Research on the Security Technology of the Internet of Vehicles

Tianran Chu

Nanjing Foreign Language School, NO.30 East Beijing Road, Nanjing, Jiangsu, China
Email: Richard_Chu2006@163.com (T.R.C.)
Manuscript received August 15, 2024; revised September 11, 2024; accepted October 14, 2024; published October 25, 2024.

***Abstract*—With the development of technology, the Internet of Vehicles has become a key component of transportation. This article mainly explores the security challenges faced by the Internet of Vehicles in the era of intelligent connected vehicles. We have paid special attention to the security issues between the network communication layer and the intelligent vehicle platform. This paper mainly focuses on the security issues at the data transmission level. Firstly, the author analyzed the threats to the security of connected vehicles, including communication risks between data centers and vehicles, as well as within vehicles. Furthermore, the article delves into the advantages and disadvantages of various security technologies, such as blockchain, public key infrastructure, machine learning, and deep learning. And we also propose an improved new chain and new solution, as we want to combine the advantages of distributed and centralized to develop new security protocols and mechanisms. Finally, the article emphasizes the importance of establishing effective security standards and systems, such as ensuring user privacy, ensuring the authenticity and integrity of data, etc.**

***Keywords*—Internet of Vehicles (IoV), vehicle safety technology, network security technology**

I. Introduction

With the rapid development of 5G technology, the practical installation and application of the automotive internal network are on the agenda. As early as the beginning of the century, the concept of the Internet of Vehicles was proposed. With this technology, cars, including many means of transportation, can communicate with external networks in real time, making it much easier than before to obtain information about the surrounding environment. Today, it has had a complete interpretation: the on-board devices on vehicles use wireless communication technology to effectively utilize all vehicle dynamic information in the information network platform, providing different functional services during vehicle operation [1]. It can be observed that the Internet of Vehicles exhibits the following characteristics: by combining sensors and road monitoring to detect the position of surrounding vehicles, the Internet of Vehicles can provide protection for the distance between vehicles, reducing the probability of vehicle collisions; The Internet of Vehicles can help car owners navigate in real-time and improve the efficiency of transportation operations through communication with other vehicles and network systems [2]. However, receiving and sending such a large amount of information synchronously will take more risks. While massive amounts of information flow, they are possibly used as tools for crime by individuals with malicious motives. Therefore, it is inevitable that issues such as how to protect user privacy and maintain a safe and orderly Internet of Vehicles environment have become one of the major prerequisites for the application of Internet of Vehicles. As a massive IoT application system, the Internet of Vehicles (IoV) contains a large amount of data, processing, and transmission nodes. Its efficient operation must be standardized by a unified standard system to ensure the authenticity and integrity of data and complete various business applications. Standardization has become an urgent requirement for the development of vehicle networking technology and a complex management technology. In addition, vehicle networking and access to services are also aimed at providing better guarantees for safe driving of vehicles, so there's no need to say more about their significance. Hence, the ability to establish an efficient standard and safety system based on the current development of the Internet of Vehicles has become a key factor determining the future development of the Internet of Vehicles technology [3]. This article will briefly elaborate and analyze the security issues faced by the Internet of Vehicles at different levels, and propose measurements to address these challenges. The research objective of this article is to analyze the security challenges of the Internet of Vehicles, including the data platforms between data centers and vehicles, between vehicles and vehicles, and within vehicles. Evaluate the advantages and disadvantages of existing security technologies, establish effective security standards and systems, such as the combination of distributed and centralized, optimized CAN protocol connections, and risk detection through machine learning and deep learning. The following chapter two is a literature summary of current technologies in the Internet of Vehicles, chapter three mainly discusses some current security technologies, and chapter four is a review of the entire project.

II. An Analysis of Emerging Threat and Incidents

With the rapid development of the Internet and industrial intelligence, the automotive industry is continuously changing towards intelligence and networking. Intelligent connected vehicles, by being equipped with advanced onboard sensors and intelligent control systems and combining with modern mobile communication technology, achieve information exchange and sharing between vehicles and people, vehicles and vehicles, vehicles and roads, and vehicles and cloud service platforms, bringing much convenience to people's transportation and helping the government establish an intelligent transportation system [4]. However, as the Internet of Vehicles expands steadily, its safety issues are becoming increasingly prominent, and safety accidents are constantly emerging.

