SecCDV: A Security Reference Architecture for Cybertwin-Driven 6G V2X

Guanjie Li, Chengzhe Lai, *Member, IEEE*, Rongxing Lu, *Fellow, IEEE*, and Dong Zheng

***Abstract*—Recently, the proposed Cybertwin-driven 6G network architecture has attracted attentions from academia, which can support the communication anchor, security agent and other functions for physical devices. Especially, Cybertwin can provide promising Vehicle-to-Everything (V2X) applications in future. However, security and privacy of Cybertwin still face various threats and challenges, which may impact future deployments for Cybertwin-driven 6G V2X. In this paper, we first introduce the architecture and promising applications of Cybertwin-driven 6G V2X. Then, we analyze essential data security and privacy preservation requirements for Cybertwin-driven 6G V2X. Particularly, we present the security reference architecture of Cybertwin-driven 6G V2X. As a case study, we investigate the migration of Cybertwin caused by vehicle mobility, and propose a handover authentication scheme to create new Cybertwin between vehicle and edge server based on proxy ring signature technique. Finally, we discuss several open research directions for achieving more secure Cybertwin-driven 6G V2X.**

***Index Terms*—Cybertwin, digital twin, V2X, data security, privacy, handover authentication.**

I. Introduction

SINCE 2020, as the 5th Generation Mobile Networks (5G) has been deployed commercially around the world, academia and industry have begun to research on the next generation of wireless communications system, known as the sixth generation (6G) [1]–[3]. It is anticipated that the transmission capacity of 6G may be 100 times higher than that of 5G, and the network delay may also drop from milliseconds to microseconds [4]. Furthermore, the 5G Internet of Things (IoT) will further evolve into the Internet of Everything (IoE) in the 6G era, which could build a wide range intelligent connection between people, data, device and virtual procedure [5]. The goal of IoE is to seamlessly connect billions of devices, accurately analyze oceans of real-time data, efficiently make intelligent decisions and further create a better human world [6]. In order to realize these aspirational visions, Terahertz, Unmanned Aerial Vehicles, Space Multiplexing and other new communication technologies are applied to compensate the shortcomings of 5G networks and to provide a wider range of ultra-fast wireless network connections [7]. In addition, as an emerging intelligent computing technology, digital twin can realize the connection, interaction and integration between the physical world and cyberspace [8].

Integrated artificial intelligence, machine learning, advanced modeling and other techniques, digital twin can dynamically map the physical entity to the virtual world and create the visualized virtual twin body under the connection of the real-time data [9]. Digital twin can not only accurately reflect the real situation and real-time changes of the physical entity, but also provide a series of services to the physical entity, such as behavior analysis, operation optimization, status prediction and decision feedback [10]. Digital twin is considered to be the one of the key technologies to realize the 6G vision, and the related research on the application of digital twin in 6G has been carried out [9], [11], [12].

With the emerging research on digital twin, Cybertwin has been received widespread attentions from academia [13], [14]. Cybertwin is digital representation of humans or devices in the virtual cyberspace as well as digital twin, but could provide with several fundamental service support such as communication assistant, behavior logger and mobility agent in the edge network [15]. In addition, operating on the edge network in close proximity of physical entity, Cybertwin has the characteristics of lower latency, higher scalability and more reliability, therefore it is more suitable for delay-sensitive applications compared to digital twin which is generally deployed in the remote central cloud.

Vehicle-to-Everything (V2X) aims to share road information and to transmit collecting data between vehicles, infrastructures, pedestrians and cloud [16]. Compared to 5G-V2X, 6G-V2X has the potential to support super fast, super reliable and low latency V2X information exchanges powered by novel technologies used in 6G [17]. The goal of 6G-V2X is to be a heterogeneous, dynamic, intelligent, autonomous, user driven connectivity and

Manuscript received July 22, 2021; revised October 6, 2021; accepted November 28, 2021. Date of publication December 9, 2021; date of current version May 20, 2022. This work was supported in part by the National Natural Science Foundation of China Research under Grant 62072371 and in part by the Key Research and Development Program of Shaanxi Province under Grant 2021ZDLGY06-02. The review of this article was coordinated by the Guest Editors of the Special Section on Cybertwin-Driven 6G for V2X Applications. *(Corresponding author: Chengzhe Lai.)*

Guanjie Li is with the School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi 710121, China, and also with the School of Cyber Engineering, Xidian University, Xian, ShaanXi 710071, China (e-mail: sinleced@msn.cn).

Chengzhe Lai is with the School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi 710121, China (e-mail: lcz_xupt@163.com).

Rongxing Lu is with the Faculty of Computer Science, University of New Brunswick, Fredericton, New Brunswick E3B 5A3, Canada (e-mail: rlu1@unb.ca).

Dong Zheng is with the School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi 710121, China, and also with the Westone Cryptologic Research Center, China (e-mail: zhengdong@xupt.edu.cn).

Digital Object Identifier 10.1109/TVT.2021.3133308

service platform for Intelligent Transportation System (ITS). In addition, 6G-V2X can further support advanced vehicular applications such as autonomous driving.

The hundreds of sophisticated sensors equipped in vehicle make the combination of V2X and Cybertwin reality [18], [19]. As Intra-twin and Inter-twin communication in [20], there are two new communication modes which can be defined in Cybertwin-driven 6G V2X, namely Cybertwin-to-Vehicle and Cybertwin-to-Cybertwin. In the Cybertwin-to-Vehicle communication, onboard sensors collect data including vehicle status and then transmit to Cybertwin located on edge server; relying on the computing resources provided by edge server, Cybertwin could integrate, process, analyze data fed by vehicle, and give vehicular operation monitoring, feedback decision, state prediction and return back to its physical vehicle. Using advanced modeling technology, Cybertwin can also use visual management to dynamically simulate and reproduce the running state of the vehicle in the virtual space. In the Cybertwin-to-Cybertwin communication, Cybertwin can communicate with other twin nodes to transfer data, share resources and improve information perception in cyberspace. Furthermore, the digitalization of Cybertwin could supply promising V2X applications. It can anticipate that Cybertwin-driven 6G V2X will bring super safe, comfortable and intelligent autonomous driving experience for human in the future 6G era.

Although the technical standards and development framework for 6G are still being envisioned and researched, 6G will not only inherit the security issues of legacy networks, but also face new several security challenges caused by new technologies. In the Cybertwin-driven 6G V2X network, the openness of wireless network and mobility of vehicles make the communication between physical devices and Cybertwin vulnerable to various threats such as eavesdropping. It is also necessary to frequently access the new edge server and migrate the corresponding twin for cruising vehicles [21]. More importantly, as an intelligent agent, Cybertwin can obtain global and sensitive information of its corresponding physical devices [13]. However, the fact that Cybertwin operates on the edge server could cause the privacy of the physical device to be comprised. There are curious edge servers may stealthily collect physical device information such as preferences or location while providing computing and storage resources. Nevertheless, different from the communication between physical devices, the communication between Cybertwins has not yet established security mechanisms such as authentication and encryption, which makes it possible for Cybeytwin to receive wrong information sent by malicious twins and cause decision-making errors, and affect the safe operation of the physical device.

Although Cybertwin-driven 6G V2X is still in its infancy, security and privacy concerns ranging from application environment and communication technology should be addressed at the stages of design. In this paper, we will focus on the vehicle and take a closer observation at security and privacy threats in Cybertwin-driven 6G V2X network. The main contributions of this paper are summarized as followed:

- We introduce the architecture of Cybertwin-driven 6G V2X network based on the features and functions of Cybertwin. Moreover, the potential and promising applications for Cybertwin-driven 6G V2X are prospected.
- We summarize the security and privacy requirements and analyze the data security or privacy threats for Cybertwin-driven 6G V2X network. Particularly, we propose the security reference architecture and potential solutions in Cybertwin-driven 6G V2X.
- As a case study, considering the mobility of the vehicle and its Cybertwin operation on the edge server, we design a handover authentication scheme based on proxy ring signature technique [22] to achieve mutual authentication, key negotiation and Cybertwin migration between the moving vehicle and edge server.

The rest of this paper is organized as follows. The system architecture and emerging applications of Cybertwin-driven 6G V2X are introduced in Section II. Security and privacy requirements, followed by the security reference architecture of Cybertwin-driven 6G V2X network are given in Section III. In addition, several potential data security solutions are also discussed in Section III. In Section IV, we take the migration of Cybertwin issue as a case study and design an authentication scheme based on proxy ring signature. Future research directions are prospected in Section V. Finally, we draw a conclusion in Section VI.

II. Architecture and Application for Cybertwin-Driven 6G V2X

In this section, we will introduce the architecture of Cybertwin-driven 6G V2X network and promising V2X applications supported by Cybertwin.

A. Architecture for Cybertwin-Driven 6G V2X Network

According to the definition and characteristics of Cybertwin [13], we present the Cybertwin-driven 6G V2X network architecture, as shown in Fig. 1. The architecture is composed of the interrelated four layers, namely physical device layer, access layer, edge layer and Cybertwin layer.

