ISSN 2616-5775 Vol. 6, Issue 7: 152-159, DOI: 10.25236/AJCIS.2023.060720

Discussion on the Application of Quantum Teleportation Technology in the Internet of Vehicles

Hongtao Yang*, Chunmei Chen, Benchao Liu

Department of Vehicle Engineering, Shandong Transport Vocational College, Weifang, Shandong, China
19445498@qq.com
**Corresponding author*

Abstract: *With the continuous progress of technologies such as lasers, electronics, and computers, their practical applications have also made great progress. Quantum Key Distribution (QKD) is currently one of the most promising quantum teleportation technologies and a hot topic in the field of secure communication. The purpose of this article was to study the application of quantum teleportation technology in the Internet of Vehicles (IoV). This article fully explained the concept, principles, and methods of quantum teleportation technology, deeply understood the absolute security attributes of quantum teleportation technology, and then pointed out its practical operability in the field of information security by introducing its development status and application prospects. Based on the security needs of the IoV and considering the shortcomings of existing security protection technologies, the risks of the IoV and the urgent need for high security of information technology were highlighted. A persistent and secure bidirectional authenticated QKD protocol was proposed, and simulation experiments were conducted on the NS-2.45 network simulation platform. The experimental results showed that the average time cost of this scheme was only 0.11 seconds when the number of vehicles was 10. Compared with other similar schemes, this scheme had lower overhead.*

Keywords: *Quantum Teleportation Technology, Quantum Key Distribution, Vehicle Networking Security, Bidirectional Authentication*

1. Introduction

The rapid development of technology has greatly changed people’s lives. While enjoying the convenience of information technology, people inevitably face the challenge of information security. How to reliably encrypt and transmit information has become an important issue related to every individual, every social unit, and even the entire national strategy. The security issue of the IoV is a hot topic of widespread concern in current society, and the requirements for IoV security have also increased accordingly. The IoV is closely related to people’s lives and property, and its safety is a fundamental function necessary for cars before they are put into use. Quantum teleportation technology is a product of the development of secure communication technology to a certain extent. It is gradually becoming a new type of secure communication technology. It is a new type of secure communication technology that can solve the problem of current communication technology methods being unable to ensure absolute information security. QKD technology is an important field for achieving the practicality of quantum secure communication technology, and it is gradually gaining the attention of governments around the world [1-2].

In recent years, with the in-depth research on quantum teleportation technology, more and more applications have begun to pay attention to quantum teleportation technology. It is a typical commercial medium that combines multiple Internet of Things devices with information communication technology to achieve information communication in a quantum system. In the future network, there would be new challenges in terms of large data transmission volume, low latency, broadband, security and privacy protection. Therefore, technological means such as quantum teleportation, quantum sensing, and quantum computing can effectively solve the above problems. In future intelligent advanced applications, data security is the most important requirement. SinghS K established a quantum teleportation model system. He explained how blockchain was applied to quantum computing and quantum encryption technology to ensure the security and confidentiality of the latest information sharing. In addition, he also discussed the international development trends in quantum teleportation technology in some countries such as the United States, Canada, the United Kingdom, and South Korea. Finally, he also explored several open research challenges faced by quantum teleportation technology in various fields such as the quantum internet and quantum computing [3]. In the era of mobile internet, car networking systems would face severe challenges. Fully leveraging the advantages of roadside storage devices enables pre buffering during off peak hours, thereby improving the quality of user experience. However, the existing content caching strategies for the IoV are difficult to effectively regulate the content in the IoV. In addition, there are security issues with several existing caching schemes. For this reason, Qian Y explored for the first time the technology of vehicle networking perception in a 5G environment. Subsequently, he utilized a perception engine to design a method to improve security. On this basis, combined with specific cases, a content caching mechanism based on perceived security and time delay sensitivity of the IoV was explored. The experimental results showed that his proposed algorithm had better performance compared to conventional caching methods [4]. Therefore, studying the application of quantum teleportation technology in vehicle networking has practical significance.

This project introduced the emerging quantum teleportation theory into automotive networks, which was not only a new exploration of the security of automotive networks, but also an exploration of quantum teleportation in automotive networks. As an emerging and rapidly developing technology, its strength lied in its integration and application with multiple disciplines. The research results of this project would promote the development and application of quantum teleportation technology in automotive networks.