In 2016, Baidu successfully cracked T-Box (Telematics Box, T-Box) and tampered with protocol transmission data

[5], to modify user instructions or sending fake commands to the Controller Area Network (CAN) bus controller, so local control and remote operation control of the vehicles are achieved. This is because there are no security mechanisms such as encryption and authentication added to the current CAN bus, which makes it easy for attackers to modify CAN bus data and forge instructions to launch attacks on the vehicle.

In 2018, a thief in the UK only used a tablet to capture the passive wireless signal of Tesla keys [6], and in less than two seconds, he used the password hidden in the signal to open the car and successfully stole it. This type of attack indicates that the network level security of the Internet of Vehicles is also crucial, and security issues caused by wireless network attacks also frequently occur [7].

From the above, it can be concluded that the main security threats in the Internet of Vehicles come from three levels:

(1) V2X (Vehicle to Everything, including various forms of entity to entity communication) network communication security [4]: Attackers can use various wireless network communication methods to tamper with or forge attack signals, and inject attack commands into the vehicle to affect the normal state of the vehicle or directly control it. In addition, various types of terminal devices have also become the entry points for attackers to invade the Internet of Vehicles system, such as cloud service platforms, automotive remote service providers TSP (Telematics Service Provider), mobile terminal apps, etc.;

(2) The platform security of the intelligent connected vehicle itself [4]: On the one hand, due to the high-speed and non-encrypted and non-authenticated characteristics of the CAN bus, its communication matrix is easily cracked by attackers, so attackers can easily forge CAN bus messages, thereby affect the vehicle status, causing safety accidents or economic losses to car owners; on the other hand, intelligent connected vehicles contain various types of sensor ECUs, which store various sensitive data of the vehicle or owner, which can easily be illegally collected by attackers, leading to user privacy leakage;

(3) Internet of Vehicles component security [4]: The Internet of Vehicles architecture contains a large number of system components, such as various functional ECUs, which attackers can exploit or implant malicious code during firmware upgrades of these components.

III. Network Communication Layer and Intelligent Vehicle Platform Security

This article mainly discusses the security of the network communication layer and the security between intelligent vehicle platforms. The network communication layer security is divided into data exchange and information transmission security between data centers and vehicles and information exchange security between vehicles.

A. Communication Security between Data Center and Vehicles

Regarding the communication security between the data center and the vehicle, Xiong Shaojun gives the corresponding security requirements based on the security risks of IoV communication, briefly introduces the basic methods to realize the security of IoV communication, and proposes the service architecture, PKI architecture and multi-PKI system mutual trust mechanism to realize the security of IoV communication based on this [8]. The Internet of Vehicles communication security service architecture is composed of functions or entities such as full data processing functions, security credential management functions, security service functions, and security credential management. They can generate and process security messages based on specific IoV application logic, interact with IoV security certificate management entities to obtain relevant security certificates or data, provide storage of security certificates and data, and provide encrypted computing services, issue various public key certificates for communication security, and provide certificate revocation lists to IoV devices. According to the purpose of the vehicle networking communication certificate, the certificate can be divided into four types: CA certificate, registration certificate, pseudonym certificate, and application certificate. Registering a CA issues a registration certificate to the connected automotive device that has been authenticated by the registration authority, which uniquely corresponds to the device. The device needs to use a registration certificate to apply for a communication certificate suitable for a certain application field from another Authorized Authority (AA). A pseudonym certificate is issued by a pseudonym CA to an OBU, which uses the pseudonym certificate to sign the active security message (Basic Security Message, BSM) it broadcasts. In order to protect user privacy, password technology will be used to encrypt user identity information. At the same time, OBU can have multiple pseudonym certificates for regular switching to avoid exposing the vehicle's driving trajectory.