- *Physical Device Layer:* In the Cybertwin-driven 6G V2X network, physical device layer consists of vehicles, roadside infrastructures, pedestrians with wearable devices and other physical devices. Data is the driver and foundation of the Cybertwin-driven 6G V2X network. Physical devices not only generate data, but also consume it. With the continuous development of intelligent vehicle, on-board sensors play an important role to collect vehicle raw data, which can perceive the driving surrounding environment information (e.g., identifying object) and record vehicle operating parameter (e.g., engineer speed). The roadside infrastructure includes roadside unit devices with communication and perception capabilities, for example, intelligent traffic lights. These fixed devices can sense a wider range of traffic information and provide V2X network with more accurate and real-time road information. In addition, pedestrians are also one of the elements in the physical device layer who usually use wearable devices to transmit physical status or

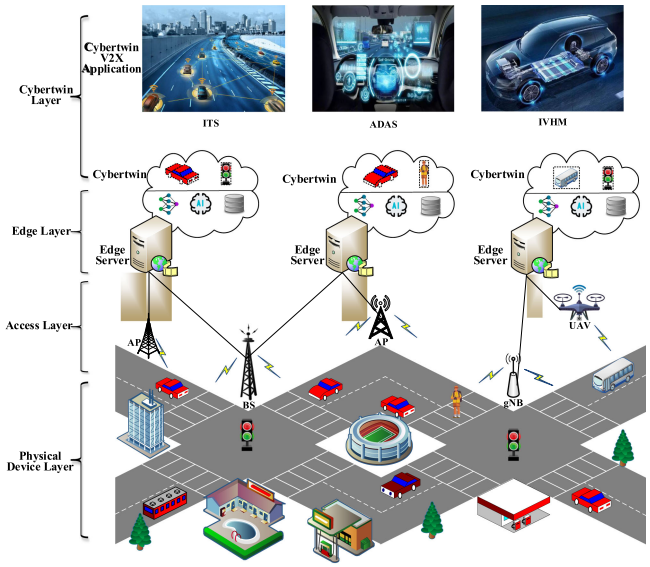


Fig. 1. Architecture of Cybertwin driven-6G V2X network.

other forms of data. This data is transmitted to Cybertwin for processing and analyzing to obtain better services.

- *Access Layer:* Access layer consists of different type of access points (AP) to provide the ubiquitous high-speed access services between the physical device and virtual Cybertwin through the collaborate deployment of various networks. In the Cybertwin-driven 6G V2X network, access layer has higher bandwidth and lower delay to fulfill the requirements of massive data acquisition on the device side and millisecond response on the Cybertwin side. The novel and promising communication technologies employed in 6G ensure the realization of these goals. As new resource of spectrum, Terahertz can realize ultra-high-rate data transmission with ultra-wide spectral bands. As Airborne base stations, Unmanned Air Vehicle (UAV) has potential to further expand the communication coverage and capacity of 6G. In addition, the control plane and data plane will be further decoupled in the access layer in order to provide more flexible access resource management.
- *Edge Layer:* The edge layer is composed of various edge servers connected to base stations. Edge server has strong computing power to support the running of deep learning or machine learning algorithms. Edge server is in proximity to the physical devices, despite its capability is inferior to the central server, edge server can provide real-time interaction and reduce response delays for physical devices and their corresponding Cybertwins, especially for delay sensitive V2X services. In addition, the distributed local storage of the edge server offers a platform for data management and data storage of Cybertwin, which enables the analysis and processing based on massive historical data to be completed rapidly and reliably.
- *Cybertwin Layer:* Cybertwin is the core function of the Cybertwin-driven 6G V2X network. As the digital representation of physical device, Cybertwin can recreate and reflect the status of physical device in virtual space after receiving the real-time data. It can not only provide basic functions such as communication assistant, but also provide novel V2X application services. On the one hand, powered by advanced modeling tools, Cybertwin can perform holographic replication of physical device in order to achieve a deeper understanding and a better optimization. On the other hand, Cybertwin can also evaluate state, analyze data, forecast operation trend, and provide decision feedback for its counterpart in physical world by employing machine learning or artificial intelligence algorithms. As mentioned above, Cybertwin can communicate with other twins in the same or different edge servers, which can refer to as Cybertwin-to-Cybertwin communication. Data is a key factor for Cybertwin, more data means Cybertwin can provide more accurate feedback to the physical device. This communication mode improves the data acquisition ability and gets rid of the limitation of space for Cybertwin, which can not only rely on the data fed by physical devices, but also can directly obtain more information from other twins in cyberspace. Moreover, since Cybertwin operates on resources provided by edge server, they can also share idle resources with each other to improve computing efficiency in Cybertwin-to-Cybertwin communication.

B. Applications of Cybertwin-Driven 6G V2X

Although Cybertwin is still in the early stages, its features imply that Cybertwin has great potential to support intelligent development of V2X in the future 6G era. In this subsection, we summarize the state-of-art works relevant to V2X applications supported by digital twin. While these twin deployment in the remote central cloud, it does not prevent us from insight into the bright future of the Cybertwin-driven 6G V2X, since Cybertwin has characteristic of low latency and high expansion which digital twin lacks.

1) Advanced Driver Assistant System: Safe driving is always the first priority and the eternal goal for the development of V2X [23]. Advanced Driver Assistant System (ADAS) is seen as a transitional stage for the realization of autonomous vehicles [24]. Based on the road information collected by sophisticated on-board sensors such as Lidar, ADAS can provide driver imperceptible dangers or even actively control vehicles to avoid dangerous accidents in the first time. ADAS can prevent and avoid traffic accidents caused by human error to the greatest extent. However, ADAS still has several limitations. One of the issues is lack of road information interaction among vehicles on road, which leads to ADAS system cannot accurately prejudge the behavior of other vehicles. In addition, ADAS makes judgments based on the information collected by the on-board sensors at the current moment while ignoring the historical behavior of the vehicle, which is due to the limited storage capability of the vehicle.

Introducing digital twin into ADAS can effectively improve the above issues. Wang *et al.* [25] proposed an advanced driving assistance system based on the digital twin vehicle, which aims to provide the driver with the optimal driving speed when the vehicle enters the road ramp. In this system, the vehicle sends

the driving information including speed, position and obstacles ahead to the digital twin which resides on the central server. After pre-processing the received data, digital twin can further create real-time road simulation and a virtual copy of the vehicle. By using machine learning and combining with historical knowledge, the optimal speed can be determined and fed back to the vehicle driving panel through V2C. Chen *et al.* [26] put forward digital twin test verification platform based on the virtual real combination. After receiving the vehicle information, the digital twin can globally plan the vehicle speed, driving path and positioning choice, and further evaluate the effect of the decision, so as to improve the safe driving of the vehicle.

ADAS can assist vehicles in recognizing or avoiding other vehicles or pedestrians on the road, often within the coverage of the same edge server. In the Cybertwin-driven 6G V2X network, Cybertwins of different vehicles running on the same edge server can communicate with each other, sharing real-time location and next actions of physical vehicles, which enables Cybertwins to obtain road information faster. Therefore, the Cybertwin can reduce ADAS response time, make driving decision more quickly and ensure safe driving of physical vehicle compared to the digital twin.

2) Intelligent Transportation System: Current several advanced technologies, such as communication, sense and artificial intelligent, have been applied to traffic management, however the lack of interaction and integration between these technologies prevents the transformation of the transportation system to true intelligence. As one of the applications of V2X, ITS can effectively and comprehensively apply these advanced technologies to transportation, break the barrier and strengthen the connection between vehicles, roads and users [27]. The vision of ITS is to improve traffic safety, optimize traffic flow, increase traffic throughput and facilitate traffic management. Nevertheless, the current ITS still has several challenges which include high management costs, inaccurate road conditions data and a lack of global perspective.

Cybertwin and digital twin can solve these challenges and make ITS even more powerful [28], [29]. Vehicles, infrastructures and pedestrians all create their own Cybertwins on edge servers. On the one hand, these twins can provide application services to physical bodies; on the other hand, Cybertwins can feed the real-time state of physical entities back to the global digital twin located in the central cloud, so that global digital twin can obtain global traffic information in a visual way. Global digital twin can run thousands of virtual traffic simulations to obtain the best traffic management, such as traffic light duration, traffic congestion alerts, or smart parking. The global digital twin returns the simulation results to the local Cybertwin, which further combines the feedback results with the real-time status of the vehicle to propose the vehicle the optimal decision.

3) Integrate Vehicle Health Management: Integrate Vehicle Health Management (IVHM) can perform diagnosis, prognosis and health management for crucial components of the vehicle through the status data provided by on-board sensors [30], [31]. IVHM overcomes the existing issues of vehicle maintenance, that is, the inability to rapidly determine the cause of malfunction and to detect potential hazards in the vehicle. IVHM can improve the vehicle reliability, ensure the safe driving and reduce the maintenance cost.

The combination of virtual twin and IVHM can provide new features and advantages [32], [33]. The system or components of vehicle can be displayed in the dynamic and virtual representation provided by the real-time and high-fidelity simulation capabilities of digital twin, which can allow that drivers gain holistic and rich knowledge about the vehicle. IVHM based on digital twin can bring more accurate and better performance for health monitoring and vehicle diagnosis. Moreover, integrated with the historical operating data of the vehicle, customized service and reasonable proposal can be provided to drivers in order to adjust driving behavior and to extent vehicle lifecycle. Suchitra *et al.* [34] developed digital twin model to monitor the operation of electric vehicle motor in Matlab. The distance and speed of the vehicle are input to the artificial neural network and fuzzy logic in real time, the temperature of the motor housing and coil is calculated as the output value. Based on these output value, the degradation rate and remaining useful life of electric motor can be predicted and the best time to refill the bearing lubricant can be found to remind driver. Ryan *et al.* [35] proposed the monitoring and prognosis of automobile brake systems based on the digital twin, which can effectively estimate the maintenance time of the brake system and detect imperceptible faults or abnormalities of automotive components according to the wear rate of the brake pads. Furthermore, machine learning algorithms used for brake system diagnosis can be continuously optimized and improved.

