

Autonomous driving system and system hacking protection using V2X communication

Eugene Rhee, Junhee Cho

Department of Electronic Engineering, College of Engineering, Sangmyung University, Cheonan, Republic of Korea

Article Info

Article history:

Received Aug 26, 2024

Revised Feb 24, 2025

Accepted Mar 26, 2025

Keywords:

Autonomous driving
Communication
Network
System hacking
V2X

ABSTRACT

In this paper, a new autonomous driving system is proposed and problems such as systematic errors that may occur in the autonomous driving system were solved through vehicle to everything (V2X) communication technology. In the actual driving environment, accidents caused by the absence of communication between drivers and communication with infrastructure are frequently exposed. To solve these problems, a system was established that linked V2X communication with a vehicle system. In order to predict and study how this technology works in real traffic situations, it requires a lot of time, manpower, and funds because it requires building an environment similar to real traffic situations and using measuring equipment. For this reason, the system was built with simple model, and the research was conducted through simple simulation. In addition, as network technology and sensing technology for autonomous vehicles develop, the risk of hacking is also increasing. In this paper, various expected attack paths and methods that can hack autonomous vehicles are explained, and methods for defending them are presented.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Junhee Cho

Department of Electronic Engineering, College of Engineering, Sangmyung University

Cheonan, Republic of Korea

Email: jh_cho@smu.ac.kr

1. INTRODUCTION

Traffic accidents due to traffic congestion with the increase in vehicles, lacks of communication between drivers and drivers, and lacks of communication between infrastructure and drivers are increasing every year. As a result, enormous human and property damage are occurring. A representative example is a case in which a traffic light changes from a green light, which means driving possibility, to a yellow light, which means caution, while the vehicle is moving. In this case, the driving driver may think about stopping and accelerating until the last moment, and may cause a big problem due to the delay in judgment. In order to solve the problem including this example, various technologies are still being studied and developed around the world, and vehicle to everything (V2X) communication technology has recently been in the spotlight [1]-[3]. V2X communication is a technology that provides information through wired or wireless networks around the vehicle. V2X is collectively referred to as vehicle to vehicle (V2V) [4]-[6], vehicle to infrastructure (V2I) [7]-[9], especially in-vehicle networking (IVN) [10]-[12], V2V and vehicle to pedestrians (V2P) [13]-[15]. By using V2X communication technology, information on vehicles, roads, environment, stability, and convenience may be improved. V2X communication technology is currently being developed based on IEEE wireless access in vehicular environments (WAVE) standards, and countries around the world, including North America and Europe, are investing a lot of money as future technologies to develop technologies and build testbeds [16]-[18].

2. AUTONOMUS DRIVING SYSTEM

Autonomous driving cars refer to vehicles those move on their own without directly manipulating handles or pedals. Various sensors must be attached to enable these cars to move on their own. Automobiles collect driving data that is essential for driving from these various types of sensors and analyze the collected data. These analyzed data replace the driver's eyes and ears. There are six levels of development of autonomous driving vehicles. Level zero is a warning of a dangerous situation. It sounds a warning when a vehicle crosses a lane or when a vehicle exists in a blind spot of a side lane that is not visible in a side mirror. This level is far from autonomous driving because the driver directly makes all the inputs for the car to run. Level one is partially an automatic control. Level one includes a cruise mode in which a car travels at a speed specified by itself without stepping on an accelerator pedal, and a lane keeping assist that returns a vehicle to the original lane when the vehicle crosses the lane without a turn signal. Although level one has been improved technically compared to level zero, it is a level that has an auxiliary tendency in that cruise mode is designated or directional indicators should be put in person. Level two is also a partial automatic control level, like level one. If only the acceleration pedal was automated in level one, level two automatically intervenes with the brake in addition to the acceleration pedal. Levels three and four include all of the levels zero to two described above, minimizing driver intervention by identifying road conditions and taking appropriate action through the initiated sensor [19]-[21]. However, the steering wheel exists and leaves room for the driver to intervene in times of emergency or difficulty. The distinction between level three and four is the difference in the concentration of the driver on driving the vehicle and whether the priority of vehicle control is on the vehicle or on the driver. In level five, all controls such as handles, brakes, and acceleration pads are removed and all can be controlled with one monitor. Now, the concept of calling a vehicle driver disappears and only the concept of a passenger remains. In any emergency, the vehicle's artificial intelligence identifies the situation, responds appropriately, and gives no room for passengers to intervene.