Zhao Junhui and others summarized three aspects of information security: IoT authentication technology, IoT trust management, and IoT privacy protection [9]. Firstly, in industrial IoT environments, when users want to securely access data from IoT sensors in real-time, they may face network attacks due to the data being transmitted through open channels. In order to solve this problem, they innovatively proposed a user and device authentication model combined with cloud computing, introduced a protocol design related algorithm, fully utilized the high reliability and fault tolerance of cloud storage systems, and protected user data privacy. Secondly, for IoV and other mobile animal networking applications, information collection and distribution are achieved by establishing a network between vehicles and infrastructure. Therefore, IoV will face security threats such as information insecurity and privacy leakage. They introduced a typical IoV trust management model and summarized some consensus algorithms, which solved the problem of unreliable information by storing vehicle trust values. Finally, in response to the privacy protection issue of IoV, they proposed a blockchain based cross domain anonymous authentication system model. Any registered user's auxiliary authentication information can be obtained from the blockchain. Anonymous authentication can achieve privacy protection for cross domain authentication, greatly saving communication costs for cross domain authentication [10].

B. Data Analysis between Vehicles and Vehicles

Due to the scarcity of computing resources on intelligent vehicles and the constantly changing nature of vehicles, secure communication between vehicles becomes more complex. Hao *et al.* [11] studied the trusted and reliable access management method in the edge computing of the 6G Internet of Vehicles based on the communication needs of the 6G zero trust network and the blockchain as a "trust bridge". Firstly, using a zero knowledge authentication algorithm based on two remaining attempts, mutual authentication and authorization between the base station and the vehicle are completed without exposing the privacy of the vehicle. Then, in order to improve verification efficiency and save energy consumption of the base station, a roadside redundant computing power incentive model based on contract theory was established. A portion of the verification tasks of the base station were allocated to edge servers or parked vehicles, and corresponding rewards were given. Finally, a 6G zero trust vehicle networking architecture based on double-layer blockchain was established, utilizing the main chain maintained by the base station group and the auxiliary chain maintained by the edge computing power to record important parameters for vehicle networking identity verification, achieving trusted access to the zero trust network environment. Compared with existing methods, this method significantly improves vehicle verification efficiency, reduces base station energy consumption, and has higher security without compromising vehicle privacy.

Zeinab El Rewini *et al.* proposed a three-layer framework (sensing, communication, and control) that enables a better understanding of automotive safety threats. The sensing layer consists of vehicle dynamics and environmental sensors, which are susceptible to interference and espionage attacks. The communication layer consists of in vehicle communication and V2X communication, which are susceptible to eavesdropping, man in the middle, and Sibyl attacks. At the top of the hierarchy is the control layer, which implements the functions of autonomous vehicles, including the automation of vehicle speed, braking, etc. Attacks targeting the sensing and communication layers can propagate upwards and affect functionality, while also compromising the security of the control layer. They have conducted the latest review on attacks and threats related to the communication layer and proposed countermeasures. This study also specifically introduces a study on using machine learning and deep learning for network security solutions. Machine learning can be divided into two types: supervised models and unsupervised models. A supervised model can be used to implement a standard anomaly detection solution, using a clean and anomalous dataset to train the model and identify anomalies. By using unsupervised models, we can create clusters from various data streams within vehicles, which can then be further analyzed to detect abnormal behavior. In the current field of vehicle networking security intrusion detection, machine learning is a very important solution.

C. Internal Communication Security of Vehicles

The CAN protocol is a multi-master protocol and employs the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) method. The CAN bus, as the most widely used in car bus communication protocol and a key step for attackers to invade the car network, is currently the focus of research. At present, the security research on CAN bus mainly focuses on the message authentication mechanism, message encryption mechanism, and anomaly detection mechanism of CAN bus. The message encryption mechanism refers to the allocation of keys to ECU nodes and the use of corresponding keys to encrypt the data domain of the message. Only ECU nodes with keys can decrypt messages to ensure their confidentiality. Encrypted message transmission can block the attack at the early stages of multiple steps by the attacker [4]. Halabi *et al.* [12] proposed a lightweight encryption solution based on the payload of CAN frames and previous key generation, providing a robust solution. They described the design of the solution and its prototype implementation, which were built to verify the functionality of the solution. They also use the Internet Security Protocol and Application Automatic Verification (AVISPA) tool to validate their solutions.

