ISSN: 2688-8645

The Key Technologies in Collaborative Communication for Internet of Vehicles Systems

Siyuan Fu[1], Bingyi Dong[2], Kaipeng Sun[2]

[1]School of Chemistry & Chemical Engineering, Henan University of Science and Technology, China

[2]College of Information Engineering, Henan University of Science and Technology, China

Abstract

Collaborative communication technology in the Internet of Vehicles (IoV) is a key component of intelligent transportation systems and has garnered widespread attention in recent years. It involves information sharing between vehicles, vehicles and infrastructure, vehicles and pedestrians, and vehicles and networks, aiming to enhance traffic management and optimization. With the advancement of 5G and the upcoming 6G technologies, IoV systems face demands for low latency, high reliability, and security, and the standardization process continues to deepen. Physical Layer Security (PLS) leverages channel characteristics to enhance communication confidentiality, addressing the limitations of traditional encryption techniques. Reconfigurable Intelligent Surfaces (IRS), as an emerging technology, optimize communication performance by dynamically adjusting signal reflections, particularly improving system performance in signal-degraded environments. Furthermore, resource optimization strategies, such as deep learning and algorithm optimization, further enhance the communication efficiency and reliability of IoV systems. In the future, the integration of these technologies will drive the development of IoV towards more efficient, intelligent, and secure systems.

Keywords

Internet of Vehicles Systems; The Key Technologies in Collaborative Communication; Reconfigurable Intelligent Surfaces.

1. Introduction

As shown in Fig. 1, Collaborative communication technology in the Internet of Vehicles (IoV) is a core component of intelligent transportation systems, aimed at optimizing traffic flow, enhancing traffic safety, reducing energy consumption, and ultimately achieving efficient traffic management through information exchange between vehicles (V2V), vehicles and infrastructure (V2I), vehicles and pedestrians (V2P), and vehicles and networks (V2N) [1]. With the integration of technologies such as the Internet of Things (IoT), cloud computing, and artificial intelligence, IoV communication systems can not only enable real-time traffic updates, emergency event responses, and traffic signal optimization but also store, process, and analyze large-scale data through cloud services, further enhancing system intelligence and response speed.

However, the widespread deployment of IoV communication systems also presents numerous technical challenges, particularly regarding communication security, resource allocation, and signal transmission efficiency. While traditional encryption techniques provide certain levels of security, their high computational complexity and resource consumption limit their applicability in resource-constrained devices. The introduction of Physical Layer Security (PLS) offers a novel communication security solution for IoV systems [2-3]. PLS enhances communication confidentiality by exploiting the inherent characteristics of wireless channels,

ISSN: 2688-8645

compensating for the shortcomings of traditional key-based encryption methods. At the same time, Reconfigurable Intelligent Surfaces (IRS), as an emerging technology, significantly improve communication system performance by precisely controlling signal reflection paths, offering substantial advantages in long-distance communication or environments with severe signal attenuation [4].