3. SENSORS

Various sensors are attached to autonomous driving vehicles to help autonomous driving. Representative ones include ultrasonic sensors [22]-[24], cameras [25]-[27], radio detection and ranging (RADAR) [28]-[30], light detection and ranging (LiDAR) [31]-[33], and others. Table 1 compares the technical characteristics of representative sensors of an autonomous driving vehicle.

Table 1. Characteristics of autonomous driving vehicle sensor

Sensor	Function	Characteristics
Ultrasonic Waves	Uses ultrasonic waves to detect near-field obstructions and measure distances	* Mature stage of technology, low unit price of product * Short measurement distance * Parking aid technology
Camera	Uses camera sensors to recognize and process surroundings as images	* Sensitive to weather (rain, snow, fog) and time zones. * Parking aid technology
RADAR	Uses electric waves to measure the distance or speed of surrounding objects	* Unrestricted use of weather and time zones
LiDAR	Uses light to detect surrounding objects and obstacles	* Unlike ultrasonic sensors, it can recognize long distances * The unit price of the product is high * High precision, capable of implementing 3D images * Less detection compared to RADAR and more weather-sensitive

4. COMMUNICATION SYSTEM

4.1. V2X communication system

V2X communication system is the next generation system of traffic control and management [34]-[36]. V2X communication system provides pedestrians with a safe road, vehicle drivers with safety, convenience and efficient driving, and, lastly, country with the improvement of road environment, like as reduction of air pollution through the establishment of an improved traffic control system, and the activation of the automotive culture industry. V2X communication system provides a safe and comfortable driving environment for future smart cars through real-time intercommunication with other things such as driver's own car and other driver's vehicle V2V [37]-[39], road infrastructure (V2I) [40]-[42], and pedestrian (V2P) [43]-[45] in the vicinity. The sensors mentioned above are vulnerable to natural phenomena such as snow, rain, and fog, and there is no significant difference in the range of normal operation of the sensor and the distance from the view seen by driving drivers in real time. Unlike many sensors with these weaknesses, V2X communication system has a fairly wide range of communication and has the ability to detect and cope with various risks before the sensor operates.

As shown in Figure 1, V2X communication system has a much wider detection radius compared to several detection sensors such as RADAR and LiDAR and other computer vision sensors. The advantage of this V2X communication system alone can be efficiently used in situations such as intersections and curved paths.