2. Theoretical Basis of Quantum Teleportation and Vehicle Networking

2.1 Quantum Teleportation Technology

The non-cloning, superposition, and entanglement of quantum states are the key to achieving quantum secure communication. Generally, quantum states are described by state vectors in vector space. Quantum states can be either pure or mixed states, and the combination of different probabilities of many pure states forms a mixed state, and different combinations also form the same mixed state [5-6].

Quantum entanglement is a more mysterious phenomenon that describes the characteristics of entanglement between two particles. Despite being far apart, the behavior of one particle still affects the state of the other. If a particle is manipulated or measured, it would cause the state of the other particle to change, and the other particle would also undergo the opposite state change [7-8].

The quantum teleportation technology discussed in this article mainly refers to QKD. In theory, generating quantum keys through quantum teleportation technology and combining them with encryption and decryption algorithms can achieve absolute confidentiality [9-10]. Quantum secure communication is a new and highly comprehensive research field based on quantum mechanics and cryptography. With the increasing maturity of single photon detection and other technologies, achieving quantum secure communication in all optical networks is no longer unattainable in the field of daily communication [11].

2.2 QKD Protocol

QKD is one of the hottest topics in the field of quantum, and it is also the simplest and most realistic technology [12-13]. QKD relies on quantum physical properties to ensure its theoretical security and does not require strict restrictions on Eve. However, most QKD protocols require both individuals to have a certain level of quantum power, and quantum generation and manipulation devices often require millions of devices, which limits the choices of most people. Therefore, how to maximize the advantages of quantum encryption technology and extend it to a smaller scope has become a hot topic.

The first QKD protocol is called the BB84 protocol. In this protocol, for example, Alice and Bob share two communication channels: One is a quantum channel used to transmit quantum bits, generally referring to single photons with different polarization states; the second is the classical channel used to transmit classical information. In the BB84 protocol, Alice first generates a series of states in a random manner, and then transmits the photons in these states to Bob in a specific order and period. Bob randomly selected a set of measurement units to measure the photons emitted by Alice. Alice and Bob announced the metric basis they used in the classical channel. When Alice and Bob choose the same measurement basis, their bit values are also the same.

In the E91 protocol, when two qubits are assigned to two qubits, the two qubits are assigned to Alice and Bob, and Alice and Bob produce diametrically opposite results under the same measurement benchmark. Therefore, referring to the method of using measurement bases in the BB84 protocol, Alice and Bob randomly selected two sets of measurement bases in advance. Alice and Bob both randomly selected measurement bases to measure particles. Afterwards, one party announced their own measurement bases through a classical channel, while the other party compared the published measurement bases and informed the former which measurement bases were valid. Both parties would use the bits measured based on these effective metric bases as the final shared key.

2.3 Internet of Vehicles

(1) Concept of IoV

The IoV belongs to a special type of mobile self-organizing network. In its network, nodes have high mobility, rapid changes in topology, and high openness. It can enable vehicles to interconnect with traffic facilities, improve traffic management systems, and avoid road congestion and reduce the occurrence of accidents [14-15]. The architecture of the IoV is divided into application layer, transmission layer, and perception layer from top to bottom, as shown in Figure 1.

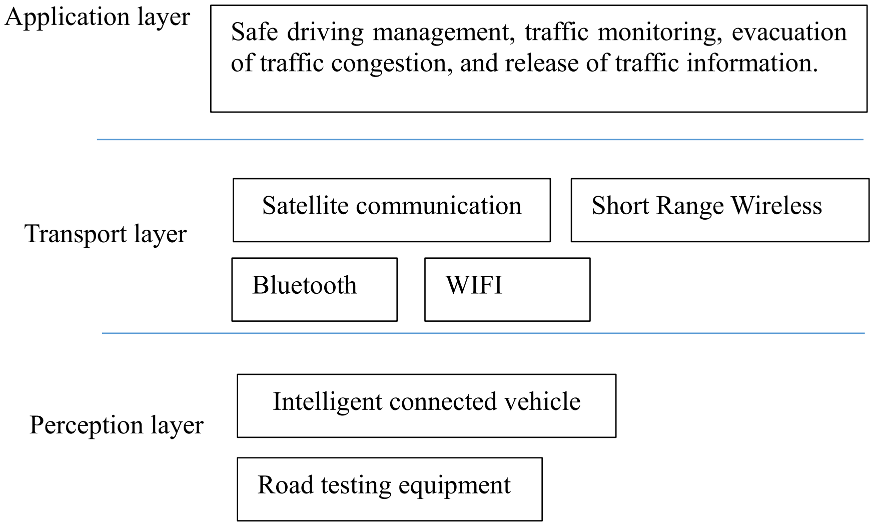
Application layer
Safe driving management, traffic monitoring, evacuation of traffic congestion, and release of traffic information.
Transport layer
Satellite communication
Short Range Wireless
Bluetooth
WIFI
Perception layer
Intelligent connected vehicle
Road testing equipment