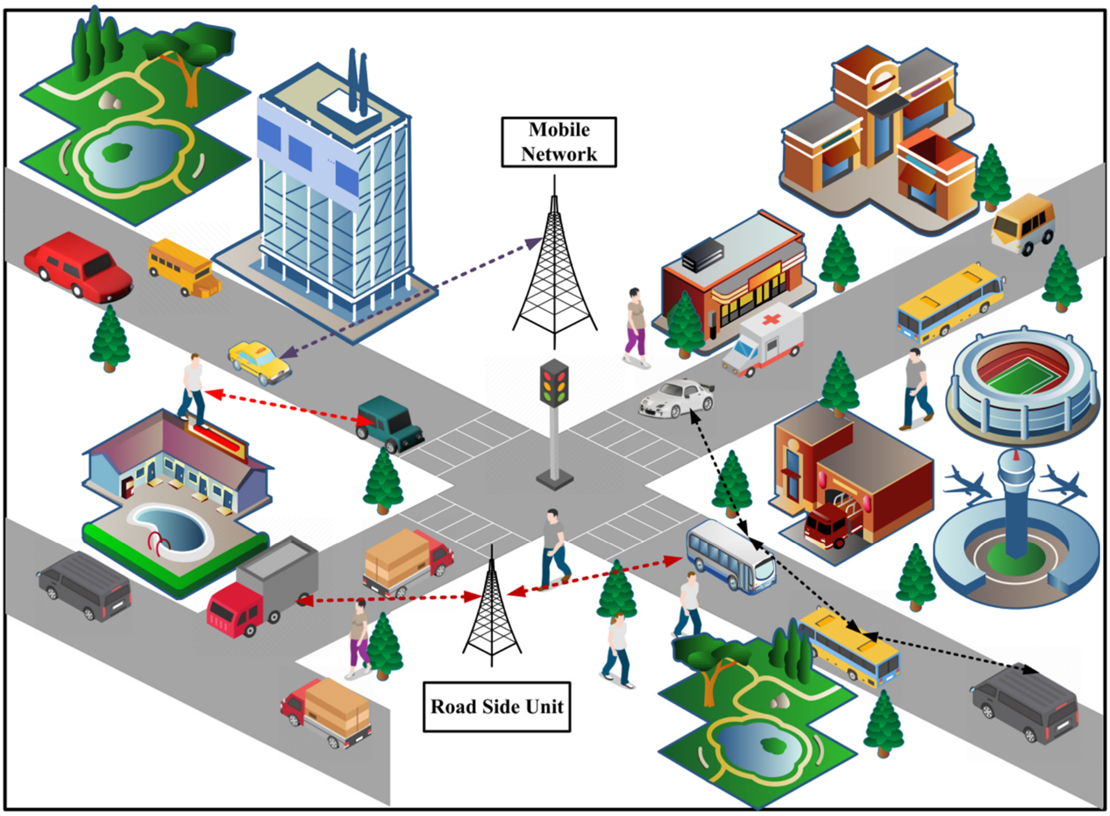

Fig 1. Scenarios of Collaborative Communication in the Internet of Vehicles

With the support of these two key technologies, resource optimization strategies for IoV systems have been continuously developed. Advanced algorithms such as deep learning and reinforcement learning are being applied to optimize spectrum utilization, power distribution, and link configuration, thereby improving the system's reliability and communication efficiency.

This paper will discuss the current research status of collaborative communication in IoV, the application of Physical Layer Security (PLS), and the use of Reconfigurable Intelligent Surfaces (IRS). The paper systematically reviews key technological advancements in IoV communication in recent years and explores future research directions. By summarizing and analyzing existing technologies, this paper aims to provide theoretical support and technical reference for the further development of IoV communication systems, driving the technology towards more efficient, intelligent, and secure solutions.

2. Current Research on Collaborative Communication in the Internet of Vehicles (IoV)

Collaborative communication in the Internet of Vehicles (IoV) refers to the interconnected communication between vehicles and various entities, including vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P), and vehicle-to-network (V2N). The goal is to enable real-time sharing and processing of traffic information, allowing vehicles

ISSN: 2688-8645

to access traffic data in real-time for intelligent traffic flow management and optimization, thereby improving traffic efficiency [5]. Research on collaborative communication in IoV is ongoing and focuses on solving complex technical challenges, such as dynamic traffic updates, emergency event responses, and traffic signal optimization, to enhance overall road operational efficiency. The integration of Internet of Things (IoT) and cloud computing technologies, along with cloud services for efficient storage, processing, and analysis of information between vehicles, further strengthens the intelligence of IoV communication systems.

Security in IoV collaborative communication is another critical issue that requires urgent attention [6]. Collaboration between vehicles relies on road condition sensing for information sharing, enabling real-time traffic updates to help drivers avoid accidents and congestion. Researchers are committed to developing secure communication protocols and mechanisms to prevent malicious attacks on vehicle networks and ensure the safety of communication between vehicles and infrastructure.