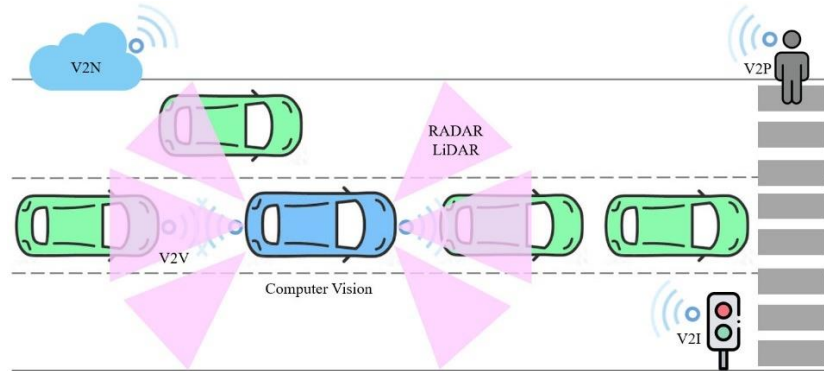


Figure 1. Range comparison of vehicle sensor and V2X communication system

4.2. Cellular-V2X communication system

Cellular-V2X (C-V2X) communication system is a cellular-based vehicle communication technology that can accelerate the emergence of autonomous vehicles [46]-[48]. C-V2X communication system compensates for the lack of sensor information such as existing vehicle cameras, RADAR, and LiDAR. As mentioned in Table 1, RADAR and LiDAR have the disadvantage that the unit price of the product is expensive or they are greatly affected by the weather. C-V2X communication system compensates for the shortcomings of existing sensors and quickly identifies the surrounding environment under intersections, blind spots in front of preceding vehicles, and non-line of sight (NLOS) conditions so that drivers can make correct and safe judgments [49], [50]. C-V2X communication system has two transmission modes as shown in Figure 2. The first transmission mode enables direct communication between vehicles, pedestrians, and road infrastructure based on long term evolution (LTE) direct technology. The second transmission mode is to use an LTE network widely constructed in the existing social infrastructure. Since LTE network is a wide-established network, it can receive news of accidents several kilometers ahead and be notified of the presence or absence of parking spaces and navigation information. Since the currently established LTE network is built to suit the mobile communication environment, research is actively underway to build an LTE network for vehicles and optimize it for vehicles.

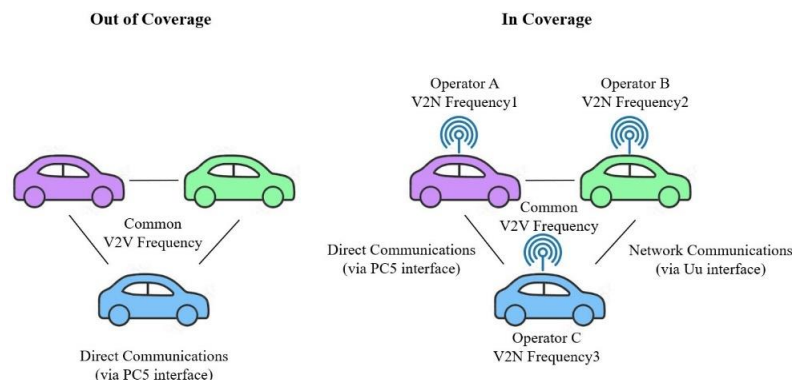


Figure 2. Two transmission methods of C-V2X communication system

In autonomous driving systems, communication interfaces are crucial for enabling vehicles to interact with each other, with infrastructure, and with the broader network. Two key interfaces in this context are the PC5 interface and the Uu interface. These interfaces are essential components of the C-V2X

communication framework, which is a foundational technology for connected and autonomous vehicles (CAVs). The PC5 interface is a direct communication link between vehicles V2V or between a vehicle and roadside infrastructure V2I, or other road users V2P. The PC5 interface allows devices to communicate directly without needing to go through a cellular base station (without the involvement of the cellular network core). This interface operates in two modes: broadcast mode (for sending messages to multiple receivers in the vicinity) and unicast mode (for direct communication with a specific device). It typically uses the 5.9 GHz intelligent transportation systems (ITS) band for communication, ensuring low latency and high reliability, which are critical for safety-related applications. The PC5 interface is used for exchanging information such as vehicle position, speed, direction, and other sensor data in real-time. This enables vehicles to coordinate maneuvers like lane changes, intersection crossing, and collision avoidance. It also supports applications like cooperative adaptive cruise control (C-ACC), where vehicles can autonomously adjust their speed based on the actions of other vehicles in the vicinity. On the other hand, the Uu interface is the standard cellular communication link between a vehicle and the cellular network base station (4G LTE or 5G). Unlike the PC5 interface, the Uu interface relies on the existing cellular infrastructure. It connects the vehicle to the cellular network, enabling long-range communication with cloud servers, other vehicles, or infrastructure that are not within direct communication range. The Uu interface supports high-bandwidth data exchange and can provide vehicles with access to broader network services, including real-time traffic updates, HD maps, and even over-the-air software updates. The Uu interface is crucial for non-safety applications that require more data and can tolerate slightly higher latencies, such as infotainment, fleet management, or cloud-based AI processing for decision-making. It also plays a role in enabling advanced driver assistance systems (ADAS) to receive updates and additional data from the cloud, such as high-definition maps and real-time traffic conditions.