One of the basic functions of Cybertwin is behavior logger, which means that Cybertwin can capture and record all information about the physical device. In the application of IVHM, Cybertwin not only can monitor and diagnose vehicle status like digital twin, but also record information such as vehicle status, cause of breakdown and reasonable suggestions. Cybertwin can remove sensitive data from this information and turn it into digital assets, and further share or recommend it to the other twins for a certain reward. At the same time, Cybertwin can also obtain suggestions from other twins to better optimize vehicle management and increase vehicle service life.

III. Security and Privacy of Cybertwin-Driven 6G V2X Network

In this section, we propose the security requirements and security reference architecture for Cybertwin-driven 6G V2X network.

A. Security and Privacy Requirements of Cybertwin-Driven 6G V2X Network

First, we present six security and privacy requirements that Cybertwin-driven 6G V2X network should be satisfied, which are confidentiality, integrity, availability, authentication, privacy and trust.

Confidentiality: Since the physical device and its Cybertwin communicate over an open wireless channel, confidentiality

requires that the transmitted data can not be accessed by unauthorized third parties. In addition, since the Cybertwin is the agent of physical device on the edge server, which means that the Cybertwin can owns all the historical behavior data of the physical device. Therefore, confidentiality also requires that unauthorized third parties can not obtain any data about the physical device from the Cybertwin operating on the edge server. In cyberspace, communication between Cybertwins also require confidentiality protection to prevent attackers from eavesdropping.

Integrity: Integrity is another essential protection to provide the data security in Cybertwin-driven 6G V2X network. It requires that data transmitted and received between the physical device and its Cybertwin is correct and identical without tampering or replay from unauthorized third parties. In addition, historical data stored by Cybertwin also requires integrity protection to prevent relevant data from being modified by unauthorized third parties on edge servers.

Availability: Availability guarantees that legitimate users can access and employ the services. In the Cybertwin-driven 6G V2X network, availability first ensures that the authorized physical device can access the edge server and create its virtual twin. Second, availability requires that the physical device can collect and provide real-time data normally. In addition, it requires that the edge server can provide the necessary computing and storage resources to Cybertwin. Furthermore, availability guarantees that Cybertwin can employ resources provided by edge servers to process data fed by devices.

Authentication: Authentication confirms the legitimacy of the identity and verifies the source of the message for involved each entities. In the Cybertwin-driven 6G V2X network, mutual authentication is essential for physical device and edge server. On the one hand, physical device transmits the raw data only after verifying that the edge server is legitimate. On the other hand, the edge server only allows the authorized physical device to employ the computing resource and to create its Cybertwin. Nevertheless, it is necessary for Cybertwin to authenticate each other before establishing communication in cyberspace, as well as to determine the source of the receiving data.

Privacy: Privacy preservation is a negligible requirement in Cybertwin-driven 6G V2X network. Cybertwin is virtual representative of physical device on the edge network, which invisible increases the risk of device privacy leakage. In order to provide more personalized and intelligent decision-making services, Cybertwin usually possess personal sensitive information of physical device such as the identity information, usage pattern and location information. Nevertheless, there are several honest-but-curious edge server providers faithfully implement computing protocols, but on the other hand secretly collect private information and compromise physical device's privacy. It's also necessary to remove the sensitive information of physical vehicle between Cybertwin communications.

Trust: Trust guarantees that the data provided by both parties is true and credible. In the Cybertwin-driven 6G V2X network, Cybertwin needs to communicate with other twins on the edge server in order to obtain more information. However, some malicious attackers can send wrong messages to their twins, and these wrong messages may be broadcast and adopted by other twins, resulting in wrong deviation results and bad effects on physical devices. Thus, trust management can help Cybertwin filter out false information as well as misbehaving twin nodes.

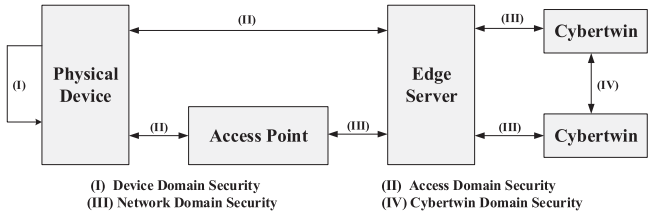


Fig. 2. Security reference architecture of Cybertwin-driven 6G V2X.

B. Security Reference Architecture of Cybertwin-Driven 6G V2X

According to the security requirements and architecture of Cybertwin-driven 6G V2X, we further propose the Cybertwin-driven 6G V2X security reference architecture, as shown in Fig. 2. Four security domains have been defined as device domain security, access domain security, network domain security and Cybertwin domain security. Furthermore, we analyze existing security threats and propose potential solutions in each security domain. The details are as follows.

1) Device domain security (I): The set of security features provide that physical devices can securely perceive and transmit surrounding raw data. Physical device status data is the cornerstone for the Cybertwin, therefore this domain should provide security mechanism which can protect confidentiality and integrity of the collected data, and the availability of physical devices.

In the case of vehicles, on-board sensors are responsible for collecting travel data, and these sensors exchange data with each other via in-vehicle network. In-vehicle network can be divided into wired communication and wireless communication [36]. However, the inherent security issues of the in-vehicle network can influence the performance of on-board sensors and the accuracy of vehicle status sent to the Cybertwin. On the one hand, in-vehicle wireless communication can simplify the vehicle network structure and optimize the vehicle space, but also brings several security threats and challenges [37]. Due to the nature of wireless communication, malicious attackers can easily launch undetectable eavesdropping attack to steal data or even directly tamper with the sensed data between various sensors. On the other hand, in-vehicle wired communication encounters security threats due to the nature of Control Area Network (CAN) protocol, which lacks authentication and encryption mechanism between on-board sensors. In addition, physical attack, such as man-made destruction or device damage, is another threat that can directly interfere the operation of the on-board sensor. Furthermore, considering the limited computing power of on-board sensors, it is not suitable to adopt complex encryption and authentication mechanism based on cryptography techniques, which can impose additional computational burden on the sensors and affect efficiency of real-time data collection.

2) Access domain security (II): The set of security features require physical devices can securely connect to access point and transmit data to the Cybertwin located on edge server. It also requires that the access point is legal and secure which bridges the gap between physical devices and virtual twin. Access domain security mainly guarantees confidentiality and integrity protection of transmitting data, and mutual authentication between physical device and access point against malicious attack on open wireless communication channel.

The primary attacks in the access domain security are eavesdropping, man-in-the-middle attack, personation attack and replay attack. The eavesdropping attack is the most direct and secret, malicious attacker can monitor the data and information transmitted between the physical device and the Cybertwin over the wireless channel [38]. Man-in-the-middle (MITM) attack is one in which attacker can create independent connections with physical device and Cybertwin. Malicious attacker can arbitrarily intercept data and insert false data, causing the Cybertwin to process the wrong data and the physical device to receive the wrong decision instructions [39]. Replay attack is one in which attacker can send data that has been eavesdropped on the channel to physical device or Cybertwin for the purpose of deception [40]. Impersonation attack is a form of attack that attempts to gain access to system by posing as an authorized user [41]. In the Cybertwin-driven 6G V2X network, when an attacker steals the identity of a legally authorized vehicle, he can use it to impersonate the legitimate user and access the edge server to enjoy the Cybertwin V2X service for free. In addition, malicious attacker can even impersonate the edge server or access point to deceive vehicle access in order to obtain the privacy information of vehicle [42].

3) Network domain security (III): The set of security features require that the edge server can operate securely and provide the essential computing and storage resources. The main security requirements of this domain are access authentication, system availability and privacy preservation.

Edge server provides operating environment, services management and essential resources for Cybertwin. However, it is more suspicious to incur security challenges from external and internal malicious attacker. Edge server is vulnerable to Denial of Service (DoS) attack [43], malicious attacker can exploit flaws of network protocols or deplete the resources that prevent edge server from providing services and computing resource to physical device and its virtual counterpart. SQL injection attack is one of the common methods used by malicious attacker to destroy edge server [44]. SQL injection attack can do unexpected harm by building special inputs as parameters to execute SQL statements into the edge server. In addition, SQL injection attack can make the attacker access the edge server illegally, obtain background data and steal sensitive information.

4) Cybertwin domain security (IV): The set of security features guarantee that the Cybertwin can securely process, analyze and store physical device data on the edge server. In addition, it also achieves secure communication between different Cybertwins in the cyberspace. The main security requirements of this domain are data confidentiality and integrity, authentication, privacy preservation, and trust management for Cybertwin.

Cybertwin is the virtual representation and intelligent agent of the vehicle, which means the operating state and component parameters of the vehicle can be analyzed and processed as digital replica in the cyberspace provided by the edge server. However, there are honest-but-curious edge server providers who encourage vehicle to access the edge server and to create Cybertwin with advanced algorithms for better analyzing raw data, but may secretly collude with the edge server to collect vehicle sensitive data and disclose vehicle privacy information such as driving status, location on their benefit.

One of the basic functions of Cybertwin is communication assistant, which means that the Cybertwin can communicate with other entities, such as the core network or other third-party service providers on behalf of the vehicle. Although Cybertwin is the intelligent agent of the physical vehicle, tripartite authentication is necessary between the vehicle, Cybertwin and the third-party service provider, which means that Cybertwin needs to obtain authorization from the vehicle and to authenticate with the third party in order to resist disguise or impersonation attacks.