Figure 1: Hierarchical division of the IoV system.

In the IoV, the perception layer can collect its surrounding environment and status information through sensors, cameras, and other devices, thus becoming nerve endings in the network, which can sense the situation inside and around the car in real-time. In the transport layer, the data information of the transport layer is concentrated on the central processor by using network technology [16]. In the IoV, the transport layer is the bridge connecting the application layer and the perception layer, which requires the safe and reliable transmission of data in a high-speed and open environment. At the application layer, computers can analyze and process massive amounts of information, and then connect with each other in the IoV, thus achieving the goal of intelligent interaction and tracking of driving paths for vehicles, calculating the optimal driving path for vehicle nodes, and also reporting real-time road information and setting reasonable signal cycle. In the IoV, the middle and bottom layers must collaborate to ensure the stable operation of the network, so as to achieve safe and efficient intelligent transportation.

(2) Security requirements

The security requirements for the IoV are availability, confidentiality, authenticity, data integrity, and non repudiation, as shown in Figure 2.

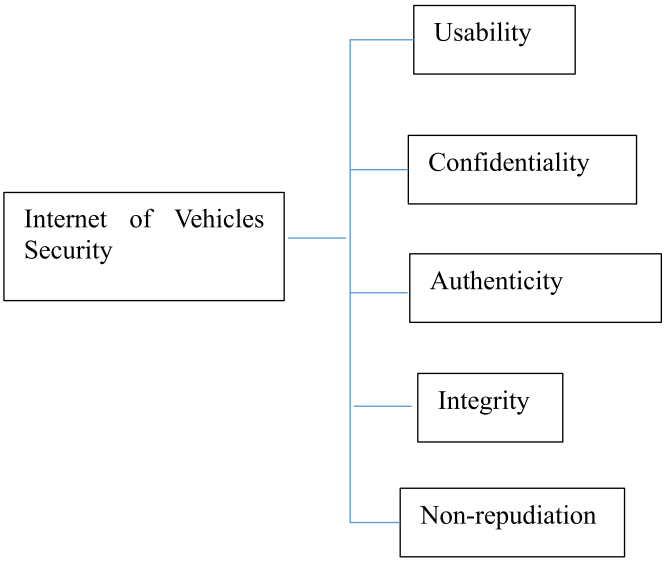

Figure 2: Security requirements for the IoV.

Availability refers to the guarantee that the IoV and its application systems can still function normally in the event of a malfunction or malicious attack on the IoV. Attacks that affect availability: Broadcast tampering attack: An internal attacker may hide correct security information from authorized vehicles by broadcasting incorrect warning messages [17].

Confidentiality refers to the ability of only specific recipients to access data. However, for the confidential information owned by each entity, external nodes cannot be understood, so an encryption method can provide confidentiality for it [18].

Authentication is a mechanism that can protect the IoV from malicious entity attacks, and is seen as the first line of defense against various attacks in the IoV [19].

Integrity refers to the fact that the messages in communication are not altered during transmission. Therefore, the data would not be generated, destroyed, or altered.

Non repudiation refers to the fact that in the event of an information dispute, the communication parties shall not refuse to send or receive the information. Negation attack is a major attack that disrupts non repudiation: When a conflict arises, the attacker can refuse to send or receive important messages [20].