In summary, The PC5 interface is for short-range, direct communication, typically within a few hundred meters, without requiring cellular infrastructure. In contrast, the Uu interface provides long-range communication through the cellular network infrastructure. And the PC5 interface is optimized for low-latency, safety-critical communication (collision avoidance), while the Uu interface is used for broader, less time-sensitive applications (cloud data retrieval, real-time traffic updates). In the context of autonomous driving, these interfaces complement each other. The PC5 interface ensures rapid, direct communication for immediate, local decisions, while the Uu interface connects the vehicle to the broader network, enabling more complex and data-intensive applications.

5. HACKING

As autonomous driving cars develop, the risk of hacking is also increasing. In the case of short-range RADARs used in autonomous driving vehicles, they are used in frequency pulses that require permission. This frequency pulse has the disadvantage of being vulnerable to hacking because it does not have a separate encoding or password. Hackers can use the RADAR's frequency to hack autonomous driving cars, manipulate the steering wheel of the vehicle, or fold side mirrors to disrupt driving. In fact, there was a case of being hacked and damaged by Chinese hackers while test-driving an autonomous car at Tesla in the U.S. There are two main ways to hack autonomous driving cars. The first is vehicle control using a smartphone infected by a virus, and the second is a method of eavesdropping and analyzing network communication such as Bluetooth, Wi-Fi, and wireless communication networks.

5.1. Vehicle control using a virus-infected smartphone

In the case of autonomous driving vehicles, various sensors connected to the vehicle are controlled through smartphones and audio video navigation (AVN), and various types of information from the vehicle are collected and utilized by linking with the smart car management system.

The expected process of controlling and operating autonomous driving vehicles using virus-infected smartphones is as follows; i) the attacker inserts a malicious virus into the smartphone application in advance and induces the driver to download and install the subtracted smartphone application, and ii) the installed application can further infect the entire smartphone and manipulate the vehicle to malfunction contrary to the driver's intention through the application.

5.2. Vehicle control through radio communication vulnerabilities and data modulation

Modern vehicles, especially autonomous and connected vehicles, rely on wireless communication systems for various functions, including V2V and V2I communication under the V2X framework. However, these wireless communication systems introduce several vulnerabilities. Data modulation plays a crucial role in ensuring secure and efficient communication between vehicles and infrastructure. It determines how digital signals are encoded for transmission over radio frequency (RF) channels. In order for autonomous driving cars to communicate with other objects, including themselves, wireless communication such as

Bluetooth, Wi-Fi, and mobile networks must be used. This communication method exposes vulnerabilities in the autonomous driving vehicle network, and attackers of the autonomous driving vehicle system can use the vulnerabilities of wireless communication to obtain control of the vehicle using signal eavesdropping, analysis, and packet modulation, and cause illegal malfunction.

6. COUNTERMEASURES AND RESULTS

There are two serious problems with autonomous driving cars. The first is the vulnerability of security. As cars become 'smart', the risk of hacking also increases, and to solve this problem, security code must be adopted and developed, and software firmware must be continuously updated. In addition, it is necessary to develop an independent computer operating system for autonomous driving vehicles to prevent viruses primarily, such as firewalls. The second is the ethical judgment of autonomous driving cars. Among the theories related to autonomous driving cars is the theory of trolley dilemma. The trolley dilemma is a theory that asks people whether the brakes can sacrifice a few to save the majority by presenting a broken trolley situation. What choice should a car make when an autonomous driving car faces an accident that cannot be avoided while driving?

There can be three cases for trolley dilemma; i) the case is that if you go straight, you will hit several pedestrians, and if you turn away, you will hit one person. Can the value of the majority take precedence over the value of the individual? ii) the case is that if you go straight, you hit one pedestrian, and if you turn away, the passenger of the car is in danger. In this case, should autonomous driving cars protect passengers or pedestrians? iii) the case is that if you go straight, you hit several pedestrians, and if you turn away, the passenger of the car is in danger. Should autonomous driving cars prioritize the protection of passengers or protect pedestrians? The trolley dilemma is not a systemic engineering flaw, but a matter of value that must be judged in terms of ethics and morality, and there is no answer. Before autonomous driving cars become a reality, social consensus must be reached on these issues. It is necessary to establish clear protection measures for the three major areas of vehicles, networks, and applications for the autonomous driving vehicle environment. This paper proposes a countermeasure for this. A method for device authentication and user authentication that can block illegal access to autonomous driving cars. For example, all access except normal access by vehicle drivers should be implemented. In order to respond to vehicle access through the network, a secure smart car environment can be implemented through data encryption and communication encryption to respond to possible eavesdropping and information leakage in all possible network sections.