To address these challenges, international standards organizations and industry players are actively collaborating to promote global standardization and technological innovation in IoV communications [7]. This collaboration has contributed to the formulation and implementation of related standards, ensuring global interoperability of IoV technologies. Cellular-based IoV technologies have also undergone a crucial standardization process, with the introduction of two communication modes in 3GPP Release 14 to optimize V2V communication: Mode 3 (centralized resource scheduling) and Mode 4 (distributed resource scheduling) [8]. Release 15 further advanced the V2X service architecture by introducing two radio interfaces, Uu and PC5. These interfaces enhance V2I link connectivity and enable direct short-range communication for V2V links, providing reliable communication solutions that support both long-range and broad-area coverage for IoV systems [9]. The Uu interface connects vehicles with base stations for long-range communication, while the PC5 interface facilitates short-range direct communication between vehicles, people, and infrastructure. In 3GPP Release 16, several new use cases and requirements were introduced to enhance 5G-V2X technology, such as high-rate vehicle-to-base station entertainment services and high-rate dynamic map updates between vehicles and the cloud [10]. By leveraging 5G-V2X technology, intelligent traffic management systems can meet the Quality of Service (QoS) requirements for V2V and V2I communications, including low transmission latency, high reliability, high data throughput, bandwidth efficiency, and security and privacy protection. Through these standardization efforts, V2X technology not only enhances its application potential in intelligent transportation systems but also opens new possibilities for the future development of IoV, contributing to the creation of safer and smarter road environments.

Jameel et al. proposed a network model for C-V2X communication that addresses resource constraints and low energy efficiency by utilizing roadside objects to charge and process information using radio frequency signals from electric vehicles [11]. He et al. introduced a decentralized resource allocation mechanism based on deep reinforcement learning for V2V communication. By applying a distributed resource allocation strategy and reinforcement learning, they ensure mutual cooperation between vehicles while satisfying V2V link reliability, achieving optimal subband selection and power transmission [12]. Sun et al. used ant colony optimization to find the optimal routing path in multi-hop links at urban intersections [13]. Jie Tian et al. proposed a multi-agent deep deterministic policy gradient algorithm to address ultra-reliable and low-latency requirements in V2V links. They created a multi-criteria objective function model based on utility maximization to solve delay sensitivity and capacity reliability issues in V2V communication, enhancing delay sensitivity and capacity reliability in IoV systems [14]. Most of these studies focus on improving link reliability and reducing communication latency by utilizing resource optimization strategies. Wang et al. addressed security issues in frequency sharing networks between vehicles by maximizing the security throughput of cellular users as the optimization objective, enhancing security performance using interference caused by end-to-end users [15]. Cheng et al. introduced Reconfigurable Intelligent Surfaces (IRS) to maximize the total capacity of the link between vehicles and infrastructure [16]. Zhang et al. developed a three-dimensional GNSS-based cooperative positioning model to address the performance degradation in urban environments caused by signal blockage and reflections, improving collaboration accuracy with V2X technology [17]. Lin et al. optimized power distribution and selection for video frame transmission in IoV based on matching theory to ensure low-latency, high-accuracy road information acquisition for autonomous driving [18]. These studies demonstrate how the integration of various technologies improves the overall collaboration and communication efficiency of IoV systems.

3. Current Research on Physical Layer Security (PLS)

Physical Layer Security (PLS) has been widely recognized as a reliable and effective approach to addressing security challenges, complementing the limitations of traditional key encryption techniques. The security of key encryption mainly depends on the computational complexity and difficulty of breaking the encryption [19], leading to high computational resource demands and increased communication latency. This is particularly problematic for resource-constrained devices, where the energy consumption required for encryption can limit its applicability [20]. In contrast, PLS exploits the inherent characteristics of wireless signal propagation, such as random fluctuations, path fading, environmental noise, and other potential interferences, to increase the difficulty for unauthorized receivers to decode information while ensuring that authorized users can receive data without error.

PLS offers a flexible and customizable security solution for wireless communication systems by dynamically adjusting resource allocation and link configuration based on real-time channel conditions. This not only strengthens the confidentiality of information transmission but also enables system designers to effectively address evolving security threats and communication environments. From an information-theoretic perspective, PLS provides a novel approach to addressing communication security issues [21]. In collaborative communication technologies, PLS can also enhance wireless communication security by leveraging channel diversity, and through cooperation among multiple nodes, it further increases the difficulty for illegal eavesdroppers to intercept signals [22].