3. Bidirectional Authentication QKD Protocol

This protocol mainly consists of two parts: one is the classical cryptosystem, and the other is QKD. Among them, the design of classical cryptosystems is mainly used to verify the identity of participants, and also provides a shared key string for the design of QKD. Under the premise of no other abnormal events (such as eavesdropping, key leakage, etc.), QKD can retain a small portion of the generated key for future use. However, in the event of anomalies, the existing verification keys and generated quantum keys would be immediately discarded, and classical cryptographic systems would be used again to verify identity and negotiate with other verification keys [21].

(1) Basic assumptions

Assumption 1: without noise; without considering the attenuation of photon energy; the detector has a 100% efficiency.

Assumption 2: Intentional DOS (Deny of Service) denial of service attacks were not considered.

(2) Participants

Alice, Bob, and Certificate Authority (CA)

(3) Protocol description

Step 1: The CA certification center issues public and private key pairs (PA, SA), (PB, SB) to Alice and Bob, sets a public directory that can only be modified and updated by the certification center, and publishes PA and PB. The CA certification center publicly selects appropriate encryption, signature, and authentication algorithms.

Step 2: Alice and Bob negotiate the authentication key AK (AuthenticateKey) through the classic channel. Bob generates a random string AK and selects a meaningful string ID B and a valid timestamp T to perform the following actions:

$$c = ENC_{PK_A}(ID_B \| T \| AK \| SIG_{SK_B}(ID_B \| T \| AK)) \tag{1}$$

Bob sends C to Alice.

Step 3: Alice performs the following actions after receiving message c. Among them, SIG represents the signature information of Bob's pair.

$$AK' = DEC_{SK_A}(c) - ID_B - T - SIG \tag{2}$$

$$RET = VER_{PK_B}(SIG_{SK_B}(ID_B \| T \| AK), SIG \tag{3}$$

If RET is true, the decrypted ID is a meaningful identification of Bob, and the message timestamp does not exceed the specified time period. AK'=AK, which is the authentication key AK (Authenticate Key) shared by Alice and Bob.

Step 4: Alice and Bob share a quantum channel. Alice first randomly generates a bit string called RAW KEY$\in\{0,1\}^{n}$.

Step 5: Alice sets the basis vector used to generate the quantum state based on the shared authentication key AK. Bit '0' is defined as representing the Z basis (0° and 90° polarized basis), and bit '1' represents the X basis (45° and 135° polarized basis). By reusing AK, each qubit can correspond to a specific basis vector. In step 4, a series of quantum states corresponding to the basis vector are produced using RAWKEY, and these photons are transmitted to Bob.

Step 6: After Bob receives these photons, he would determine the measurement basis required for each photon based on his AK sequence, measure each photon, and record the measurement result sequence. In this way, Bob has an n-bit key called SIFT KEY.

Step 7: Alice and Bob calculated the error rate on the public channel. They would randomly select the positions of the bits to be compared, and the bits involved in the comparison are called TESTKEY.

Step 8: Subsequent processing of QKD protocol: error code verification and privacy enhancement. Due to the presence of channel noise, there may be differences in the SIFTKEY values shared by Alice and Bob, so these differences must be corrected, removed, or corrected. Considering the existence of Eve as a potential "eavesdropper", it is assumed that Eve only eavesdropped on a portion of it, it would have a certain impact on the final error rate. However, if the error rate is still within the pre-set threshold, Eve can unknowingly obtain a portion. Therefore, to eliminate this possibility, there must be a step of privacy protection, which is to generate a shorter and more secure key from a secure long key string. The keystring after privacy enhancement is called FINALKEY.

Step 9: Alice and Bob retain a portion of the bits in the FINAL KEY as the next round of authentication key AK, while the remaining bit string is used as the session key SK (Session Key) for each round of encryption.

4. Simulation Experimental Results of QKD Applied in the IoV

In this paper, when the vehicle broadcast road information in the IoV, it would lead to privacy disclosure. QKD technology is used to process the broadcast information to ensure the traffic safety of this scheme in practical applications.

In order to evaluate the efficiency of vehicle networking applications, this article chose to use a bidirectional authenticated QKD protocol scheme for simulation. The simulation tool is NS (Network Simulator)-2.45. The length of the intersection is set to 800 meters, and the simulated running time is 300 seconds. Vehicles move freely in the area at an average speed of 12 kilometers per hour. The setting parameters of the vehicle network are shown in Table 1.