In the Cybertwin-to-Cybertwin communications, malicious attackers can directly eavesdrop on the edge server or tamper with messages sent between Cybertwins. Malicious attackers can also pretend to be legitimate twins to send false data and to interfere with other Cybertwins. Furthermore, the Cybertwin can share or recommend digital assets to other twins. However, these assets can expose the private information of the vehicle, such as driving route or personal preference. Therefore, malicious attackers can indirectly obtain and analyze the private information of the vehicle after accepting the digital assets shared by the legal twin.

In addition, secure data storage can not be neglected in Cybertwin domain security. The accurate decisions or predictions made by the Cybertwin for vehicle not only rely on the real-time data provided from the vehicle, but also on the stored historical data about vehicle behavior. Attackers or curious servers can peep and steal historical data, causing privacy leakage of physical device. There are several attackers can directly and maliciously tamper with historical data, leading to deviations in decision made by Cybertwin. Furthermore, the rapid mobility of vehicle not only requires the creation and access of new Cybertwin on the new edge server, but also requires the migration of historical data to the new edge server in order to provide data supplements.

C. Potential Security Solutions for Cybertwin-Driven 6G V2X Network

In this subsection, the corresponding potential security solutions are given according to the characteristics, security requirements and security issues of each layer.

1) Device Domain Security (I): Physical layer security (PLS) makes use of the randomness and fading of the wireless channel to improve the legal channel better than the eavesdropping channel, so as to reduce the information leakage [45]. PLS does not depend on encryption algorithm but can realize communication authentication and communication encryption. Physical

layer authentication uses wireless randomness and mutuality to authenticate information or devices. Physical layer encryption is to generate the physical layer key after quantifying the extracted feature information in the wireless channel, so as to realize the encryption of the sent information. PLS has the characteristics of low complexity and low delay, therefore it is more suitable for on-board sensors with low computing power, which can effectively improve the security and reliability of data transmission [46].

2) Access Domain Security (II): Specified by the Third Generation Partnership Project (3GPP) standard, 5G-Authentication and Key Agreement (5G-AKA) protocol is an effective approach to achieve secure communication between physical device and access point via wireless access channel [47]. On the one hand, 5G-AKA protocol provides the primary mutual authentication between physical device and access point against impersonation attack. On the other hand, 5G-AKA protocol supports physical device and access point jointly negotiate session key which can achieve secure communication on access layer against eavesdropping and other attacks. In addition, 5G-AKA protocol also further protects the identity information privacy of the physical device compared to Evolution Packet System-Authentication and Key Agreement (EPS-AKA) protocol [48]. However, recent researches have shown that 5G-AKA protocol still has various vulnerabilities and weaknesses. Syed *et al.* [49] and David *et al.* [50] reveal that there are violations of anchor key and authentication by performing fine-grained formal analysis based on TAMARIN model. Therefore, it is necessary to design a more secure secret key negotiation and robust authentication protocol to remedy these vulnerabilities on the basis of 5G-AKA protocol for Cybertwin-driven 6G V2X network.

3) Network Domain Security (III): Access control mechanism can ensure that legitimate and authorized physical devices can access the protected edge server resources, it also prevents malicious attackers from entering the protected network resources, or legitimate users from accessing unauthorized network resources [51]. Access Control refers to the approach by which the server restricts the ability of user to leverage computing and storage resources. It is usually used by service provider to control user access to network resources such as servers, directories and files. In Cybertwin-driven 6G V2X network, access control mechanism is one of the key strategies to protect the security of network resources.

4) Cybertwin Domain Security (IV): Homomorphic encryption (HE) is a cryptographic technique based on the computational complexity theory of mathematical problem, which allows that the data can be directly calculated and processed without knowing any information [52]. HE provides a way to process encrypted data, which means that result of the operation on the ciphertext is still the result of encryption, and the result obtained by decrypting is the same as performing the same operation on the plaintext. HE can directly overcome the confidentiality issue caused by the edge server snooping on the perceived data processed by Cybertwin. However, since HE often costs high computational overhead and causes a certain delay, it is more suitable for delay-insensitive Cybertwin V2X applications such as IVHM.

Differential Privacy (DP) is a lightweight but substantial privacy preservation technique by adding a certain amount of noise and perturbing original real-time data [53]. DP guarantees that the result of any challenges from an adversary cannot disclose sufficient information about any individual identification. In general, there are two different working mechanisms for differential privacy: central differential privacy (CDP) and local differential privacy (LDP). CDP requires that the existence of a trusted third party can issue private information after processing and perturbing raw data received from data owner, while LDP allows the user to employ the DP strategy to perturb the raw data independently and send it to untrusted server. LDP is more suitable solution to provide privacy preservation for Cybertwin-driven 6G V2X application with higher communication efficiency and lower computation complexity. However, more real-time data perturbation leads to better privacy protection, the accuracy of decision made by Cybertwin could be influenced which will further affect the actual safe driving of the vehicle. Therefore, it is necessary to balance the accuracy and privacy when vehicle locally perturbs real-time data by using DP strategy.

Attribute-based encryption (ABE) is an effective and flexible cryptographic technique for data secure storage and fine-grained access control [54]. The data owner can use the public key to encrypt data, set an access strategy and store these ciphertexts in an untrusted third party, such as central cloud. Only when the attributes of the data users meet the access strategy can they have the right to access and decrypt the corresponding data. There are two main types of attribute encryption, Key-Policy Attribute-based Encryption (KP-ABE) and Ciphertext-Policy Attribute-based Encryption (CP-ABE). In KP-ABE, private key of the data user is associated with the access policy, and the ciphertext is associated with the attribute set. In CP-ABE, the ciphertext corresponds to the access structure and the private key of the data user corresponds to the attribute set. ABE is suitable for Cybertwin V2X application, especially when vehicle is connected to a new edge server. Vehicle can set access policies and store behavior data or feedback decisions in form of ciphertext on the central cloud. Only those newly created Cybertwins that meet the policies and conditions can legally access the encrypted storage data of the vehicle.

IV. A Case Study: Migration of Cybertiwn

Vehicle can enjoy the relevant Cybertwin V2X applications only after accessing the edge server and creating its virtual counterpart. However, due to the rapid mobility of the vehicle and the limited coverage of the edge server, the moving vehicle has to migrate its Cybertwin to the newly accessed edge server. In this section, we take Cybertwin migration as a case study and design a handover authentication scheme for moving vehicle in order to securely access new edge server and further migrate its Cybertwin. Furthermore, the security of the scheme is proved by BAN logic and the effectiveness of the scheme is analyzed.

A. The System Model

The system model is illustrated in Fig. 3, and the entities involved in the scheme consists of Road Trust Authority, Edge Server and Vehicle.

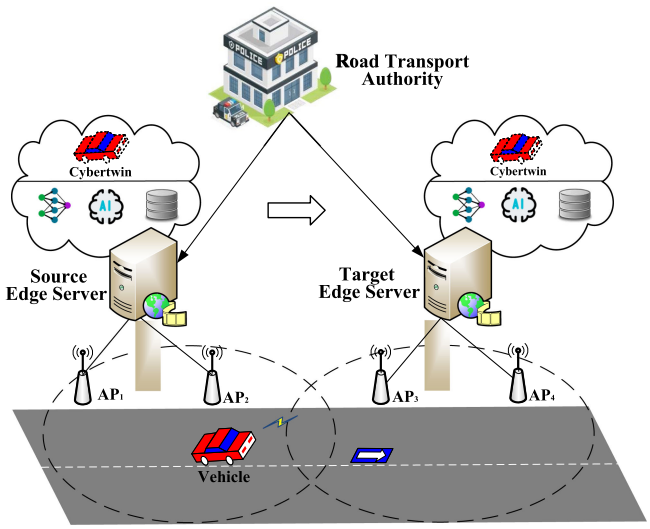


Fig. 3. System model.

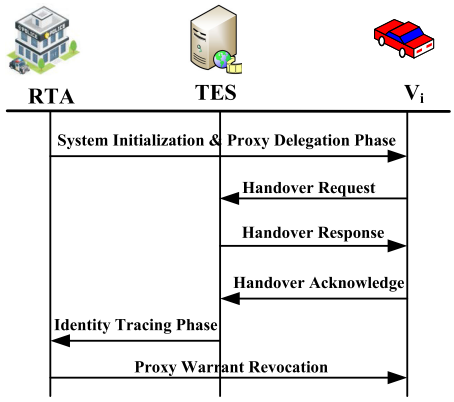


Fig. 4. Process in handover authentication.

TABLE I
NOTATION AND DESCRIPTION

Notation	Description
σ_i	Proxy delegation
w_i	Proxy warrant
s_i	Authentication signature
seq	Sequence number
P	Generator of the group
H_i	Secure hash function
TS	Timestamp
AK	Authentication key
PTK	Pairwise transient key
pk_i/sk_i	Public/private key pair
R_i, y_i	Proxy delegation signature

Road Transport Authority (RTA): RTA plays an important role in the system, which is responsible for the initialization of the system and generation of the public and private key pairs. Furthermore, RTA issues the proxy warrant w for edge server and vehicle. On the one hand, w indicates that the edge server has the capabilities to support the creation and operation of different type of the Cybertwin V2X applications, which has been verified by the RTA to be legitimate and trusted. On the other hand, it indicates that the vehicle has been authorized by RTA and can access the edge server to create the Cybertwin V2X application which listed in the proxy warrant w.

