Proceedings of CONF-MSS 2025 Symposium: Automation and Smart Technologies in Petroleum Engineering
DOI: 10.54254/2755-2721/149/2025.KL22727

6G-V2X Security: Overcoming Challenges for a Safer, Smarter Transportation Future

Sicheng Xin

Institute of Xidian University, Xi'an, China
15011231760@163.com

Abstract: 6G-V2X is poised to revolutionize vehicular networks by achieving terabit-per-second (Tb/s) transmission rates, microsecond-level latency, and an integrated space-air-ground-sea architecture, addressing the limitations of 5G-V2X. These advancements enhance network coverage, mitigate signal blind spots, and improve communication reliability, fostering a secure intelligent transportation system. However, the complexity and immaturity of 6G technologies introduce multifaceted security challenges, spanning both physical safety in vehicular environments and cyber threats. While recent research has made significant progress, key challenges remain. This paper reviews enabling technologies for 6G-V2X security, analyzes existing solutions and unresolved issues, and outlines future research directions.

Keywords: 6G-V2X, Vehicular Networks, Intelligent Transportation

1. Introduction

Currently, the mainstream technology for Vehicle-to-Everything (V2X) in the automotive industry, 5G-V2X, faces several bottlenecks in real-world applications and is generally considered insufficient to meet the future demands of Intelligent Transportation Systems (ITS). For instance, in extreme situations like emergency braking, the efficiency of information decision-making is not ideal. Additionally, handling large volumes of data often leads to delays, congestion, and disconnections in high-speed mobility scenarios. Moreover, 5G-V2X is not capable of addressing the explosive growth in connectivity demands expected for future V2X networks. 6G-V2X technology, however, is seen as a promising solution to these issues and has garnered significant attention [1]. Driven by 6G, V2X technology theoretically holds the potential to address challenges related to communication reliability in high-mobility environments. As advancements in V2X and autonomous driving systems continue, new challenges will arise, alongside entirely new in-vehicle service demands [2], such as tactile communication, immersive in-car entertainment, and holographic intelligent interaction systems. These innovations will push the limits of wireless communication networks, expanding standards for data transmission rate, latency, environmental impact, and spectrum resources—requirements that are currently difficult for 5G-V2X to meet. However, with the ongoing breakthroughs in 6G communication technology, networks capable of supporting complex and diverse environments are becoming a reality, making the integration of V2X with traditional communication networks more intelligent, scalable, and environmentally friendly.

The development of 6G-V2X faces numerous challenges, particularly regarding the security and privacy of information transmission. As V2X applications become more intelligent, there are

DOI: 10.54254/2755-2721/149/2025.KL22727

increasing concerns about the possibility of technological defects and cyberattacks that could lead to severe traffic accidents. Additionally, centralized data storage in cloud computing environments may lead to privacy breaches and unauthorized use of personal data. When building V2X networks, manufacturers must balance cost reduction, user experience optimization, and the protection of privacy, security, and data integrity. Moreover, large-scale data exchanges between V2X devices and surrounding systems make the network particularly vulnerable to hacker attacks.

This paper focuses on the security aspects of 6G-V2X applications, addressing both vehicle safety issues caused by communication challenges and the network security concerns arising from the characteristics of the technology itself. The former includes problems such as signal interference and information complexity, while the latter involves large-scale user data transmission and identity verification issues. Blockchain-based distributed ledger technology can significantly enhance security management in 6G-V2X communication, but due to its need for real-time data processing, it must be integrated with low-latency 6G algorithms. The second section will review the mature technologies that help address V2X security issues and emerging communication technologies in development, discussing their progress, advantages, and challenges. The third section will predict the potential bottlenecks and key issues that may arise in the development of V2X under 6G. The fourth section will summarize the new technologies and advantages brought by 6G-V2X in the context of the development of V2X networks.

2. G-V2X security technological developments

2.1. Intelligent reflective surface (IRS)

IRS is considered a promising technology for providing an intelligent and reconfigurable radio transmission environment for 6G systems. An IRS is a two-dimensional plane made up of numerous passive reflective elements, with each element capable of independently controlling the amplitude and phase of incoming signals. This technology can fundamentally address issues such as wireless channel attenuation and interference, providing high availability and fault tolerance for 6G-V2X systems, thus enhancing their security.