7. CONCLUSION

In this paper, the purpose of this study was to exchange information in real time through interworking with vehicles, pedestrians, and infrastructure networks using V2X communication technology to establish an autonomous driving vehicle system. Currently, autonomous driving vehicles have reached the level two of research among the six research levels and are entering the third stage. In order to commercialize autonomous driving cars, it is necessary to replace existing sensors at high prices, and V2X communication technology enables this. V2X communication technology provides information in real time through a network with a vehicle, which provides information ahead of various sensors attached to the vehicle, thereby replacing existing sensors and providing a safer situation to the driver.

FUNDING INFORMATION

This research was funded by a 2024 research Grant from Sangmyung University(2024-A000-0108).

AUTHOR CONTRIBUTIONS STATEMENT

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Eugene Rhee	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓
Junhee Cho		✓	✓	✓	✓	✓	✓	✓		✓		✓		

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY




Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES




- [1] K. Sehla, T. M. T. Nguyen, G. Pujolle, and P. B. Velloso, "Resource allocation modes in C-V2X: from LTE-V2X to 5G-V2X," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8291–8314, Jun. 2022, doi: 10.1109/JIOT.2022.3159591.
- [2] F. Jameel, M. A. Javed, S. Zeadally, and R. Jantti, "Efficient mining cluster selection for blockchain-based cellular V2X communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4064–4072, Jul. 2021, doi: 10.1109/TITS.2020.3006176.
- [3] A. Ihsan, W. Chen, S. Zhang, and S. Xu, "Energy-efficient NOMA multicasting system for beyond 5G cellular V2X communications with imperfect CSI," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 8, pp. 10721–10735, Aug. 2022, doi: 10.1109/TITS.2021.3095437.
- [4] D. Han, B. Bai, and W. Chen, "Secure V2V communications via relays: resource allocation and performance analysis," *IEEE Wireless Communications Letters*, vol. 6, no. 3, pp. 342–345, Jun. 2017, doi: 10.1109/LWC.2017.2690292.
- [5] N. Ma, J. Chen, P. Zhang, and X. Yang, "Novel 3-D irregular-shaped model for massive MIMO V2V channels in street scattering environments," *IEEE Wireless Communications Letters*, vol. 9, no. 9, pp. 1437–1441, Sep. 2020, doi: 10.1109/LWC.2020.2993237.
- [6] N. Avazov, S. M. R. Islam, D. Park, and K. S. Kwak, "Statistical characterization of a 3-D propagation model for V2V channels in rectangular tunnels," *IEEE Antennas and Wireless Propagation Letters*, vol. 16, pp. 2392–2395, 2017, doi: 10.1109/LAWP.2017.2720469.
- [7] D. Suo, B. Mo, J. Zhao, and S. E. Sarma, "Proof of travel for trust-based data validation in V2I communication," *IEEE Internet of Things Journal*, vol. 10, no. 11, pp. 9565–9584, Jun. 2023, doi: 10.1109/JIOT.2023.3236623.
- [8] X. Wen, J. Chen, Z. Hu, and Z. Lu, "A p -opportunistic channel access scheme for interference mitigation between V2V and V2I communications," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3706–3718, May 2020, doi: 10.1109/JIOT.2020.2967647.
- [9] Z. Du *et al.*, "Integrated sensing and communications for V2I networks: dynamic predictive beamforming for extended vehicle targets," *IEEE Transactions on Wireless Communications*, vol. 22, no. 6, pp. 3612–3627, Jun. 2023, doi: 10.1109/TWC.2022.3219890.