The CAN bus message anomaly detection mechanism is based on statistical anomaly detection, which analyzes the information entropy, time interval, time series, etc. of a large number of historical message records, detects abnormal CAN bus messages, and provides timely feedback. The information entropy on the bus is defined as the frequency of messages with different IDs on the CAN bus within a time window here, and when an attacker injects a large number of messages into the CAN bus, the change in information entropy on the bus is different from normal. Perform anomaly detection on messages on the bus based on changes in information entropy. Groza *et al.* [13] proposed an intrusion detection mechanism that utilizes Bloom filtering to test frame periodicity based on message identifiers and partial data fields, which helps detect potential replay or modification attacks. This has been proven to be an effective method, as most traffic from the in car bus is essentially cyclic, and due to rigid signal allocation, the format of the data fields is fixed. Bloom filters provide an effective time memory trade-off, which benefits the limited resources of automotive grade controllers.

Based on the above literature, whether it is between the backend center and the vehicle, between the vehicle and the vehicle, or within the platform, identity verification and intrusion detection are all crucial technologies. With the emergence of new technologies such as 5G, 6G, cloud computing, blockchain, machine learning, and deep learning, these technologies have gradually been introduced into security solutions for the Internet of Vehicles. With the high-speed bandwidth of 5G technology, multiple high-speed authentication can be achieved. By leveraging the powerful security features of cloud systems, privacy protection of vehicle information can be achieved. By leveraging the decentralized and anonymous features of blockchain, cross domain authentication between vehicles has been further improved. Further training of intrusion detection models through deep learning, continuously updating iterative models to cope with unknown attacks that constantly change with vehicle movement. In the subsequent solutions, new technologies such as edge computing can be used for reference to further improve the safety characteristics of interior components and platforms.

IV. The Choice of Distributed Technology

A. Background and Selection of Technologies

With the rapid development of mobile Internet and industrial intelligence, the Internet of Vehicles centered on intelligent connected vehicles has gradually penetrated into people's lives. It has brought convenience to travel but exposed security threats such as remote control and malicious attacks as well.

Among numerous security technologies, blockchain based distributed technology has full advantages. By building a peer-to-peer network, blockchain can solve the problem of centralized trust. The data records of the blockchain system are transparent to all network nodes, and all nodes can review and trace historical authentication records. Blockchain uses digital signature and hash operations for distributed unified storage, making the information in the blockchain permanently stored and unable to be modified once authenticated and written. Compared with traditional cross domain authentication schemes, blockchain assisted cross domain authentication can improve authentication efficiency and resist distributed denial of service attacks. By applying blockchain technology, the system can achieve higher stability and scalability. However, distributed systems have the drawback of complex communication structures, as a single node needs to interact with multiple nodes.

I suppose that although distributed computing is more complex, with the trend of increasingly powerful terminals and the enhancement of edge computing and other capabilities, it can respond to more complex environments more quickly.

B. Comparison between Centralized and Distributed Technologies

The traditional identity authentication protocol is mainly a one-to-one centralized authentication mode [14]. There are two inevitable problems in this authentication: first, the central authentication server is overloaded. When multiple vehicles are authenticated with the same roadside infrastructure, due to the limited resources of edge computing nodes, the central server is overloaded. Secondly, a single central server is more susceptible to malicious attacks. Blockchain technology can effectively solve these problems. It initially served as a supporting technology for Bitcoin's underlying layer, playing a significant role in tamper prevention and decentralization. The current application of blockchain is no longer limited to Bitcoin. Blockchain technology itself can be used for trust issues in various scenarios, and its essence is a decentralized and tamper proof distributed ledger. Multiple proxy vehicle edge computing nodes jointly maintain a blockchain, and authentication records are stored in a distributed manner, independent of central processing nodes (RSU or base station), thus realizing distributed data recording, storage and update. When blockchain technology is applied to cross domain anonymous authentication, the system divides the large area into several small areas, namely domain A, domain B, and domain C. Each region is managed by a base station, which is responsible for building a consistent blockchain network and storing partial user authentication information. When users arrive in a new area, they need to change their kana in order to authenticate with the base station, which uses information stored in the blockchain and information provided by the user to verify their identity.