Edge Server (ES): Connected to several access points, edge server has powerful computing and storage resources to support the operation of Cybertwin V2X application. Generally, different types of Cybertwin V2X applications are composed of different deep learning or machine learning algorithms. These algorithms can be used to analyze and to process the input real-time data and stored the historical data of vehicle, and finally give feedback decision to the vehicle. However, edge servers could secretly collect privacy information of the vehicle.

Vehicle (V): Vehicle consists of two parts: the vehicle in the physical world and Cybertwin in the virtual space. Only after being licensed by RTA, the vehicle can create its Cybertwin on the edge server and further enjoy related Cybertwin V2X applications. However, the cruising vehicle has to access new base stations and new edge servers frequently, so the Cybertwin also needs to migrate to the new edge server as the vehicle moves. In addition, vehicles may tamper with the contents of the proxy warrant w in order to enjoy unauthorized Cybertwin V2X applications.

B. Overview

We assume that the vehicle and the access point have already negotiated the session key for secure communication based on 5G-AKA protocol at the beginning. As shown in Fig. 4, firstly, the RTA sends the proxy warrant to the edge server that can support the operation of the Cybertwin V2X application. At the same time, the RTA also issues the proxy warrant to the vehicles that apply for the same Cybertwin V2X application within the same time period. When the vehicle enters the coverage area of the target edge server, the vehicle sends the proxy warrant to the target edge server in order to indicate that it is legal to create Cybertwin and to enjoy Cybertwin V2X application by using resources of edge server. If the validation is correct, the target edge server will allow the vehicle to create the authorized Cybertwin, otherwise edge server will reject the vehicle's access request, and the RTA will manage the tracking. Target edge server sends warrant to vehicle at the same time, in order to show the legitimacy of the identity. If authentication fails, the vehicle refuses to access and remain with the source edge server connection. Otherwise, the vehicle will create Cybertwin on the new edge server and disconnect from the source edge server connection. While the vehicle and the target edge server mutually authenticate each other, the pairwise transient key used to achieve secure communication is jointly negotiated.

C. The Proposed Scheme

First, we detail our proposed scheme for handover authentication between vehicle and edge server, which consists of four phases: system initialization, proxy delegation, handover authentication and identity tracking. Some definitions of notations are listed in Table I.

1) System Initialization Phase: Let κ be a security parameter, G_1 be a cyclic addition group and G_2 be a multiplicative cyclic group of order q ($q > 2^{\kappa}$) with generator P, $e : G_1 \times G_1 \to G_2$ be a bilinear pairing. The RTA executes system initialization. The RTA randomly selects $sk_{rta} \in Z_q^*$ as the system master key and computes $pk_{rta} = sk_{rta} * P$ as the system public key. The RTA selects secure cryptographic hash functions H_1, H_2, H_3, H_4 and H_5, where $H_1 : \{0,1\}^* \times G_1 \to Z_q^*$, $H_2 : \{0,1\}^* \times G_1 \times G_1 \to Z_q^*$, $H_3 : \{0,1\}^* \times G_1 \times G_1 \times G_1 \to Z_q^*$, $H_4 : G_1 \to \{0,1\}^l$ and $H_5 : G_1 \times \{0,1\}^* \to \{0,1\}^l$. The RTA issues system public parameters $params = \{G_1, G_2, e, P, pk_{rta}, H_1, H_2, H_3, H_4, H_5\}$ and keeps sk_{rta} in secret.

The vehicle V selects $sk_v \in Z_q^*$ as private key and computes the public key $pk_v = sk_v * P$ for achieving secure communication. The edge server ES performs the same operations as the vehicle and finally generates the public and private key pairs (sk_{es}, pk_{es}). Furthermore, the V sends identity information (ID_v, pk_v) to the RTA. On receiving ID_v from the V, the RTA stores (ID_v, pk_v) in the local database.

2) Proxy Delegation Phase: In this phase, RTA will issue the proxy delegation for legal edge server and vehicle.

• Between RTA and ES: The RTA verifies that Cybertwin V2X applications such as ADAS or IVHM can operate on each edge server in advance. Different applications are composed of different artificial intelligence, machine learning or simulation algorithms. On the one hand, these algorithms lay the foundation for the operation of the Cybertwin, the vehicle can create its own Cybertwin and enjoy the revelent services by providing real-time status data as input to algorithms; on the other hand, these algorithms will be further optimized and improved as more data is input.

After verifying Cybertwin V2X applications on the ES, the RTA firstly generates an authorization proxy warrant $w_{es} = (\mathrm{ID_{RTA}}, \mathrm{ID_{ES}}, \mathrm{APP_{ES_i}}, \mathrm{ET_{Start}}, \mathrm{ET_{End}})$, where $\mathrm{ID_{RTA}}$ is the identity of the RTA, $\mathrm{ID_{ES}}$ is the identity of the ES, $\mathrm{APP_{ES_i}}$ is the authorized Cybertwin V2X applications, $\mathrm{ET_{Start}}$ and $\mathrm{ET_{End}}$ are the authorization start time and end time for the ES respectively.

Then, the RTA randomly selects $r_{es} \in Z_q^*$ to compute the proxy delegation for ES. The proxy signature pair (y_{es}, R_{es}) of ES is computed as follows:

$$\begin{aligned} R_{es} &= r_{es} * P \\ h_{es} &= H_1(w_{es}, R_{es}) \\ y_{es} &= (r_{es} + h_{es} * sk_{rta}) \ mod \ q \end{aligned}$$

Finally, the proxy delegation $\sigma_{es} = (w_{es}, y_{es}, R_{es})$ is sent to the ES from the RTA via secure channel.

On receiving the σ_{es}, the ES first checks the contents of w_{es} and determines whether the σ_{es} is correct by verifying the following equations.

$$\begin{aligned} h_{es} &= H_1(w_{es}, R_{es}) \\ y_{es} * P &= (r_{es} + h_{es} * sk_{rta}) * P \\ &= R_{es} + h_{es} * pk_{rta} \end{aligned}$$

If the verification fails, the ES will request the valid proxy delegation from the RTA again. Otherwise, the ES receives proxy delegation σ_{es} which will be used to show the authority and legitimacy of the ES to the vehicle $\mathrm{V_i}$ in handover authentication phase.

• Between RTA and $\mathrm{V_i}$: Only with the permission and authorization of the RTA can the vehicle access the edge server and create its own Cybertwin. Assuming there are a certain number of vehicle users $\mathrm{V} = (\mathrm{V_1}, \mathrm{V_2}, \ldots, \mathrm{V_n})$ who are applying for authorization from the RTA, each vehicle user sends $(\mathrm{ID_i}, \mathrm{APP_i})$ to the RTA via secure channel.

On receiving $(\mathrm{ID_i}, \mathrm{APP_i})$, the RTA checks the number of vehicle user applying for the same application in the same period. If the applied users exceeds a certain number, such as 10 users, the RTA first generates an authorization warrant $w_v = (\mathrm{ID_{RTA}}, \mathrm{L}, \mathrm{APP_{V_i}}, \mathrm{VT_{Start}}, \mathrm{VT_{End}})$ for these vehicle users who apply for the same application in the period, where L is the public key information string of these vehicles, $\mathrm{APP_{V_i}}$ is the Cybertwin V2X application that vehicle can create, $\mathrm{VT_{Start}}$ and $\mathrm{VT_{End}}$ are the authorization start time and end time for each vehicle user $\mathrm{V_i}$.

Then, the RTA selects random number $r_{v_i} \in Z_q^*$ and computes the proxy delegation σ_{v_i} for $\mathrm{V_i}$. The proxy signature pair (y_{v_i}, R_{v_i}) is generated as follows:

$$\begin{aligned} R_{v_i} &= r_{v_i} * P \\ h_{v_i} &= H_1(w_v, R_{v_i}) \\ y_{v_i} &= (r_{v_i} + sk_{rta} * h_{v_i}) \ mod \ q \end{aligned}$$

Similarly, the RTA transmits the proxy delegation $\sigma_{v_i} = (w_v, y_{v_i}, R_{v_i})$ to the applying vehicle users $\mathrm{V} = (\mathrm{V_1}, \mathrm{V_2}, \ldots, \mathrm{V_n})$ via secure channel.

After receiving the proxy delegation $\sigma_{v_i} = (w_v, y_{v_i}, R_{v_i})$ from the RTA, each vehicle user reviews whether information in authorization warrant w_v is correct and validates the received proxy delegation as follows:

$$\begin{aligned} y_{v_i} * P &= (r_{v_i} + sk_{rta} * h_{v_i}) * P \\ &= R_{v_i} + h_{v_i} * pk_{rta} \end{aligned}$$

If the verification is correct, the vehicle accepts σ_{v_i} as proxy delegation.

3) Handover Authentication Phase: Assuming that $\mathrm{V_i}$ has already accessed to a source edge server SES and created its Cybertwin. When the $\mathrm{V_i}$ is about to move from the coverage of SES to the coverage of target edge server TES, the $\mathrm{V_i}$ triggers handover authentication procedure with the TES in order to migrate new Cybertwin and to guarantee the QoE of Cybertwin V2X application.