The research scope of PLS is extensive, covering areas such as physical layer key generation and authentication techniques [23], anti-eavesdropping channel coding design [24], multi-antenna technologies [25], artificial noise [26], and security-enhanced relay cooperative communication [27]. Thanh V. Pham et al. studied PLS design in visible light communication systems using artificial noise-assisted precoding in the presence of multiple eavesdroppers [28]. Wang H et al. explored the potential of PLS in millimeter-wave multiple-input multiple-output (MIMO) systems [29]. Yerrapragada et al. proposed a key-based PLS protocol to ensure low latency and high security in wireless systems [30]. Wang C et al. researched PLS in artificial noise-assisted C-V2X networks [31]. Jangsher et al. introduced an efficient PLS protocol for secure communication in distributed drone clusters [32]. Sheng et al. studied a new information and artificial noise transmission scheme, where drones send confidential information to users in one time slot and transmit artificial noise in the next, optimizing time allocation, bandwidth, and power to maximize users' secrecy rates [33]. He et al. proposed a low-complexity phased array PLS scheme for millimeter-wave V2X applications based on twisted pair cabling [34]. Yun Ai et al. utilized Reconfigurable Intelligent Surfaces (IRS) to ensure secure vehicular communication in the presence of eavesdroppers, demonstrating that IRS can enhance confidentiality in V2V and V2I communications [35]. These studies primarily focus on optimizing system design to achieve the best secure communication strategies. The research

ISSN: 2688-8645

framework for PLS in recent years, as shown in Figure 1-2, mainly includes three parts: foundational theory, performance analysis, and application areas.

The primary strategy for achieving physical layer security is to reduce the signal-to-noise ratio (SNR) at the eavesdropper or increase the SNR at the legitimate user to ensure a positive secrecy rate [36]. Based on information theory, by exploring secrecy capacity and coding techniques, messages can be transmitted without being decoded by any eavesdropper. The research on information-theoretic security has expanded into various aspects. Leung et al. studied Gaussian eavesdropping channels, noting that secrecy capacity is the difference between the main channel and the eavesdropper's channel capacity [37]. Barros et al. investigated the security capacity in slow fading channels, introducing the concept of interruption into the security problem for the first time [38]. Orthogonal Frequency Division Multiple Access (OFDMA) efficiently transmits multiple flows of data by optimizing power, subcarriers, and bit allocation across different users. A large body of research has focused on resource allocation in downlink networks using OFDMA. For example, Wang et al. proposed a PLS optimization model that fine-tunes end-to-end user access strategies to optimize network resource allocation [39]. Wang W et al. discussed security issues in end-to-end spectrum-sharing networks, improving cellular user security by exploiting interference generated by end-to-end users [40]. Liu et al. proposed a secure cellular-based V2V communication scheme for wireless resource and functionality management, deriving closed-form optimal power distribution expressions in interference-limited and noise-limited scenarios to maximize the secrecy rate of V2V links [41]. The goal of subcarrier allocation strategies is to find the optimal spectrum utilization plan to improve system spectral efficiency and security performance. Adaptive power distribution, which dynamically adjusts transmission power based on the communication environment, achieves the best balance between confidentiality and communication quality.

4. Current Research on Reconfigurable Intelligent Surfaces (IRS)

Due to the randomness of wireless environments, signal propagation often undergoes reflection, diffraction, and scattering before reaching the receiver, resulting in random attenuation and delay of the signal along different paths. This channel fading effect has become a primary limiting factor in maximizing wireless network energy efficiency (EE) [42] and spectral efficiency (SE) performance. Traditional wireless network optimization paradigms can no longer fully meet the three major application scenarios of 5G, namely enhanced mobile broadband, ultra-reliable low-latency communication, and machine-type communication. Future mobile networks must not only address human-to-human communication but also provide users with immersive experiences, such as augmented reality, virtual reality, and ultra-high-definition (3D) video. Moreover, they must solve communication issues between humans and things, as well as things-to-things, to meet the requirements of IoT applications like mobile healthcare, IoV, smart homes, industrial control, and environmental monitoring. Hence, new solutions need to be found to overcome these challenges.

The IRS technology consists of a large number of passive scattering units, each designed with special physical structures. These units can change the electromagnetic characteristics (such as phase) of the reflected signal via software-defined methods. The reflection phase of the incident signal can be adjusted arbitrarily, enabling precise control of the reflected signal's propagation direction. The reflected RF signal can be coherently combined to enhance the received signal power or destructively combined to mitigate interference [43]. By introducing IRS technology into wireless communication environments, the reconfigurability of IRS can improve wireless network transmission performance, providing new ideas for the development of wireless communications.