The PKI (Public Key Infrastructure) mentioned in Xiong Shaojun's research is another mature technology used for identity verification and secure communication [8]. In this system, each participant has a pair of public and private keys, as well as a certificate issued by a trusted Certificate Authority (CA), which verifies the ownership of the public key. The challenges faced by PKI systems include maintaining certificates that require regular updates to maintain security. When a vehicle enters a new area or changes service providers, it must be able to quickly obtain a new certificate. To prevent key leakage, certificate abuse, and other situations, it is necessary to ensure that certificates can be revoked at any time. Because vehicles may cross different network regions while moving, the certificate update and revocation mechanism must be able to respond in real-time.

Compared to PKI technology, blockchain based distributed technology does not have a core module to serve as a hub for communication within a certain range. This greatly reduces its security vulnerabilities as attackers lose their main attack direction. Moreover, blockchain is built with multiple nodes, so it will not experience the huge central load of centralized technologies such as PKI, and its communication latency and maintenance costs will also be reduced.

C. Overcoming Disadvantages of Distributed Technology

Although distributed technology has obvious advantages in the security of the Internet of Vehicles, its implementation process also faces some challenges. Due to the fact that each node needs to participate in authentication and store user information, a large number of users will increase the storage pressure on each node, and multiple validations will have high requirements for the node. In addition, when a node leaves or new nodes join, it can make the operation more complex. Therefore, blockchain is not suitable for large-scale authentication environments [9].

There are many studies available to address and optimize these shortcomings. For example, for system management, problems can be solved through automated management tools, optimization of network structure, and data storage strategies.

V. The Introduction of Hybrid Technology and Artificial Intelligence

A. Development of Hybrid Technology

Distributed technology and centralized technology have their own advantages and disadvantages. If the advantages of both can be combined, a more excellent security technology can be developed. As mentioned earlier, the central end concentrates a large amount of data, has a high computational load, and is highly vulnerable to attacks. To address these shortcomings, we can adopt a distributed structure for the central end, setting it as a main chain that only collects some of the most core and basic information, such as the brand and manufacturer of the vehicle, while real-time location information of the vehicle is handed over to the auxiliary chain for distributed recording. Similarly, some drawbacks of

distributed technology, such as complex operations, storage of nodes, and high computational pressure, can also be addressed in this solution, as some management functions (scheduling and decomposition of complex tasks) are controlled by the central end, resulting in reduced complexity.

B. The Technology Selection of Machine Learning and Deep Learning

In the field of vehicle communication security, various traditional solutions can be integrated as mentioned above, and new technologies such as machine learning and deep learning can also be introduced. I believe that machine learning and deep learning will definitely be an essential part of future vehicle networking security solutions. The advancement of Machine Learning (ML) and Deep Learning (DL) has led to a paradigm shift in software development methods [15]. In software solutions based on ML and DL, the most critical component is not the algorithm/model, but the availability of data that can be used to train models to perform useful functions. Fortunately, the interconnectivity of the next generation of cars means that hundreds of terabytes of automotive operation and diagnostic data are generated and stored from vast geographic areas every day, which may be an important resource for developing next-generation network security solutions for automotive platforms and clouds. In addition, solutions based on classical statistical models and rule-based logic will not be able to fully utilize this scale of data. The ML detection model is data-driven, meaning it forms rules from the data. Therefore, the model architecture developed for specific detection problems in specific subsystems can be reused on multiple vehicle platforms. Deep learning models can be used for complex architectures that utilize information from multiple temporal and spatial separated data streams to perform robust detection [16].

Although successful in many applications, ML/DL based solutions still face some fundamental challenges when applied to automotive network security:

Protecting ML/DL models from adversarial attacks: In recent years, it has been found that convolutional neural networks are susceptible to adversarial inputs, leading to misclassification of images (such as classifying cars as trees or people as traffic signs). Due to almost all computer vision in ADAS systems using CNN, this is a legitimate network security threat [17]. During adversarial attacks, the attacker adds a specific amount of noise to the image output by the camera before processing it by the computer vision system (which cannot be detected by the human eye). Therefore, before developing networks security solutions that rely on CNN architecture, it is necessary to determine a CNN architecture that is strong enough against adversarial attacks and firewalls to protect image data pipelines.