In 6G-V2X applications, IRS can overcome issues like channel blockage, Doppler effects, and improve positioning accuracy and safety. It can create virtual line-of-sight links in obstructed environments, bypassing obstacles between transmitters and receivers, even under limited coverage conditions. Additionally, IRS can be used to suppress or eliminate interference between co-channel or neighboring cells, stabilizing the channel and improving road safety for vehicular networks. This makes IRS particularly beneficial in environments with multiple obstacles or obstructed traffic roads. For example, IRS can be installed on roads far from intersections or on building surfaces to mitigate the signal attenuation problem in vertical street communications under 6G-V2X [3]. Due to its two-dimensional structure, IRS is easy to deploy and can be dynamically reconfigured. By adjusting the phase and amplitude of the emitted signals, it can maximize the energy directed toward legitimate receivers and even counteract eavesdropping signals, enhancing the physical layer security of communication [4].

The key security challenges of integrating IRS with 6G-V2X environments include:

1. Addressing signal interference caused by spectrum sharing in complex environments, ensuring safe operation of multiple elements without mutual interference, and optimizing system management strategies and algorithms.
2. IRS utilizes discrete beamforming for network optimization [5], requiring suitable algorithms to handle signal degradation and displacement caused by obstacles, gusts, and other environmental factors.

DOI: 10.54254/2755-2721/149/2025.KL22727

3. IRS requires the stacking of numerous elements, which leads to high power consumption; thus, how to allocate energy efficiently in resource-constrained environments is a research-worthy direction.
4. For V2X communication enabled by IRS, determining the appropriate technical platform to meet critical tasks such as traffic management and decision-making remains an important challenge to address.

2.2. RF-VLC visible light communication

The new 6G-V2X system requires ultra-high transmission rates and low-latency reliability to maintain continuous service. However, traditional RF-based short-range vehicle communication is highly susceptible to interference in environments with high signal density, causing transmission delays and blockages [6]. A promising alternative is the combination of RF and Visible Light Communication (VLC) in the 6G-V2X environment, which leverages the advantages of VLC in being immune to electromagnetic interference to assist radio communication. VLC based on Light Emitting Diodes (LEDs) can theoretically achieve ultra-high transmission rates, making it an ideal technology for vehicle network security in new environments, with potential deployment through street lights, traffic lights, and vehicle-mounted LEDs or Laser Diodes (LD).

The RF-VLC technology envisions networking through the installation of LEDs/LDs on vehicles, traffic lights, and roads to enable spatially coherent optical communication. This technology not only assists communication by increasing transmission rates but also overcomes certain communication limitations in complex environments, thereby enhancing transmission capabilities. For example, in high-density traffic, transmitting vehicles can use optical communication to send messages to nearby large vehicles, which then relay the information to vehicles in shadowed areas. Additionally, this technology aims to solve the issue of information transmission in vertical environments such as road intersections by using traffic lights as relay stations, thereby improving communication between vehicles on two intersecting streets and reducing data packet loss in traditional RF-V2X communication. This provides a solution to communication challenges in complex environments and ensures vehicle communication security in 6G-V2X systems.

Despite its advantages, combining RF and VLC presents some challenges, primarily related to the coordination between the two technologies and deployment planning. In certain outdoor environments, VLC communication may suffer from visible light interference, reducing communication performance. Moreover, due to the high mobility of vehicle network devices, changes in the channel and fluctuations in signal strength can also affect the stability of signal transmission [7].

2.3. Cloud computing-supported 6G-V2X vehicle communication

Under the Cloud-based Internet of Vehicles (CIOV) framework, the initial purpose of communication between vehicles in 6G-V2X systems was to address safety requirements through periodic message exchanges with nearby vehicles. With the rapid development of cloud computing, cloud storage, and related technologies, 6G-V2X enables vehicles to offload heavy computational tasks to more powerful cloud systems, alleviating resource consumption on the vehicle side. Vehicles collect data, report it to the cloud, and conduct cloud-based analysis in collaboration with other vehicles, ensuring safety while maintaining high accuracy. Additionally, in complex traffic situations, drivers can request remote assistance from the cloud for assisted driving, or under certain conditions, cloud systems can take over the vehicle's control, further leveraging the communication advantages of 6G-V2X to ensure safe driving.