Table 1: Vehicle networking parametersl.

Parameter Type	Value
Vehicle speed (km/h)	12
Vehicle spacing (m)	40
Effective bandwidth (Mbps)	6
Number of lanes (nos.)	5
Communication range (m)	300

RSU (Road Side Unit) was located in the middle of the intersection, and the number of vehicles gradually increased from 10 to 50.

The simulation experiment mainly tested the average latency and data throughput of the vehicle network. Here, latency refers to the average latency of each vehicle, while data throughput refers to the average throughput rate of each vehicle. The results are shown in Figure 3. The average data throughput and average latency increase with the increase of the number of vehicles [22].

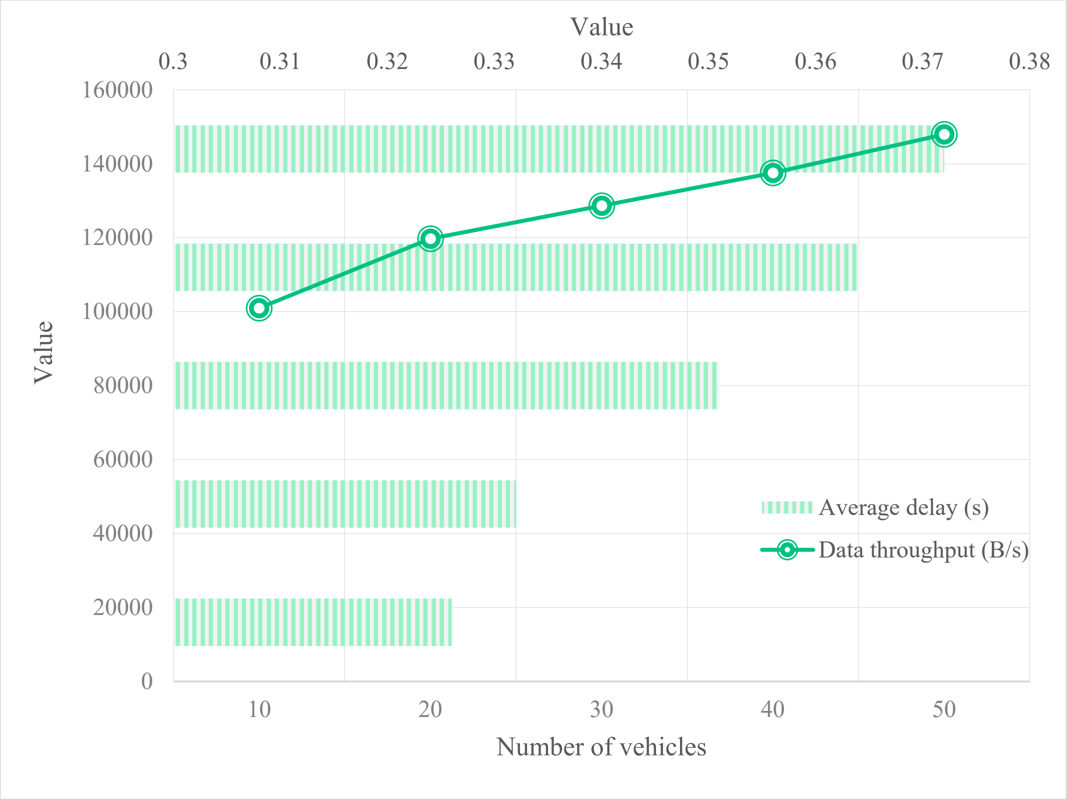

Figure 3: Changes in average data throughput and average latency as the number of vehicles increases.

Under the same parameters and environment, performance was tested using three other schemes, namely the four state SQKD (Semi—Quantum Key Distributio) protocol, the two state SQKD protocol, and the one state SQKD protocol. For the sake of comparison, the keys of all vehicles were preset in the simulation experiment, ignoring the process of generating internal keys within the vehicles. The results are shown in Figure 4. Compared with existing schemes, the scheme used in this article had greater advantages compared to the one state SQKD protocol, and also had obvious advantages compared to the other two schemes.