Optimize model architecture: Most of the computational operations in ML/DL models are addition and multiplication. However, completing one inference may require hundreds of thousands of such operations. Due to the strict limitations on computing, memory, and power consumption imposed by the computing hardware on automotive platforms, ML/DL based solutions must be limited. However, precise computing technologies such as FP16, model pruning, and specialized computing hardware based on reduced floating-point provide solutions [18].

VI. Security Enhancement of CAN Protocol

A. Protection Methods for CAN Protocol Information

In the field of in car communication, I believe that adopting a safety enhanced CAN protocol is a good way. Compared with other bus protocols, the short frame structure of the CAN protocol has the following advantages:

1) Small data volume, short sending and receiving time, and high real-time performance.

2) Small data volume, low probability of interference, and strong anti-interference ability.

Due to the simple message type and length of the CAN protocol, it lacks an effective authentication mechanism and is vulnerable to replay attacks and information tampering threats. In addition, the non encrypted nature of the CAN protocol makes communication content easily intercepted and analyzed. The protection mechanism for it cannot be too complex, and its computational and communication costs must be fully considered.

Encrypting CAN protocol information is one solution. This solution uses symmetric key encryption to encrypt the payload of CAN frames, where each encryption key is bound to the frame identifier itself. The encryption key for the identifier is regenerated after each frame with that identifier is transmitted. The regeneration mechanism is a pseudo-random number generator with a blockchain like algorithm, in which the encryption key sequence forms an encrypted hash chain that depends on the transmission history of the corresponding identifier. In addition, all processing occurs within the payload of the frame, so there is no need to modify the standard CAN frame format.

This encryption mechanism is robust because it relies on the actual transmission of messages between components. The advantage of this mechanism also comes from the randomness of key generation, which is due to the rehashing of previously randomly generated hashes. In addition, compared to CPU intensive asymmetric encryption schemes, hashing and encryption mechanisms are lightweight. This ensures that the solution does not impose additional limitations on the design of CAN bus components, nor does it impose commercial restrictions that hinder large-scale production of CAN bus components.

We can also adopt appropriate security measures by analyzing the characteristics of abnormal attacks. The vast majority of actual attacks are completed by replaying previously recorded frames on the bus or injecting modified versions of recorded frames. These clearly violate the periodicity of frames. Due to the fact that communication on the CAN bus is mostly completed within precise communication cycles, and signal allocation within specific frameworks is strict, detecting such intrusions is feasible. In this work, Groza and Murvey [13] designed and evaluated an intrusion detection mechanism based on frame periodicity and its content, by considering the infrequently changing parts of data fields.

Due to the inconvenience of storing all the information required for each frame (due to obvious memory limitations), they used Bloom filters to identify messages and their

contents [19]. The size of the ID, which is 11 bits for regular frames and 29 bits for extended frames, makes it impossible to store all the information of each frame on each node. In contrast, Bloom filters allow for time memory trade-offs when testing set membership relationships, making them suitable for a large number of network applications. Each ID only stores a few Bloom filters and a byte mask, which requires storing one bit for each byte of the message. By using these, the most important number of frames can be filtered out, namely the cyclic frames that are regularly reported. Event frames can be processed through different and less effective mechanisms without causing too much interference to the bus, as they account for a smaller proportion of the total traffic.

CAN was used in early industrial control systems, so it was very simple. The current industrial control system has significantly increased computing resources and transmission channels, so it is possible to design a more comprehensive protocol, expand the existing CAN protocol content, add security frames, and achieve the goal of balancing security and system performance, and facing more complex network attacks.

VII. Conclusion

With the development of technology and the Internet, the application of Internet of Vehicles technology is gradually increasing, and the space occupied by these applications in people's lives is also constantly expanding. So this background gave rise to the concept of connected cars. Now, in order to truly bring Internet of Vehicles technology into daily life, its security issues have become the main focus of research.