DOI: 10.54254/2755-2721/149/2025.KL22727

Although cloud computing and vehicular networks have been developed for many years, the integration of both still faces several challenges. The first issue is the operability of cloud operating systems. The cloud ecosystem includes not only vehicle clouds but also various entities such as road management departments, service providers, and network operators. Cloud services require most data to be migrated to the cloud for processing, which necessitates the integration of security technologies like blockchain to ensure trust and security within the vehicular network, along with the creation of new service security frameworks and scheduling protocols. Furthermore, wireless resource allocation for cloud-based vehicular networks is highly complex [8]. Due to the multi-access characteristics of cloud networks, vehicles can utilize various network resources. However, given the high mobility of vehicles and frequent network handovers, a unified solution framework is still lacking.

Another critical issue is the security and privacy of vehicle cloud networks. Since vehicles generate a large amount of sensitive data and transmit it to surrounding vehicles and the cloud, developers must ensure proper handling of this data and store it in private clouds. At the same time, cloud networks need to proactively prevent architectural conflicts and safeguard sensitive data from being tampered with or stolen [9].

2.4. Aerial platform-assisted communication

Satellite communication systems are widely used in positioning and remote sensing fields, and they are expected to be effectively applied for positioning purposes in 6G-V2X. UAV-based communication systems, as auxiliary communication tools for 6G-V2X, offer broad coverage, strong spatial flexibility, and significant cost-effectiveness [10]. By equipping UAVs with sensors and communication devices as relay stations, communication range can be extended, effectively enhancing communication capabilities.

Under 6G-V2X, aerial platforms can collect data on a broad scale, not just limited to specific users. UAVs can simultaneously share data with multiple parties and manage wireless networks, helping drivers maintain safety while assisting traffic management departments in monitoring traffic flow and performing scheduling. In emergency situations, aerial platforms can quickly issue warnings and rapidly reach the accident scene to provide communication support, constantly monitoring violations and potential hazards to improve safety. As a potential technology for 6G-V2X, satellites can maintain secure communication between vehicles and remote data servers in areas beyond ground coverage.

Although aerial platform-supported 6G-V2X systems can enhance communication transmission rates to some extent, the challenge remains in addressing the high mobility of vehicular networks, particularly the dual mobility of UAVs and ground vehicles, which leads to highly dynamic channel characteristics that are difficult to solve.

3. Future technological directions

3.1. Terahertz communication

The introduction of terahertz (THz) communication alleviates the issue of spectrum scarcity, greatly enhancing network capacity [11], and with its high throughput, it makes many V2X application scenarios possible. THz communication can offer data rates up to 1 Tbps and enormous bandwidth, solving the problem of massive data transmission between vehicles without requiring more device connections, and can be applied under onboard conditions.

However, despite the new capabilities brought by the THz spectrum, it faces many challenges, especially in the 6G-V2X environment. The high-frequency THz spectrum suffers from high free-space path loss, making it suitable only for short-distance V2X communication. A potential solution is to design THz communication systems with high directional gain transceiver nodes using numerous

DOI: 10.54254/2755-2721/149/2025.KL22727

antennas to offset the extensive path loss. Additionally, due to the much shorter wavelength of THz waves, it is more feasible to pack numerous antennas at higher frequencies compared to microwave antennas.

3.2. Quantum computing/communication

Quantum computing, as one of the most transformative technologies, is still in its early stages of development and remains far from practical application. As mentioned in [12], quantum computing and quantum communication are expected to enter the 6G communication field towards the end of 6G development and have the potential to enhance 6G-V2X applications.

Quantum computing is anticipated to significantly enhance the security of 6G-V2X. In quantum encryption, the entanglement property of quantum systems prevents malicious attacks, as any attempt to eavesdrop or tamper with data would be immediately detected. Additionally, quantum computing ensures secure and unbreakable exchange and sharing of quantum keys. Quantum computing will also provide powerful computational capabilities to process and analyze the massive data generated by V2X, solving optimal path problems that traditional computing cannot address [13].

However, quantum computers currently only operate in extremely low-temperature environments, and using them stably in vehicles presents a major challenge for quantum computing chip research. Moreover, the application of quantum computing lacks the necessary architectural designs, particularly regarding security protocols used to protect V2X devices from attacks and the decryption of encrypted security protocols.

