC.2016.7581471
44. Days, W., Shagdar, O., Nashashibi, F., Tohme, S.: Performance study of CAM over IEEE 802.11p for cooperative adaptive cruise control. In: 2017 Wireless Days, Porto, 2017, pp. 70–76 (2017). https://doi.org/10.1109/WD.2017.7918118

45. Anadu, D., Mushagalusa, C., Alsbou, N., Abuabed, A.S.A.: Internet of Things: vehicle collision detection and avoidance in a VANET environment. In: IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Houston, TX, USA, 2018, pp. 1–6 (2018). https://doi.org/10.1109/I2MTC.2018.8409861
46. Hilt, B., Berbineau, M., Vinel, A., Pirovano, A.: Simulation of convergent networks for intelligent transport systems with VSimRTI. In: Networking Simulation for Intelligent Transportation Systems: High Mobile Wireless Nodes, 2017, pp. 1–28. Wiley (2017). https://doi.org/10.1002/9781119407447.ch1
47. VENTOS - VEhicular NeTwork Open Simulator. https://maniam.github.io/VENTOS/. Accessed 1 Mar 2021
48. iTETRIS Platform. http://www.ict-itetris.eu. Accessed 1 Mar 2021
49. NetSim-Network Simulator & Emulator. https://www.tetcos.com. Accessed 3 Mar 2021
50. Artery. https://github.com/riebl/artery. Accessed 7 Mar 2021
51. Veins. https://veins.car2x.org/. Accessed 7 Mar 2021
52. Haidari, M.J., Yetgin, Z.: Veins based studies for vehicular ad hoc networks. In: International Artificial Intelligence and Data Processing Symposium (IDAP), Malatya, Turkey, 2019, pp. 1–7 (2019). https://doi.org/10.1109/IDAP.2019.8875954
53. Soua, A., Shagdar, O., Lasgouttes, J.: Toward efficient simulation platform for platoon communication in large scale C-ITS scenarios. In: International Symposium on Networks, Computers and Communications (ISNCC), Rome, 2018, pp. 1–6 (2018). https://doi.org/10.1109/ISNCC.2018.8530962
54. Fraunhofer Fokus, Eclipse MOSAIC - A Multi-Domain and Multi-Scale Simulation Framework for Connected and Automated Mobility. https://www.eclipse.org/mosaic/. Accessed 11 Mar 2021
55. EstiNet - Simulator. https://www.estinet.com/ns/. Accessed 11 Mar 2021
56. VNS - Simulator. https://github.com/enriquefynn/libvns. Accessed 11 Mar 2021
57. Ivanov, I.V., Maple, C., Watson, T., Lee, S.: Cyber security standards and issues in V2X communications for Internet of Vehicles. In: Living in the Internet of Things: Cybersecurity of the IoT - 2018, IET London, Savoy Place, 28–29 March 2018 (2018). ISBN 9781785618437. https://doi.org/10.1049/cp.2018.0046
58. Abdel Hakeem, S.A., Hady, A.A., Kim, H.W.: 5G-V2X: standardization, architecture, use cases, network-slicing, and edge-computing. Wirel. Netw. **26**(8), 6015–6041 (2020)
59. Alnasser, A., Sun, H., Jiang, J.: Cyber security challenges and solutions for V2X communications: a survey. Comput. Netw. **151**, 52–67 (2019)