Wu et al. studied IRS-assisted wireless communication systems, deriving closed-form expressions for approximately optimal solutions to maximize energy efficiency in line-of-sight (LoS) channels [44]. Tang et al. employed an alternating optimization algorithm to jointly optimize base station beamforming vectors, IRS reflection phase matrices, and power distribution ratios to maximize system energy efficiency [45]. Kang et al. investigated the use of passive IRS technology and designed groupings of IRS elements to maximize spectral efficiency [46]. Rehman et al. maximized user spectral efficiency by minimizing the total mean square error of user-received symbols [47]. Khan et al. utilized IRS to enhance the physical layer security of UAV networks, applying alternating optimization to maximize the secrecy capacity of IRS-enhanced UAV scenarios in the presence of multiple eavesdroppers [48].

IRS effectively reduces signal fading [49], enhances signal strength [50], and improves signal coverage by precisely controlling the reflection path of wireless signals. Additionally, IRS can significantly enhance wireless network performance without increasing additional transmission power and spectrum resources. Shi et al. verified that distributed IRS in millimeter-wave cellular networks could enhance network coverage and improve system performance [51]. In high-density network environments, IRS can dynamically adjust the state of its reflective elements to provide customized signal enhancement or interference suppression for different users, thus meeting diverse service requirements. Xu et al. proposed an interference alignment strategy using a minimal interference leakage criterion and an enhanced Riemann conjugate gradient algorithm for IRS-assisted multi-user multiple-output systems, ensuring maximum sum rate while satisfying a given minimal interference leakage threshold [52]. Li et al. introduced a novel IRS-assisted wireless communication and energy transmission non-orthogonal multiple access network architecture, optimizing base station transmission power using a two-stage algorithm [53].

Moreover, IRS can dynamically adjust the phase and amplitude of reflected signals to compensate for Doppler frequency shifts. Thomas et al. proposed a delay-Doppler domain IRS-assisted Orthogonal Time Frequency Space (OTFS) system architecture, where the reconfigurability of IRS units significantly alleviated multipath fading effects in high-Doppler channels. They demonstrated that IRS had significant advantages in non-line-of-sight (NLoS) urban and high-Doppler frequency shift wireless communication scenarios [54].

As one of the key technologies for next-generation wireless communication networks, IRS shows great potential in overcoming the existing network performance limitations and leading the future development of communication technologies. Especially in long-range communications or environments with severe signal attenuation, strategically deploying IRS can effectively solve issues like signal blind spots, signal attenuation, and adjacent interference. For example, if an IRS is deployed between a base station and a user, it can intelligently reflect signals and bypass physical obstacles, forming a virtual line-of-sight (LoS) path between them, effectively expanding the coverage of the base station's signal. It is worth noting that each IRS unit can independently adjust the reflection phase of the signal, thereby enhancing the strength of the signal received by edge users and effectively reducing the interference impact from nearby areas, significantly improving overall communication efficiency.

Yang et al. proposed a practical channel estimation transmission protocol that utilizes the correlation of channel transmission to group IRS elements and share reflection coefficients, thus reducing training overhead [55]. Evmorfos et al. modeled the optimization objective as a Markov process and used reinforcement learning algorithms to solve the problem of traditional non-convex optimization becoming convex [56]. Sweta et al. studied beam steering in a dual-function radar and communication system with MIMO support, using IRS to optimize radar and beam steering to enhance secure communication while maintaining link service quality through simulations [57].

ISSN: 2688-8645

5. Conclusion

In conclusion, collaborative communication technologies in the Internet of Vehicles (IoV) are pivotal to the evolution of intelligent transportation systems. As IoV faces the demands of low latency, high reliability, and security with the advent of 5G and future 6G technologies, the integration of advanced techniques like Physical Layer Security (PLS) and Reconfigurable Intelligent Surfaces (IRS) has shown significant potential in improving both communication security and system performance. PLS offers a novel approach to enhance the confidentiality of communications by exploiting the natural characteristics of wireless channels, while IRS improves signal propagation and optimizes network performance, particularly in challenging environments with severe signal attenuation.

The ongoing research in IoV collaborative communication technologies is critical for realizing the future of smart, autonomous, and secure transportation systems. As technologies continue to evolve and converge, the prospects for IoV systems to achieve greater efficiency, intelligence, and security will further expand, providing the groundwork for more effective traffic management, enhanced user experience, and a safer transportation environment.