3.3. Blockchain technology

In the 6G-V2X vision, entities connected to vehicles not only provide useful data but also introduce unprecedented risks. Vehicles must contend with a variety of intrusions from different entities, which are diverse and dynamic in nature. Blockchain, as a decentralized and distributed digital ledger, was originally used in the Bitcoin cryptocurrency network [14] and is now considered a disruptive technology that can enhance security compared to traditional technologies by removing the need for other security and privacy services.

With the integration of blockchain technology, 6G-V2X communication can implement distributed security management, reducing computational burdens. By encrypting most of the communication processes with blockchain, third parties find it difficult to decrypt key information, thus protecting the sender's privacy while verifying the authenticity of messages in 6G-V2X [15]. Blockchain's ability to manage unlicensed spectrum allows users to share the same spectrum, offering a low-cost, efficient, secure, and decentralized spectrum-sharing mechanism [16].

Although attempts have been made to implement blockchain-based communication networks, they are not well-suited for V2X due to the dynamic nature of the network and the real-time data processing requirements. Despite blockchain's immense potential to enhance security and network management, it still faces high latency issues.

3.4. Artificial intelligence

With the continuous advancement of artificial intelligence (AI), many new technologies, such as autonomous driving and voice assistants, have become possible. This makes machine learning (ML) an essential component for the future development of 6G vehicular networks. By enhancing V2X with intelligent computing and machine learning, vast amounts of data can be processed quickly, and potential changes in the vehicular environment can be predicted, enabling predictions about other vehicles' movements [17] and addressing the risks faced by traditional communication systems that struggle to model precise channel estimates.

DOI: 10.54254/2755-2721/149/2025.KL22727

In future autonomous driving systems, AI algorithms can analyze data in real-time, combining various algorithmic designs to achieve high safety levels. For example, regression algorithms can provide a positioning solution for autonomous vehicles, while decision matrix algorithms will help identify, analyze, and assess the relationship between information and decisions. Machine learning (ML) can also help vehicles make decisions based on end-to-end learning methods and assist in the prediction of road safety indices (Si) through visual analysis and city feature recognition.

The future integration of V2X and ML signals advances in information transmission efficiency and accuracy. Machine learning will enhance vehicle network performance and interact with other internet applications surrounding the vehicle. Given the complex environment of V2X, the future development of collaborative applications such as 3D object visualization and 4D perception, using resource data integration, may become an intriguing research direction [18].

4. Challenges in 6G-V2X security

4.1. Trust and verification mechanisms in data centers

Data centers ensure the security of data communication through trust and auditing mechanisms. These mechanisms are intended to protect the privacy of vehicle data from network threats and attacks. However, the lack of unified authentication standards and mechanisms currently hinders further enhancement of the security performance of vehicular networks [19].

4.2. High dynamics and delay constraints

Mobility management is a key function in traffic systems, aiming to effectively track and monitor vehicles. V2X data packets often carry specific temporal and spatial meanings. 6G communication technology could offer alternative solutions to mobility issues, by designing vehicle communication protocols that provide stable and low-latency performance despite constraints such as vehicle speed, unstable links, and rapidly changing network topologies [20].

4.3. Security and privacy solutions in the internet of vehicles (IoV)

In the IoV, vehicles equipped with intelligent sensors and Internet of Things (IoT) devices gather environmental information and transmit sensor data to remote computing devices for further analysis using advanced communication technologies. This information helps with secure navigation, obstacle detection, route optimization, and traffic management. A major issue with vehicle data is its vulnerability, making it crucial to develop effective strategies and protocols to ensure security, trust, and privacy, and to protect vehicle data from malicious entities. Given the numerous connected devices on vehicles that have direct access to sensitive information, ensuring the security and privacy of transmitted data is a significant challenge [21-22].

5. Conclusion

This paper highlights the significant advancements in vehicular network security enabled by 6G-V2X technology. It introduces revolutionary elements compared to 5G-V2X. Furthermore, the paper outlines potential issues that might arise with the new generation of 6G-V2X technology and categorizes these technologies into mature and emerging stages. It provides insights into technological progress, identifies pressing challenges, and predicts possible development directions. This article aims to offer useful insights for those interested in 6G-V2X security issues, encouraging further research and discussions on related technologies.