Step1: $\mathrm{V_i} \to \mathrm{TES}$: HANDOVER REQUEST Req_{V_i}

- The $\mathrm{V_i}$ first selects a random number $k_i \in Z_q^*$ to compute $K_{v_i} = k_i * P$.
- Then, the $\mathrm{V_i}$ generates timestamp TS_1 and randomly chooses $\lambda \in Z_q^*$, $\varepsilon_j \in Z_q^* (j = 1, 2, \ldots, i-1, i+1, \ldots, n)$ to compute h_2 and ε_i as follows where pk_j is the public key information of each authorized vehicle listed

in L.

$$X_1 = \lambda * P + \sum_{j \neq i}^{n} \varepsilon_j * pk_j$$

$$X_2 = h_{v_i} * pk_{rta} + R_{v_i} + h_{v_i} * K_{v_i}$$

$$h_2 = H_2(w_v || TS_1, X_1, X_2)$$

$$\varepsilon_i = h_2 - \sum_{j \neq i}^{n} \varepsilon_j;$$

Furthermore, the $\mathrm{V_i}$ computes proxy ring authentication signature pair (s_{v_1}, s_{v_2}) as follows:

$$s_{v_1} = (\lambda - \varepsilon_i * sk_{v_i}) \ mod \ q$$

$$s_{v_2} = (y_{v_i} + k_i * h_{v_i}) \ mod \ q$$

- In order to prevent disclosure of w_v and replay attack, the $\mathrm{V_i}$ generates a sequence number seq and selects $\alpha_i \in Z_q^*$ to compute A_i, U_i and ciphertext C_i as follows:

$$A_i = \alpha_i * P$$

$$U_i = \alpha_i * pk_{tes}$$

$$C_i = (w_v || seq) \oplus H_4(U_i)$$

In addition, the $\mathrm{V_i}$ chooses $t_j \in Z_q^*$ $(j = 1, 2, \ldots, n)$ and computes tracking factors as follows:

$$TK_j = t_j * pk_j$$

$$T_j = t_j * P$$

$$T = sk_{v_i} * \left(\sum_{j=1}^{n} T_j \right)$$

- When the $\mathrm{V_i}$ enters the coverage area of the TES, the $\mathrm{V_u}$ sends the Handover Request message including $Req_{V_i} = (C_i, A_i, R_{v_i}, K_{v_i}, s_{v_1}, s_{v_2}, T, W, TS_1)$ to the TES where $W = (\varepsilon_j, TK_j, j = 1, 2 \ldots, n)$.

Step2: TES→$\mathrm{V_i}$: HANDOVER RESPONSE Rep_{tes}, MAC_1

- On receiving message from the $\mathrm{V_i}$, the TES first verifies freshness of TS_1. Then the TES uses private key sk_{tes} to compute U_i and to decrypt w_v from C_i as follows:

$$U_i = sk_{tes} * A_i = sk_{tes} * \alpha_i * P$$

$$w_v || seq = C_i \oplus H_4(U_i)$$

- Next, the TES checks the correctness of w_v and verifies legitimacy of the $\mathrm{V_i}$ as follows:

$$h_{v_i} = H_1(w_v, R_{v_i})$$

$$E = s_{v_1} * P + \sum_{j=1}^{n} (\varepsilon_j * pk_j)$$

$$s_{v_2} * P = h_{v_i} * pk_{rta} + R_{v_i} + h_{v_i} * K_{v_i}$$

$$\sum_{j=1}^{n} (\varepsilon_j) = H_2(w_v || TS_1, E, s_{v_2} * P)$$

- If the validation fails, the TES quits the handover authentication and sends (w_v, T, TK_j) to the RTA in order to trace the true identity of $\mathrm{V_i}$. Otherwise, the TES believes that the $\mathrm{V_i}$ has been legally authorized by the RTA and allows the $\mathrm{V_i}$ to access edge server and to create corresponding Cybertwin. The TES selects $k_{tes} \in Z_q^*$ to generate the pairwise transient key PTK according to the Equations (1)-(3), where AK will be used to confirm the successful handvoer authenticaiton and PTK will be used as a temporary session key for encrypting real-time data and establishing secure communication channel between TES and $\mathrm{V_i}$.

$$K_{tes} = k_{tes} * P \tag{1}$$

$$AK = k_{tes} * K_{v_i} \tag{2}$$

$$PTK = H_5(AK, w_v, w_{tes}, seq + 1) \tag{3}$$

- Then, the TES selects a random number $z_{tes} \in Z_q^*$ and generates Timestamp TS_2 to compute authentication signature s_{tes} and message authentication code MAC_1 as follows:

$$Z_{tes} = z_{tes} * P$$

$$n_{tes} = H_3(w_{tes}, TS_2, R_{tes}, Z_{tes}, K_{tes})$$

$$s_{tes} = (y_{tes} + z_{tes} + sk_{tes} * n_{tes}) \ mod \ q$$

$$MAC_1 = H_5(AK, PTK, seq + 1, TS_2)$$

- The TES sets Handover Response message which includes $Rep_{tes} = (w_{tes}, s_{tes}, R_{tes}, Z_{tes}, K_{tes}, TS_2)$ and MAC_1. The TES sends Handover Response message to the $\mathrm{V_i}$.

Step3: $\mathrm{V_i}$→TES: ACKNOWLEDGE MAC_2, TS_3

- On receiving Rep_{tes} from the TES, the $\mathrm{V_i}$ checks the freshness of TS_2 and recalculates h_{tes}, n_{tes}. Then, the $\mathrm{V_i}$ verifies the legitimacy of the TES as follows:

$$h_{tes} = H_1(w_{tes}, R_{tes})$$

$$s_{tes} * P = R_{tes} + Z_{tes} + h_{tes} * pk_{rta} + n_{tes} * pk_{tes}$$

- If the equation does not hold, the $\mathrm{V_i}$ quits authentication with TES and remains connected to the source edge server SES. Otherwise, the $\mathrm{V_i}$ can compute AK and PTK as follows:

$$AK = k_i * K_{tes}$$

$$PTK = H_5(AK, w_{tes}, w_v, seq + 1)$$

- Then, the $\mathrm{V_i}$ recalculates MAC_1' and verifies Equation (4). If the verification is correct, the $\mathrm{V_i}$ can consider that the TES is authorized and can access the TES to create its Cybertwin.

$$MAC_1' = MAC_1 \tag{4}$$

- Finally, the V_i generates Timestamp TS_3 and sends Acknowledge message which includes MAC_2 to the TES as handover authentication confirmation.

$$MAC_2 = H_5(AK, PTK, seq + 2, TS_3)$$

4) Identity Tracking Phase: If the vehicle has malicious or dispute behavior that causes the handover authentication failure, such as tampering with the content of the warrant w_v to enjoy unauthorized Cybertwin V2X applications, the RTA needs to intervene in the investigation and to reveal the true identity of the vehicle.

- The TES sends (w_v, T, TK_j) to the RTA via secure channel. Only the RTA has the right to ask each vehicle member V_j on the w_v for tracing factor as follows:

$$T_j = sk_j^{-1} * TK_j$$

- After receiving T_j from each vehicle V_j, the RTA verifies $e(TK_j, P) = e(T_j, pk_j)$. If the validation fails, the RTA considers T_j to be invalid and suspects that the corresponding vehicle is dishonest. Otherwise, the RTA can obtain the public key pk_{v_i} and find (ID_{v_i}, pk_{v_i}) from local storage according to the Equations (5)-(6).
- Finally, the RTA further outputs the vehicle's true identity information ID_{v_i}. If the $\mathrm{V_i}$ does have malicious behavior, the RTA will eventually revoke the proxy warrant w_v granted to the vehicle $\mathrm{V_i}$.

$$B = \sum_{j=1}^{n} T_j \tag{5}$$

$$e(T, P) = e(B, pk_{v_i}) \tag{6}$$

D. Security Analysis

In this subsection, we first analyze the security properties informally and further give the logic proof of the proposed scheme based on Burrows-Abadi-Needham (BAN) logic.

1) Security Properties: The informal security properties is analyzed.

Mutual Authentication: The proposed scheme can achieve the mutual authentication between $\mathrm{V_i}$ and TES according to the proxy warrant w issued by the TES during handover phase. The $\mathrm{V_i}$ sends the encrypted w_v and proxy signature to the TES. After receiving the message, the TES can decrypt and obtain the w_v by using the private key sk_{tes}. Since the proxy signature is not forgeable, the modified proxy warrant and the forged proxy signature cannot be verified. Therefore, the TES can verify whether the proxy signature is correct according to Equations (7)-(8). Similarly, after receiving the proxy signature and proxy warrant sent by the TES, the $\mathrm{V_i}$ can determine the legitimacy of TES by verifying whether Equation (9) is correct. Thus, the proposed scheme can achieve mutual authentication between $\mathrm{V_i}$ and TES through the proxy delegation and warrant issued by the RTA.

$$\begin{aligned} s_{v_2} * P &= (y_{v_i} + k_i * h_{v_i}) * P \\ &= (r_{v_i} + sk_{rta} * h_{v_i} + k_i * h_{v_i}) * P \\ &= (R_{v_i} + h_{v_i} * pk_{rta} + h_{v_i} * K_{v_i}) \end{aligned} \tag{7}$$

$$\begin{aligned} \sum_{j=1}^{n}(\varepsilon_j) &= H_2(w_v||TS_1, E, s_{v_2} * P) \\ &= H_2(w_v||TS_1, s_{v_1} * P + \sum_{j=1}^{n}(\varepsilon_j * pk_j), s_{v_2} * P) \\ &= H_2(w_v||TS_1, (\lambda - \varepsilon_i sk_{v_i}) * P \\ &\quad + \sum_{j=1}^{n}(\varepsilon_j * pk_j), s_{v_2} * P) \\ &= H_2(w_v||TS_1, \lambda * P + \sum_{j\neq i}^{n} \varepsilon_j * pk_j, s_{v_2} * P) \\ &= H_2(w_v||TS_1, X_1, R_{v_i} + h_{v_i} * pk_{rta} + h_{v_i} * K_{v_i}) \\ &= H_2(w_v||TS_1, X_1, X_2) \\ &= h_2 \end{aligned} \tag{8}$$

$$\begin{aligned} s_{tes} * P &= (y_{tes} + z_{tes} + sk_{tes} * n_{tes}) * P \\ &= (r_{tes} + z_{tes} + h_{tes} * sk_{rta} + sk_{tes} * n_{tes}) * P \\ &= R_{tes} + Z_{tes} + h_{tes} * pk_{rta} + n_{tes} * pk_{tes} \end{aligned} \tag{9}$$

In addition, the $\mathrm{V_i}$ and the TES can verify the validity of the identity by computing the correctness of the MAC_i. Since the seq is hidden in C_i, only the legal TES can use the private key sk_{tes} to decrypt the seq and further calculate the MAC_1. If the $\mathrm{V_i}$ fails to validate MAC_1, it can be deduced that the TES does not decrypt to obtain the correct seq or that the message is tampered with by malicious attacker.