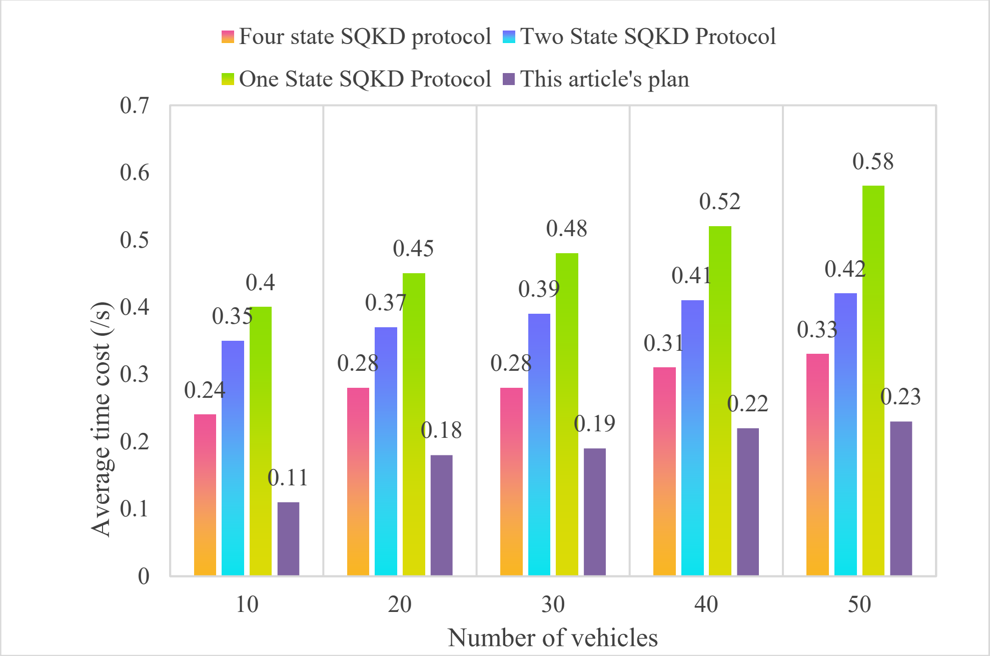

Figure 4: Scheme comparison diagram.

5. Conclusions

In recent years, quantum teleportation technology based on quantum mechanics has made significant progress, ensuring the security of information. With the rapid development of information technology and software technology, the IoV technology is also developing rapidly. In response to the various network attacks faced by the current IoV and how to improve its security, this project planed to combine quantum teleportation technology with the IoV, and explored the use of quantum teleportation technology to solve data security issues in the IoV. This article was only a new attempt to study the application of quantum teleportation technology in the security requirements of the IoV, and it did not reach the stage where it could be widely promoted and applied. There is still a long way to go before it can be truly widely applied in the security requirements of the IoV, and the research content of this paper needs to be further enriched and explored.

References

[1] Michael A. Cusumano: From Quantum Computing to Quantum Communications. Commun. ACM 66(1): 24-27 (2023)
[2] Eric Chitambar, Ian George, Brian Doolittle, Marius Junge: The Communication Value of a Quantum Channel. IEEE Trans. Inf. Theory 69(3): 1660-1679 (2023)
[3] SinghS K, AzzaouiA E, Salim M, et al. Quantum Communication Technology for Future ICT -Review. J. Journal of Information Processing Systems. 16(6):1459-1478 (2021)
[4] Qian Y, Zhang Y, et al. Security-Enhanced Content Caching for the 5G- Based Cognitive Internet of Vehicles. J. IEEE Network. 35(2):40-45 (2021)
[5] Seid Koudia, Angela Sara Cacciapuoti, Kyrylo Simonov, Marcello Caleffi: How Deep the Theory of Quantum Communications Goes: Superadditivity, Superactivation and Causal Activation. IEEE Commun. Surv. Tutorials 24(4): 1926-1956 (2022)
[6] Shantom Kumar Borah, Sainath Bitragunta: An Intelligent Link Selection Mechanism for Hybrid Classical-Quantum Communication Systems. IEEE Commun. Lett. 26(2): 301-305 (2022)
[7] Daryus Chandra, Angela Sara Cacciapuoti, Marcello Caleffi, Lajos Hanzo: Direct Quantum Communications in the Presence of Realistic Noisy Entanglement. IEEE Trans. Commun. 70(1): 469-484 (2022)
[8] Daryus Chandra, Marcello Caleffi, Angela Sara Cacciapuoti: The Entanglement-Assisted Communication Capacity over Quantum Trajectories. IEEE Trans. Wirel. Commun. 21(6): 3632-3647 (2022)
[9] Fatemeh Aliabadi, Mohammad-Hassan Majidi, Saeed Khorashadizadeh: Chaos synchronization