- [10] W. Wu *et al.*, "A survey of intrusion detection for in-vehicle networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 3, pp. 919–933, Mar. 2020, doi: 10.1109/TITS.2019.2908074.
- [11] Y. Peng, B. Shi, T. Jiang, X. Tu, D. Xu, and K. Hua, "A survey on in-vehicle time-sensitive networking," *IEEE Internet of Things Journal*, vol. 10, no. 16, pp. 14375–14396, Aug. 2023, doi: 10.1109/JIOT.2023.3264909.
- [12] J. Xiao, H. Chen, and F. Zhong, "A novel feature extraction framework using graph node attention network for in-vehicle networks intrusion detection," *IEEE Systems Journal*, vol. 18, no. 1, pp. 150–161, Mar. 2024, doi: 10.1109/JSYST.2023.3337091.
- [13] P. Merdrignac, O. Shagdar, and F. Nashashibi, "Fusion of perception and V2P communication systems for the safety of vulnerable road users," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 7, pp. 1740–1751, Jul. 2017, doi: 10.1109/TITS.2016.2627014.
- [14] C. Zhang *et al.*, "Implementation of a V2P-based VRU warning system with C-V2X technology," *IEEE Access*, vol. 11, pp. 69903–69915, 2023, doi: 10.1109/ACCESS.2023.3293122.
- [15] A. Kabil, K. Rabieh, F. Kaleem, and M. A. Azer, "Vehicle to pedestrian systems: survey, challenges and recent trends," *IEEE Access*, vol. 10, pp. 123981–123994, 2022, doi: 10.1109/ACCESS.2022.3224772.
- [16] IEEE, "IEEE standard for wireless access in vehicular environments - security services for applications and management messages," in *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013) - Redline*, 2016, pp. 1–884.
- [17] A. Raza, S. J. Nawaz, S. Wyne, A. Ahmed, M. A. Javed, and M. N. Patwary, "Spatial modeling of interference in inter-vehicular communications for 3-D volumetric wireless networks," *IEEE Access*, vol. 8, pp. 108281–108299, 2020, doi: 10.1109/ACCESS.2020.3001052.
- [18] S. Khan *et al.*, "5G vehicular network resource management for improving radio access through machine learning," *IEEE Access*, vol. 8, pp. 6792–6800, 2020, doi: 10.1109/ACCESS.2020.2964697.
- [19] G. Binghong, "Automotive Radar Technology & Test Solution for Autonomus Driving," in *2019 IEEE MTT-S International Wireless Symposium (IWS)*, May 2019, pp. 1–2, doi: 10.1109/IEEE-IWS.2019.8803901.
- [20] F. Zubeck, A. Melichar, I. Kenicky, L. Korosi, and I. Sekaj, "Autonomus systems control design using neuro-evolution," in *2022 Cybernetics & Informatics (K&I)*, Sep. 2022, pp. 1–6, doi: 10.1109/KI55792.2022.9925928.
- [21] H. Abaza *et al.*, "RDMA-based deterministic communication architecture for autonomous driving," in *2023 IEEE 29th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA)*, Aug. 2023, pp. 137–146, doi: 10.1109/RTCSA58653.2023.00025.
- [22] E. Odat, J. S. Shamma, and C. Claudel, "Vehicle classification and speed estimation using combined passive infrared/ultrasonic sensors," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 5, pp. 1593–1606, May 2018, doi: 10.1109/TITS.2017.2727224.
- [23] H. Zhao and Z. Wang, "Motion measurement using inertial sensors, ultrasonic sensors, and magnetometers with extended kalman filter for data fusion," *IEEE Sensors Journal*, vol. 12, no. 5, pp. 943–953, May 2012, doi: 10.1109/JSEN.2011.2166066.
- [24] Z. El-Rewini, K. Sadatsharan, N. Sugunraj, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity attacks in vehicular sensors," *IEEE Sensors Journal*, vol. 20, no. 22, pp. 13752–13767, Nov. 2020, doi: 10.1109/JSEN.2020.3004275.