References

[1] Noor-A-Rahim Md, Liu Z, Lee H, et.al. 6G for Vehicle-to-Everything (V2X) Communications: Enabling Technologies, Challenges, and Opportunities[J]. Proceedings of the IEEE, 2022, 110(6): 712-734.

[2] Abolade O, Okandeji A, Oke A, et al. Overhead effects of data encryption on TCP throughput across IPSEC secured network[J]. Scientific African, 2021, 13: e00855.

[3] Sánchez J D V, Urquiza-Aguiar L, Paredes M C P, et al. Survey on physical layer security for 5G wireless networks[J]. Annals of Telecommunications, 2021, 76(3-4): 155-174.

[4] Wu Q, Zhang S, Zheng B, et.al. Intelligent Reflecting Surface-Aided Wireless Communications: A Tutorial[J]. IEEE Transactions on Communications, 2021, 69(5): 3313-3351.

[5] Sehla K, Nguyen T M T, Pujolle G, et.al. Resource Allocation Modes in C-V2X: From LTE-V2X to 5G-V2X[J]. IEEE Internet of Things Journal, 2022, 9(11): 8291-8314.

[6] Jameel F, Javed M A, Zeadally S, et.al. Secure Transmission in Cellular V2X Communications Using Deep Q-Learning[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(10): 17167-17176.

[7] Garcia M H C, Molina-Galan A, Boban M, et.al. A Tutorial on 5G NR V2X Communications[J]. IEEE Communications Surveys Tutorials, 2021, 23(3): 1972-2026.

[8] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Study on LTE-based V2X Services; (Release 14), 3GPP TR 36.885 V14.0.0, 2016.

[9] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for V2X services; (Release 15), 3GPP TR 23.285 V15.1.0, 2019.

[10] Cao X, Liu L, Cheng Y, et.al. Towards Energy-Efficient Wireless Networking in the Big Data Era: A Survey[J]. IEEE Communications Surveys & Tutorials, 2018, 20(1): 303-332.

[11] Jameel F, Khan W U, Kumar N, et.al. Efficient Power-Splitting and Resource Allocation for Cellular V2X Communications[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(6): 3547-3556.

[12] Liang L, Ye H, Li G Y. Spectrum Sharing in Vehicular Networks Based on Multi-Agent Reinforcement Learning[J]. IEEE Journal on Selected Areas in Communications, 2019, 37(10): 2282-2292.

[13] Sun G, Zhang Y, Yu H, et.al. Intersection Fog-Based Distributed Routing for V2V Communication in Urban Vehicular Ad Hoc Networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 21(6): 2409-2426.

[14] Tian J, Liu Q, Zhang H, et.al. MultiAgent Deep-Reinforcement-Learning-Based Resource Allocation for Heterogeneous QoS Guarantees for Vehicular Networks[J]. IEEE Internet of Things Journal, 2022, 9(3): 1683-1695.

ISSN: 2688-8645

[15] Wang P, Di B, Zhang H, et.al. Cellular V2X Communications in Unlicensed Spectrum: Harmonious Coexistence with VANET in 5G Systems[J]. IEEE Transactions on Wireless Communications, 2018, 17(8): 5212-5224.

[16] Chen Y, Wang Y, Zhang J, et.al. Resource Allocation for Intelligent Reflecting Surface Aided Vehicular Communications[J]. IEEE Transactions on Vehicular Technology, 2020, 69(10): 12321-12326.

[17] Zhang G, Ng H F, Wen W, et.al. 3D Mapping Database Aided GNSS Based Collaborative Positioning Using Factor Graph Optimization[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(10): 6175-6187.

[18] Lin J, Yang P, Zhang N, et.al. Low-Latency Edge Video Analytics for On-Road Perception of Autonomous Ground Vehicles[J]. IEEE Transactions on Industrial Informatics, 2023, 19(2): 1512-1523.

[19] Xiong H, Yao T, Wang H, et.al. A Survey of Public-Key Encryption With Search Functionality for Cloud-Assisted IoT[J]. IEEE Internet of Things Journal, 2022, 9(1): 401-418.

[20] Chhikara P, Tekchandani R, Kumar N, et.al. An Efficient Container Management Scheme for Resource-Constrained Intelligent IoT Devices[J]. IEEE Internet of Things Journal, 2021, 8(16): 12597-12609.