Key Agreement: In the proposed scheme, the pairwise transient key PTK can be negotiated between the $\mathrm{V_i}$ and the TES based on $AK, w_v, w_{tes}, seq + 1$. The two parties can independently derive the authentication key and pairwise transient key. In addition, the relevant parameters used to calculate the session key are not transmitted publicly in the communication channel. On the one hand, according to CDH, even though there is malicious attack can eavesdrop $k_{tes} * P$ and $k_i * P$ from public channel, it is difficult to calculate secret key $AK = k_{tes} * k_i * P$ without k_{tes} and k_i. On the other hand, only the legal TES can obtain w_v and seq by utilizing the private key sk_{tes}.

Withstanding Attacks: First, the proposed scheme can resist replay attack by using the sequence number which has been encrypted by pk_{tes}. Second, the scheme can realize the integrity protection by using the message authentication code. Without knowing seq and AK, the malicious attacker cannot generate the tampered message into MAC that can be verified by the vehicle. In addition, by using the timestamp, the proposed scheme is resistant to Man-in-Middle attacks. If the $\mathrm{V_i}$ or the TES receives the timestamp attached to handover message that exceeds the time threshold, authentication will be quitted. Even if a malicious attacker tampers with the timestamp, the correct MAC cannot be generated.

Anonymity: The proposed scheme can achieve unconditional anonymity for the $\mathrm{V_i}$ during handover authentication phase. The TES just can infer that the $\mathrm{V_i}$ is legal and belongs to set of proxy signers $\mathrm{V} = (\mathrm{V_1}, \mathrm{V_2}, \ldots, \mathrm{V_n})$ by verifying the correctness of

w_V. The probability that the TES can conclude the true identity of the $\mathrm{V_i}$ is not more than $\frac{1}{n}$.

Traceability: When malicious or dispute behavior occurs, the RTA can reveal the true identity of the $\mathrm{V_i}$. The RTA has the right to collect T_j from members of each vehicle listed on the w_v. The RTA verifies the correctness of T_j as follows:

$$\begin{aligned} e(TK_j, P) &= e(t_j * sk_j * P, P) \\ &= e(t_j * P, sk_j * P) \\ &= e(T_j, pk_j) \end{aligned}$$

If the verification is correct, the RTA can find pk_{v_i} according to Equation (10). The RTA can output the true identity information of vehicle based on (ID_{v_i}, pk_{v_i}) stored on the local server.

$$\begin{aligned} e(T, P) &= e\left(\sum_{j=1}^{n} sk_{v_i} * T_j, P\right) \\ &= e\left(\sum_{j=1}^{n} T_j, sk_{v_i} * P\right) \\ &= e(B, pk_{v_i}) \end{aligned} \tag{10}$$

2) Logic Proof by BAN Logic: BAN logic is modal logic based on subject knowledge and belief reasoning, which is proposed by Michael Burrows, Martin Abadi and Roger Needham. The BAN logical has been widely used to prove that the protocol can achieve the mutual authentication and key agreement by deducing whether the subject can obtain the belief from the received message. We first give the rules of BAN Logic that need to be used in the proof as follows:

1) The fresh-promotion rule: $\frac{P|\equiv\sharp(X)}{P|\equiv\sharp(X,Y)}$
2) The nonce-verification rule: $\frac{P|\equiv\sharp(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$
3) The decomposition rule: $\frac{P|\equiv Q|\equiv(X,Y)}{P|\equiv Q|\equiv X}$, $\frac{P|\equiv(X,Y)}{P|\equiv X}$
4) The composition rule: $\frac{P|\equiv X, P|\equiv Y}{P|\equiv(X,Y)}$
5) The jurisdiction rule: $\frac{P|\equiv Q|\Rightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$
6) The message-meaning rule: $\frac{P|\equiv P\overset{K}{\leftrightarrow}Q, P\{X\}_K}{P|\equiv Q|\sim X}$

Then, we list the goals of proposed scheme in BAN-logic as follows:

1) Goal1: $\mathrm{V_i}|\equiv \mathrm{V_i} \overset{PTK}{\longleftrightarrow} \mathrm{TES}$
2) Goal2: $\mathrm{TES}|\equiv \mathrm{TES} \overset{PTK}{\longleftrightarrow} \mathrm{V_i}$
3) Goal3: $\mathrm{V_i}|\equiv \mathrm{TES}|\equiv \mathrm{TES} \overset{PTK}{\longleftrightarrow} \mathrm{V_i}$
4) Goal4: $\mathrm{TES}|\equiv \mathrm{V_i}|\equiv \mathrm{V_i} \overset{PTK}{\longleftrightarrow} \mathrm{TES}$

We give the five essential but reasonable assumptions as follows in order to better analyze the proposed scheme:

1) Assumption1: $\mathrm{TES}|\equiv \mathrm{V_i}|\Rightarrow Req_{V_i}$
2) Assumption2: $\mathrm{TES}|\equiv \sharp(\mathrm{TS_1})$
3) Assumption3: $\mathrm{TES}|\equiv \sharp(\mathrm{TS_3})$
4) Assumption4: $\mathrm{V_i}|\equiv \mathrm{TES}|\Rightarrow Rep_{tes}$
5) Assumption5: $\mathrm{V_i}|\equiv \sharp(\mathrm{TS_2})$

We prove that the proposed scheme can achieve mutual authentication and establish session key between TES and $\mathrm{V_i}$ according to the BAN logic as follows:

Since TES received Req_{V_i}, we have:

S1: $\mathrm{TES} \lhd Req_{V_i}$

According to Assumation2 and the fresh-promotion rule, we have:

S2: $\mathrm{TES}|\equiv \sharp(Req_{V_i})$

If Equations (7) and (8) are correct, according to S1, we have:

S3: $\mathrm{ES_t}|\equiv \mathrm{V_i}|\sim Req_{V_i}$

According to S2, S3 and the nonce-verification rule, we have:

S4: $\mathrm{TES}|\equiv \mathrm{V_i}|\equiv Req_{V_i}$

According to S4 and the decomposition rule, we have:

S5: $\mathrm{TES}|\equiv \mathrm{V_i}|\equiv k_i * P$, $\mathrm{TES}|\equiv \mathrm{V_i}|\equiv (w_v, seq)$

According to S5, Assumption1 and jurisdiction rule, we have:

S6: $\mathrm{TES}|\equiv k_i * P$, $\mathrm{TES}|\equiv (w_v, seq)$

In the scheme, TES randomly selects $k_{tes} \in Z_q^*$, we have:

S7: $\mathrm{TES}|\equiv k_{tes}$,

According to S6, S7 and the composition rule, we have:

S8: $\mathrm{TES}|\equiv AK = k_{tes} * k_i * P$

That is, $\mathrm{TES}|\equiv \mathrm{TES} \overset{AK}{\longleftrightarrow} \mathrm{V_i}$

Since TES has already kept the w_{tes}, according to S6, S8 and composition rule, we have:

S9: $\mathrm{TES}|\equiv PTK = H_5(AK, w_{tes}, w_v, seq+1)$

That is, $\mathrm{TES}|\equiv \mathrm{TES} \overset{PTK}{\longleftrightarrow} \mathrm{V_i}$ (Goal 2)

Since $\mathrm{V_i}$ received (Rep_{tes}, MAC_1), we have

S10: $\mathrm{V_i} \lhd (Rep_{tes}, MAC_1)$

According to Assumption5 and the fresh-promotion rule, we have:

S11: $\mathrm{V_i}|\equiv \sharp(Rep_{tes})$

If Equation (9) is correct, according to S10, we have:

S12: $\mathrm{V_i}|\equiv \mathrm{TES}|\sim Rep_{tes}$

According to S11, S12 and the nonce-verification rule, we have:

S13: $\mathrm{V_i}|\equiv \mathrm{TES}|\equiv Rep_{tes}$

According to S13 and the decomposition rule, we have:

S14: $\mathrm{V_i}|\equiv \mathrm{TES}|\equiv k_{tes} * P$, $\mathrm{V_i}|\equiv \mathrm{TES}|\equiv w_{tes}$