DOI: 10.54254/2755-2721/149/2025.KL22727

References

[1] M.Giordani,M.Polese,M.Mezzavilla,S.Rangan,andM.Zorzi,"Toward 6Gnetworks: Use cases and technologies," IEEE Commun. Mag., vol. 58, no. 3, pp. 55–61, Mar. 2020

[2] U. M. Malik, M. A. Javed, S. Zeadally, and S. U. Islam, "Energy efficient fog computing for 6G enabled massive I oT: Recent trends and future opportunities," IEEE Internet Things J., to be published, doi: 10.1109/JIOT.2021.30 68056.

[3] Exploring Sum Rate Maximization in UAV-based Multi-IRS Networks: IRS Association, UAV Altitude, and Phase Shift Design\nDOI:10.1109/TCOMM.2022.3206884

[4] Z. Ji, X. Guan, J. Tu, Q. Wu and W. Yang, "Robust Trajectory and Communication Design in IRS-Assisted UAV C ommunication under Malicious Jamming," 2022 IEEE International Conference on Communications Workshops (ICC Workshops), Seoul, Korea, Republic of, 2022, pp. 1023-1028, doi: 10.1109/ICCWorkshops53468.2022.9814 480.

[5] W. U. Khan et al., "Opportunities for Intelligent Reflecting Surfaces in 6G Empowered V2X Communications," in IEEE Internet of Things Magazine, vol. 7, no. 6, pp. 72-79, November 2024, doi: 10.1109/IOTM.001.2300096.

[6] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo,"Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks," IEEE Transactions on Network Science and Engineering, Aug. 2019.

[7] A. Memedi and F. Dressler, "Vehicular visible light communications: A survey," IEEE Commun. Surveys Tuts.,vol. 23, no. 1, pp. 161–181, Oct. 2020.

[8] Y. Tang, N. Cheng, W. Wu, M. Wang, Y. Dai, and X. Shen, "Delay-minimization routing for heterogeneous VANETs with machine learning based mobility prediction," IEEE Trans. Veh. Technol.,vol. 68, no. 4, pp. 3967–3979, Apr. 2019.

[9] Q. Jiang, J. Ni, J. Ma, L. Yang, and X. Shen,"Integrated authentication and key agreement framework for vehicular cloud computing," IEEE Netw.,vol. 32, no. 3, pp. 28–35, May/Jun. 2018.

[10] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam and M. Debbah, "A Tutorial on UAVs for Wireless Networks: Applications Challenges and Open Problems", IEEE Communications Surveys & Tutorials, 2019.

[11] Y. Yuan, Y. Zhao, B. Zong, and S. Parolari,"Potential key technologies for 6G mobile communications," Sci. China Inf. Sci.,vol. 63,no. 8, Aug. 2020, Art. no. 183301.

[12] Post-Quantum_Era_in_V2X_Security_Convergence_of_Orchestration_and_Parallel_Computation

[13] P.Botsinis et al.,"Quantum search algorithms for wireless communications," IEEE Common. Surveys Tuts.,vol. 21, no. 2, pp. 1209–1242, Apr. 2019.

[14] Nakamoto et al., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[15] X. Wang et al., "An improved Authentication Scheme for Internet of Vehicles Based on Blockchain Technology," IEEE Access, vol. 7, 2019, pp. 45,061–072.

[16] Z. Zhang et al.,"6G wireless networks: Vision, requirements, architecture, and key technologies," IEEE Veh. Technol. Mag.,vol. 14, no. 3, pp. 28–41, Sep. 2019.

[17] E. S. A. Ahmed and R. A. Saeed, "A survey of big data cloud computing security," International Journal of Computer Science and Software Engineering (IJCSSE), vol. 3, no. 1, pp. 78–85, 2014.

[18] H. Wu, "Developing vehicular data cloud services in the IoT environment," IEEE Transactions on Industrial

[19] Informatics, vol. 10, no. 2, pp. 1587–1595, 2014.

[20] H. Wu, "Developing vehicular data cloud services in the IoT environment," IEEE Transactions on Industrial Informatics, vol. 10, no. 2, pp. 1587–1595, 2014.

[21] H. F. Salama, D. S. Reeves and Y. Viniotis, "A distributed algorithm for delay-constrained routig", IEEE/ACM Transactions on Networking, vol. 8, no. 2, pp. 84, 1997.

[22] S. Woo, H. J. Jo and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle can", IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 2, pp. 993-1006, 2015.