using adaptive quantum neural networks and its application in secure communication and cryptography. Neural Comput. Appl. 34(8): 6521-6533 (2022)

[10] Mahdi Chehimi, Walid Saad: Physics-Informed Quantum Communication Networks: A Vision Toward the Quantum Internet. IEEE Netw. 36(5): 32-38 (2022)

[11] Uzi Pereg: Communication Over Quantum Channels With Parameter Estimation. IEEE Trans. Inf. Theory 68(1): 359-383 (2022)

[12] Roberto Ferrara, Riccardo Bassoli, Christian Deppe, Frank H. P. Fitzek, Holger Boche: The Computational and Latency Advantage of Quantum Communication Networks. IEEE Commun. Mag. 59(6): 132-137 (2021)

[13] Aleksandrs Belovs, Arturo Castellanos, Francois Le Gall, Guillaume Malod, Alexander A. Sherstov: Quantum communication complexity of distribution testing. Quantum Inf. Comput. 21(15&16): 1261-1273 (2021)

[14] Imran Ahmed, Gwanggil Jeon, Awais Ahmad: Deep Learning-Based Intrusion Detection System for Internet of Vehicles. IEEE Consumer Electron. Mag. 12(1): 117-123 (2023)

[15] Goodness Oluchi Anyanwu, Cosmas Ifeanyi Nwakanma, Jae Min Lee, Dong-Seong Kim: Novel hyper-tuned ensemble Random Forest algorithm for the detection of false basic safety messages in Internet of Vehicles. ICT Express 9(1): 122-129 (2023)

[16] Swapnil Sadashiv Shinde, Daniele Tarchi: Collaborative Reinforcement Learning for Multi-Service Internet of Vehicles. IEEE Internet Things J. 10(3): 2589-2602 (2023)

[17] Akhtar Badshah, Muhammad Waqas, Fazal Muhammad, Ghulam Abbas, Ziaul Haq Abbas, Shehzad Ashraf Chaudhry, Sheng Chen: AAKE-BIVT: Anonymous Authenticated Key Exchange Scheme for Blockchain-Enabled Internet of Vehicles in Smart Transportation. IEEE Trans. Intell. Transp. Syst. 24(2): 1739-1755 (2023)

[18] Lukas Malina, Pavel Seda, Zdenek Martinasek, Jirí Pokorný, Miroslav Srotyr, Miroslav Vanis, Zdenek Lokaj: On Security and Privacy in Vehicle Speed-Limiting Services in the Internet of Vehicles. IEEE Intell. Transp. Syst. Mag. 15(1): 8-22 (2023)

[19] Saman Shojae Chaeikar, Alireza Jolfaei, Nazeeruddin Mohammad: AI-Enabled Cryptographic Key Management Model for Secure Communications in the Internet of Vehicles. IEEE Trans. Intell. Transp. Syst. 24(4): 4589-4598 (2023)

[20] Insaf Ullah, Muhammad Asghar Khan, Neeraj Kumar, Ako Muhammad Abdullah, Abeer Abdul-Aziz Alsanad, Fazal Noor: A Conditional Privacy Preserving Heterogeneous Signcryption Scheme for Internet of Vehicles. IEEE Trans. Veh. Technol. 72(3): 3989-3998 (2023)

[21] Lv Z., Chen D., & Wang Q. (2020). Diversified technologies in internet of vehicles under intelligent edge computing. IEEE Transactions on Intelligent Transportation Systems, PP (99), 1-12.

[22] Ramu N., Pandi V., Lazarus J. D., & Radhakrishnan S. (2020). A Novel Trust Model for Secure Group Communication in Distributed Computing. Journal of Organizational and End User Computing (JOEUC), 32(3), 1-14.