[21] Zhang N, Ai Y, Zhang D, et.al. Advances and Challenges in Physical Layer Security: A Comprehensive Review[C]//2023 International Conference on Ubiquitous Communication (Ucom). 2023: 83-87.

[22] Kumar Megha S, Ramanathan R, Jayakumar M. Key less physical layer security for wireless networks: A survey[J]. Engineering Science and Technology, an International Journal, 2022, 35: 101260.

[23] Jorswieck E, Tomasin S, Sezgin A. Broadcasting Into the Uncertainty: Authentication and Confidentiality by Physical-Layer Processing[J]. Proceedings of the IEEE, 2015, 103(10): 1702-1724.

[24] Oggier F, Solé P, Belfiore J C. Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis[J]. IEEE Transactions on Information Theory, 2016, 62(10): 5690-5708.

[25] Li M, Ti G, Liu Q. Secure Beamformer Designs in MU-MIMO Systems With Multiuser Interference Exploitation[J]. IEEE Transactions on Vehicular Technology, 2018, 67(9): 8288-8301.

[26] Ruby R, Pham Q V, Wu K, et.al. Enhancing Secrecy Performance of Cooperative NOMA-Based IoT Networks via Multiantenna-Aided Artificial Noise[J]. IEEE Internet of Things Journal, 2022, 9(7): 5108-5127.

[27] Jameel F, Wyne S, Kaddoum G, et.al. A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security[J]. IEEE Communications Surveys & Tutorials, 2019, 21(3): 2734-2771.

[28] Pham T V, Pham A T. Energy Efficient Artificial Noise-Aided Precoding Designs for Secured Visible Light Communication Systems[J]. IEEE Transactions on Wireless Communications, 2021, 20(1): 653-666.

[29] Wang H, Ju Y, Zhang N, et.al. Resisting Malicious Eavesdropping: Physical Layer Security of mmWave MIMO Communications in Presence of Random Blockage[J]. IEEE Internet of Things Journal, 2022, 9(17): 16372-16385.

[30] Yerrapragada A K, Eisman T, Kelley B. Physical Layer Security for Beyond 5G: Ultra Secure Low Latency Communications[J]. IEEE Open Journal of the Communications Society, 2021, 2: 2232-2242.

[31] Wang C, Li Z, Xia X G, et.al. Physical Layer Security Enhancement Using Artificial Noise in Cellular Vehicle-to-Everything (C-V2X) Networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(12): 15253-15268.

[32] Jangsher S, Al-Dweik A, Iraqi Y, et.al. Group Secret Key Generation Using Physical Layer Security for UAV Swarm Communications[J]. IEEE Transactions on Aerospace and Electronic Systems, 2023, 59(6): 8550-8564.

[33] Sheng Z, Tuan H D, Nasir A A, et al. Secure UAV-Enabled Communication Using Han–Kobayashi Signaling[J]. IEEE Transactions on Wireless Communications, 2020, 19(5): 2905-2919.

[34] He M, Ni J, He Y, et.al. Low-Complexity Phased-Array Physical Layer Security in Millimeter-Wave Communication for Cybertwin-Driven V2X Applications[J]. IEEE Transactions on Vehicular Technology, 2022, 71(5): 4573-4583.

[35] Ai Y, deFigueiredo F A P, Kong L, et.al. Secure Vehicular Communications Through Reconfigurable Intelligent Surfaces[J]. IEEE Transactions on Vehicular Technology, 2021, 70(7): 7272-7276.

[36] Hamamreh J M, Furqan H M, Arslan H. Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey[J]. IEEE Communications Surveys & Tutorials, 2019, 21(2): 1773-1828.

[37] Leung-Yan-Cheong S, Hellman M. The Gaussian wire-tap channel[J]. IEEE Transactions on Information Theory, 1978, 24(4): 451-456.

[38] Barros J, D. Rodrigues M R. Secrecy Capacity of Wireless Channels[C]//2006 IEEE International Symposium on Information Theory. 2006: 356-360.

[39] Wang L, Liu J, Chen M, et.al. Optimization-Based Access Assignment Scheme for Physical-Layer Security in D2D Communications Underlaying a Cellular Network[J]. IEEE Transactions on Vehicular Technology, 2018, 67(7): 5766-5777.