- [25] H. M. Hsu, J. Cai, Y. Wang, J. N. Hwang, and K. J. Kim, "Multi-target multi-camera tracking of vehicles using metadata-aided re-ID and trajectory-based camera link model," *IEEE Transactions on Image Processing*, vol. 30, pp. 5198–5210, 2021, doi: 10.1109/TIP.2021.3078124.
- [26] D. Chang, S. Huang, Y. Zhou, X. Qin, R. Ding, and M. Hu, "Target-free stereo camera-GNSS/IMU self-calibration based on iterative refinement," *IEEE Sensors Journal*, vol. 24, no. 3, pp. 3722–3730, Feb. 2024, doi: 10.1109/JSEN.2023.3343371.
- [27] H. Li, A. Zheng, L. Sun, and Y. Luo, "Camera topology graph guided vehicle re-identification," *IEEE Transactions on Multimedia*, vol. 26, pp. 1565–1577, 2024, doi: 10.1109/TMM.2023.3283054.
- [28] F. Abushakra *et al.*, "A miniaturized ultra-wideband radar for UAV remote sensing applications," *IEEE Microwave and Wireless Components Letters*, vol. 32, no. 3, pp. 198–201, Mar. 2022, doi: 10.1109/LMWC.2021.3129153.
- [29] B. Zhu, Y. Sun, J. Zhao, S. Zhang, P. Zhang, and D. Song, "Millimeter-wave radar in-the-loop testing for intelligent vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 8, pp. 11126–11136, Aug. 2022, doi: 10.1109/TITS.2021.3100894.
- [30] F. Roos, D. Kellner, J. Dickmann, and C. Waldschmidt, "Reliable orientation estimation of vehicles in high-resolution radar images," *IEEE Transactions on Microwave Theory and Techniques*, vol. 64, no. 9, pp. 2986–2993, Sep. 2016, doi: 10.1109/TMTT.2016.2586476.
- [31] Y. Ren, B. Liu, R. Cheng, and C. Agia, "Lightweight semantic-aided localization with spinning LiDAR sensor," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 1, pp. 605–615, Jan. 2023, doi: 10.1109/TIV.2021.3099022.
- [32] Y. Ding *et al.*, "Long-distance vehicle dynamic detection and positioning based on Gm-APD Lidar and LIDAR-YOLO," *IEEE Sensors Journal*, vol. 22, no. 17, pp. 17113–17125, Sep. 2022, doi: 10.1109/JSEN.2022.3193740.
- [33] P. Sun, X. Zhao, Z. Xu, R. Wang, and H. Min, "A 3D LiDAR data-based dedicated road boundary detection algorithm for autonomous vehicles," *IEEE Access*, vol. 7, pp. 29623–29638, 2019, doi: 10.1109/ACCESS.2019.2902170.
- [34] K. Sehla, T. M. T. Nguyen, G. Pujolle, and P. B. Velloso, "Resource allocation modes in C-V2X: from LTE-V2X to 5G-V2X," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8291–8314, Jun. 2022, doi: 10.1109/JIOT.2022.3159591.
- [35] M. H. C. Garcia *et al.*, "A tutorial on 5G NR V2X communications," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 3, pp. 1972–2026, 2021, doi: 10.1109/COMST.2021.3057017.
- [36] L. Lusvardi, B. Coll-Perales, J. Gozalvez, and M. L. Merani, "Link level analysis of NR V2X sidelink communications," *IEEE Internet of Things Journal*, vol. 11, no. 17, pp. 28385–28397, Sep. 2024, doi: 10.1109/JIOT.2024.3402551.
- [37] S. M. Hussain, K. M. Yusof, R. Asuncion, and S. A. Hussain, "Artificial intelligence based handover decision and network selection in heterogeneous internet of vehicles," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 22, no. 2, pp. 1124–1134, May 2021, doi: 10.11591/ijeecs.v22.i2.pp1124-1134.
- [38] H. A. Ameen, A. K. Mahamad, S. Saon, D. M. Nor, and K. Ghazi, "A review on vehicle to vehicle communication system applications," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 18, no. 1, pp. 188–198, Apr. 2019, doi: 10.11591/ijeecs.v18.i1.pp188-198.
- [39] C. Giovannetti, N. Decarli, S. Bartoletti, R. A. Stirling-Gallacher, and B. M. Masini, "Target positioning accuracy of V2X Sidelink joint communication and sensing," *IEEE Wireless Communications Letters*, vol. 13, no. 3, pp. 849–853, Mar. 2024, doi: 10.1109/LWC.2023.3346937.