This article discusses the security technologies of the Internet of Vehicles, including PKI technology, distributed technology based on blockchain, machine learning technology, symmetric and asymmetric encryption technology, and compares the advantages and disadvantages of centralized and distributed technologies. There are PKI technology and distributed technology based on blockchain and their fusion-based authentication for the Internet of Vehicles. Machine learning technology has achieved intrusion detection in the Internet of Vehicles, and the CAN protocol has enhanced the security of communication in the Internet of Vehicles. Our next task is to study how artificial intelligence can assist in maintaining the security of connected vehicles. I think a more effective security system can use centralized and distributed methods to facilitate secure communication between data centers and vehicles, as well as use machine learning and deep learning algorithms to detect whether the transmitted data is risky, and use the CAN protocol to ensure the security of hardware data flow inside the vehicle. I think these three systems can more effectively enhance the security of the Internet of Vehicles.

Conflict of Interest

The author claims that no conflict of interest exists.

References

[1] A. Kavianpour and M. C. Anderson, "An overview of wireless network security," in *Proc. 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, 2017, pp. 306–309.

[2] F. Goudarzi, H. Asgari, and H. S. Al-Raweshidy, "Traffic-aware VANET routing for city environments—A protocol based on ant colony optimization," *IEEE Systems Journal*, vol. 13, no. 1, 2018, pp. 571–581.

[3] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 122–129, 2017.

[4] X. H. Li, C. Zhong, Y. Chen, H. L. Zhang, and J. Weng, "Survey of internet of vehicles security," *Journal of Cyber Security*, vol. 4, no. 3, pp. 17–33, 2019.

[5] Baidu successfully cracked the T-BOX system and the security of the Internet of Vehicles has reached a new height. 2016. [Online]. Available: http:// www.elecfans.com/qichedianzi/20161130453520.html 2016.11

[6] Watch thieves stealing a Tesla through Keyfob hack and struggling miserably to unplug it. 2018 October. [Online]. Available: https://electrek.co/2018/10/21/tesla- stealing-video-keyfob-hack/

[7] X. Zheng, Y. Liu, and J. Q. Ke, "Research on cluster head selection and data transmission strategy based on fuzzy logic in Internet of Vehicles," *Information Security and Communication Secrecy*, vol. 41 no. 7, pp. 1458–1460, 2020.

[8] S. J. Xion, "Research on security communication technology of internet of vehicles based on 5G technology," in *Proc. Journal of Physics: Conference Series*, IOP Publishing, 2021, vol. 2066, no. 1, p. 012058.

[9] J. Zhao, H. Hu, F. Huang, Y. Guo, and L. Liao, "Authentication technology in internet of things and privacy security issues in typical application scenarios," *Electronics*, vol. 12, no. 8, p. 1812, 2023.

[10] N. S. Bitcoin. 2008. A peer-to-peer electronic cash system. *Decentralized Business Review*. [Online]. Available: https: //bitcoin.org/.

[11] H. Hao, D. Ye, R. Yu, J. Wang, and J. Liao, "Blockchain empowered trustworthy access scheme for 6G zero-trust vehicular networks," *Journal of Electronics & Information Technology*, vol. 44, no. 9, pp. 3004–3013, 2022.

[12] J. Halabi and H. Artail, "A lightweight synchronous cryptographic hash chain solution to securing the vehicle CAN bus," in *Proc. 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*, 2018, pp. 1–6.

[13] B. Groza and P. S. Murvay, "Efficient intrusion detection with bloom filtering in controller area networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 1037–1051, 2018.

[14] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, 1508–1532, 2019.

[15] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, 2020, 100214.

[16] L. Zhang, L. Shi, N. Kaja, and D. Ma, "A two-stage deep learning approach for can intrusion detection," in *Proc. Ground Vehicle Syst. Eng. Technol. Symp. (GVSETS)*, 2018 Aug, pp. 1–11.

[17] M. Yousefi-Azar, V. Varadharajan, L. Hamey, and U. Tupakula, "Autoencoder-based feature learning for cyber security applications," in *Proc. 2017 International Joint Conference on Neural Networks, (IJCNN)*, 2017, pp. 3854–3861.

[18] W. Tong, A. Hussain, W. X. Bo, and S. Maharjan, "Artificial intelligence for vehicle-to-everything: A survey," *IEEE Access.*, vol. 8, no. 7, pp. 10823–10843, 2019.

[19] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, no. 7, pp. 422–426, 1970.