[40] Wang W, Teh K C, Li K H. Enhanced Physical Layer Security in D2D Spectrum Sharing Networks[J]. IEEE Wireless Communications Letters, 2017, 6(1): 106-109.

[41] Liu Y, Wang W, Chen H H, et.al. Secrecy Rate Maximization via Radio Resource Allocation in Cellular Underlaying V2V Communications[J]. IEEE Transactions on Vehicular Technology, 2020, 69(7): 7281-7294.

[42] Chen Y, Zhang B, Hu J, et.al. Analysis on Energy Efficiency of Large Scale Intelligent Reflecting Surface-Enabled Networks[J]. IEEE Communications Letters, 2023, 27(10): 2802-2806.

[43] Sun H, Zhao Z, Cheng H, et.al. IRS-Assisted RF-Powered IoT Networks: System Modeling and Performance Analysis[J]. IEEE Transactions on Communications, 2023, 71(4): 2425-2440.

[44] Peng Q, Wu Q, Chen G, et.al. Hybrid Active-Passive IRS Assisted Energy-Efficient Wireless Communication[J]. IEEE Communications Letters, 2023, 27(8): 2202-2206.

[45] Tang J, Peng Z, So D K C, et.al. Energy Efficiency Optimization for a Multiuser IRS-Aided MISO System With SWIPT[J]. IEEE Transactions on Communications, 2023, 71(10): 5950-5962.

[46] Kang Z, You C, Zhang R. Active-Passive IRS aided Wireless Communication: New Hybrid Architecture and Elements Allocation Optimization[J]. IEEE Transactions on Wireless Communications, 2024: 1-1.

[47] Ur Rehman H, Bellili F, Mezghani A, et.al. Joint Active and Passive Beamforming Design for IRS-Assisted Multi-User MIMO Systems: A VAMP-Based Approach[J]. IEEE Transactions on Communications, 2021, 69(10): 6734-6749.

[48] Khan W U, Lagunas E, Ali Z, et.al. Opportunities for Physical Layer Security in UAV Communication Enhanced with Intelligent Reflective Surfaces[J]. IEEE Wireless Communications, 2022, 29(6): 22-28.

[49] Huang Z, Zheng B, Zhang R. Transforming Fading Channel from Fast to Slow: IRS-Assisted High-Mobility Communication[M]. 2021.

[50] Wang X, Shu F, Shi W, et.al. Beamforming Design for IRS-Aided Decode-and-Forward Relay Wireless Network[J]. IEEE Transactions on Green Communications and Networking, 2022, 6(1): 198-207.

[51] Shi X, Deng N, Zhao N, et.al. Coverage Enhancement in Millimeter-Wave Cellular Networks via Distributed IRSs[J]. IEEE Transactions on Communications, 2023, 71(2): 1153-1167.

[52] Xu X, Ren H, Bao J, et.al. An Enhanced Interference Alignment Strategy With MIL Criterion and RCG Algorithm for IRS-Assisted Multiuser MIMO[J]. IEEE Communications Letters, 2023, 27(3): 1001-1005.

[53] Li Z, Chen W, Wu Q, et al. Joint Beamforming Design and Power Splitting Optimization in IRS-Assisted SWIPT NOMA Networks[M]. 2021.

[54] Thomas A, Deka K, Sharma S, et al. IRS-Assisted OTFS System: Design and Analysis[J]. IEEE Transactions on Vehicular Technology, 2023, 72(3): 3345-3358.

ISSN: 2688-8645

[55] Yang Y, Zheng B, Zhang S, et.al. Intelligent Reflecting Surface Meets OFDM: Protocol Design and Rate Maximization[J]. IEEE Transactions on Communications, 2020, 68(7): 4522-4535.

[56] Evmorfos S, Petropulu A P, Poor H V. Actor-Critic Methods for IRS Design in Correlated Channel Environments: A Closer Look Into the Neural Tangent Kernel of the Critic[J]. IEEE Transactions on Signal Processing, 2023, 71: 4029-4044.

[57] Sweta S, Dubey A, Nguyen V L. Efficient IRS-Aided Rate Optimizations for Dual Functional Radar and Communications[J]. IEEE Communications Letters, 2024, 28(1): 39-42.