- [40] J. Chen, Z. Wang, and T. Mao, "Resource management for hybrid RF/VLC V2I wireless communication system," *IEEE Communications Letters*, vol. 24, no. 4, pp. 868–871, Apr. 2020, doi: 10.1109/LCOMM.2020.2969624.
- [41] Y. Yao, F. Shu, X. Cheng, H. Liu, P. Miao, and L. Wu, "Automotive radar optimization design in a spectrally crowded V2I communication environment," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 8, pp. 8253–8263, Aug. 2023, doi: 10.1109/TITS.2023.3264507.
- [42] M. Zhou, Y. Li, Y. Sun, and Z. Ding, "Outage performance of RIS-assisted V2I communications with inter-cell interference," *IEEE Wireless Communications Letters*, vol. 12, no. 6, pp. 962–966, Jun. 2023, doi: 10.1109/LWC.2023.3253854.
- [43] M. Li, X. Yang, F. Khan, M. A. Jan, W. Chen, and Z. Han, "Improving physical layer security in vehicles and pedestrians networks with ambient backscatter communication," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 9380–9390, Jul. 2022, doi: 10.1109/TITS.2021.3117887.
- [44] P. Sewalkar and J. Seitz, "MC-COCO4V2P: multi-channel clustering-based congestion control for vehicle-to-pedestrian communication," *IEEE Transactions on Intelligent Vehicles*, vol. 6, no. 3, pp. 523–532, Sep. 2021, doi: 10.1109/TIV.2020.3046694.
- [45] M. G. Doone, S. L. Cotton, D. W. Matolak, C. Oestges, S. F. Heaney, and W. G. Scanlon, "Pedestrian-to-vehicle communications in an urban environment: channel measurements and modeling," *IEEE Transactions on Antennas and Propagation*, vol. 67, no. 3, pp. 1790–1803, Mar. 2019, doi: 10.1109/TAP.2018.2885461.
- [46] P. Wang, B. Di, H. Zhang, K. Bian, and L. Song, "Cellular V2X communications in unlicensed spectrum: harmonious coexistence with VANET in 5G systems," *IEEE Transactions on Wireless Communications*, vol. 17, no. 8, pp. 5212–5224, Aug. 2018, doi: 10.1109/TWC.2018.2839183.
- [47] C. Campolo, A. Molinaro, A. O. Berthet, and A. Vinel, "On latency and reliability of road hazard warnings over the cellular V2X Sidelink interface," *IEEE Communications Letters*, vol. 23, no. 11, pp. 2135–2138, Nov. 2019, doi: 10.1109/LCOMM.2019.2931686.
- [48] Z. Naghsh and S. Valaee, "Conflict-free scheduling in cellular V2X communications," *IEEE/ACM Transactions on Networking*, vol. 29, no. 1, pp. 106–119, 2021, doi: 10.1109/TNET.2020.3030850.
- [49] J. Zhang, J. Salmi, and E. S. Lohan, "Analysis of kurtosis-based LOS/NLOS identification using indoor MIMO channel measurement," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 6, pp. 2871–2874, Jul. 2013, doi: 10.1109/TVT.2013.2249121.
- [50] J. Xie, W. Wang, X. Liu, I. Rashdan, C. Di, and J. Qin, "Identification of NLOS based on soft decision method," *IEEE Wireless Communications Letters*, vol. 12, no. 4, pp. 703–707, Apr. 2023, doi: 10.1109/LWC.2023.3240846.

BIOGRAPHIES OF AUTHORS

Eugene Rhee    received the Ph.D. degree in electronics from Hanyang University, Korea, in 2010. He was a visiting professor at Chuo University, Japan from 2010 to 2011. Since 2012, he has been with Sangmyung University, Korea, where he is currently a professor in the department of electronic engineering. His research area includes microwave, electromagnetic compatibility, electromagnetic interference, and reverberation chamber. He can be contacted at email: eugenerhee@smu.ac.kr.



Junhee Cho    received his Ph.D. degree in electrical engineering from University of Cambridge, U.K. in 2017. Since 2020, he has been an assistant professor in the department of electronics engineering, Sangmyung University, Republic of Korea. His current research interests include nanophotonics-based secure communications. He can be contacted at email: jh_cho@smu.ac.kr.