According to S14, Assumption 4 and the jurisdiction rule, we have:

S15: $\mathrm{V_i}|\equiv k_{tes} * P$, $\mathrm{V_i}|\equiv w_{tes}$

Since $\mathrm{V_i}$ randomly selects k_i, we have:

S16: $\mathrm{V_i}|\equiv k_i$

According to S15, S16 and the composition rule, we have:

S17: $\mathrm{V_i}|\equiv AK = k_i * k_{tes} * P$

That is, $\mathrm{V_i}|\equiv \mathrm{V_i} \overset{AK}{\longleftrightarrow} \mathrm{TES}$

Since $\mathrm{V_i}$ has already kept the w_v and seq, according to S15, S17 and composition rule, we have:

S18: $\mathrm{V_i}|\equiv PTK = H_5(AK, w_{tes}, w_v, seq+1)$

That is, $\mathrm{V_i}|\equiv \mathrm{V_i} \overset{PTK}{\longleftrightarrow} \mathrm{TES}$ (Goal 1)

Since TES received MAC_2 we have:

S19: $\mathrm{TES} \lhd MAC_2$,

According to to S8, S19 and the message-meaning rule, we have:

S20: $\mathrm{TES}|\equiv \mathrm{V_i}| \sim (PTK, TS_3, seq+2)$

According to Assumption3 and the fresh-promotion rule, we have:

S21: $\mathrm{TES}|\equiv \sharp(PTK, TS_3, seq+2)$

According to S20, S21 and the nonce-verification rule, we have:

S22: $\mathrm{TES}|\equiv \mathrm{V_i}|\equiv (PTK, TS_3, seq+2)$

According to S22 and the decomposition rule, we have:
S23: $\mathrm{TES}|\equiv \mathrm{V_i}|\equiv PTK$
That is, $\mathrm{TES}|\equiv \mathrm{V_i}|\equiv \mathrm{V_i} \overset{PTK}{\longleftrightarrow} \mathrm{TES}$ (Goal 4)
Since $\mathrm{V_i}$ received MAC_1, we have:
S24: $\mathrm{V_i} \lhd MAC_1$
According to S17, S24 and message meaning rule, we have:
S25: $\mathrm{V_i}|\equiv \mathrm{TES}| \sim (PTK, TS_2, seq+1)$
According to Assumption5 and fresh promotion rule, we have:
S26: $\mathrm{V_i}|\equiv \sharp(PTK, TS_2, seq+1)$
According to S25, S26 and the nonce-verification rule, we have:
S27: $\mathrm{V_i}|\equiv \mathrm{TES}|\equiv (PTK, TS_2, seq+1)$
According to S27 and the decomposition rule, we have:
S28: $\mathrm{V_i}|\equiv \mathrm{TES}|\equiv PTK$
That is, $\mathrm{V_i}|\equiv \mathrm{TES}|\equiv \mathrm{TES} \overset{PTK}{\longleftrightarrow} \mathrm{V_i}$ (Goal 3)

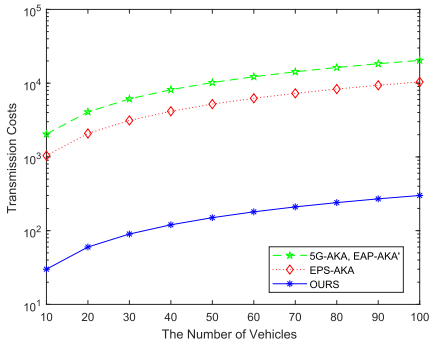
E. Performance Evaluation

In this subsection, we analyze the performance of proposed scheme in terms of transmission costs, bandwidth consumption and computation costs during handover authentication phase respectively.

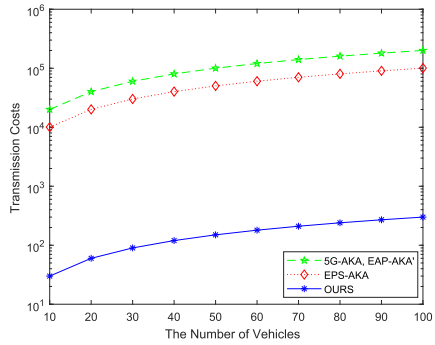
1) Transmission Costs: Here, we compare our proposed scheme with the standard mechanisms: 5G-AKA [47], EAP-AKA' [47] and EPS-AKA [55]. The transmission costs consumed in 5G-AKA and EAP-AKA' is $3+4b+2c$ and in EPS-AKA is $4+2b$, where b indicates the authentication packet unit forwarded between SN (AMF) and HN (AUSF), and c indicates the authentication packet unit forwarded between AUSF and UDM. The scheme we propose handover authentication for migration of Cybertwin consumes 3 unit. In addition, signaling cost, namely number of signaling messages, consumed in 5G-AKA and EAP-AKA' is 9, consumed in EPS-AKA is 6 and consumed in our proposed scheme is 3. As shown in Fig. 5, we can obtain that transmission costs of our proposed scheme is better than other protocols.

2) Bandwidth Consumption: Let q be 256 bits in ECC algorithm, the outputs length of the hash function is 128 bits, the size of the random number is 128 bits, the size of warrant is 128 bits, the length of identity and the size of timestamp are 32 bites. Bandwidth consumption is sizes of authentication messages. The bandwidth consumed for vehicle in 5G-AKA is $(1920+786t)n$ bits, in EAP-AKA' is $(2048+768t)n$ bits, in EPS-AKK is $(896+640t)n$ bits and in our proposed scheme is $(1120+256m)n$ bits, where t is number of authentication vectors (AVs) delivered by the AUSF, n is number of vehicles and m is number of public keys listed in proxy warrant. As shown in Fig. 6, with the number of m increases, that is, the more public keys on the proxy warrant, the bandwidth consumption of our proposed scheme increases, but it can bring better anonymity for vehicle during handover authentication. In addition, we can see that our proposed scheme is less than other protocols in bandwidth consumption from Fig. 6.

3) Computation Costs: We only consider the computation costs for the cryptographic primitive operation during the authentication process, in terms of hash function T_h, the point addition operation T_a, the modular exponentiation operation

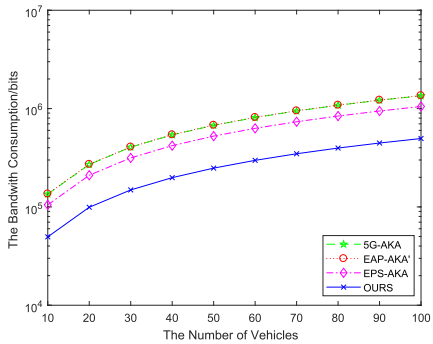


(a)

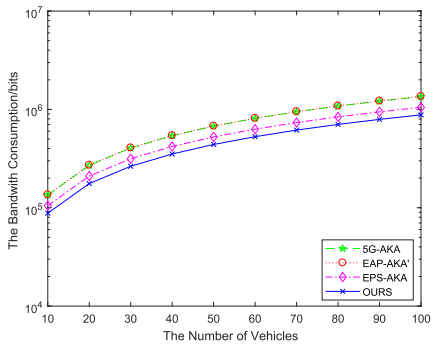


(b)

Fig. 5. Comparison of the transmission costs. (a) $b=50$ and $c=0.4$. (b) $b=500$ and $c=0.4$.



(a)

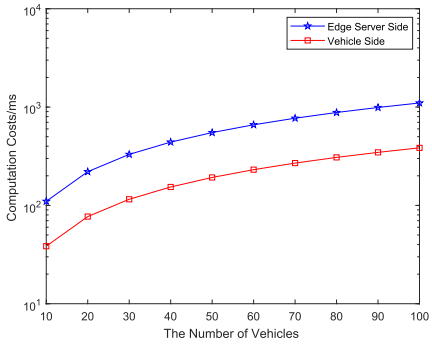


(b)

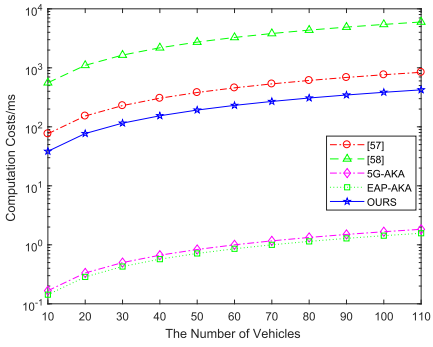
Fig. 6. Comparison of bandwidth consumption. (a) $m=15$ and $t=15$. (b) $m=30$ and $t=15$.

TABLE II
COMPUTATION COSTS OF THE PRIMITIVE CRYPTOGRAPHY OPERATIONS

User \ Time (ms)	T_h	T_a	T_m	T_e	T_p
V_i	0.00238	0.00253	0.96	1.89	16.5
TES	0.00139	0.00121	0.5	1	8.36



(a)



(b)

Fig. 7. Comparison of computation costs. (a) Between vehicle side and edge side of our proposed scheme. (b) Between our proposed scheme and other protocols on vehicle side.

T_e, the bilinear pairing operation T_p and point multiplication operation T_m. The above operations have been investigated in [56] by using OpenSSL with Intel m3-6Y30 CPU @0.9 GHz as V_i and Intel i7-7500 U CPU @2.70 GHz as TES. The details of the computation cost are listed in Table II.

We compare the computation costs used for the vehicle V_i side and target edge server the TES side during handover authentication phase. The computation costs for edge server is $(4T_h + (7+m)T_m)n\,ms$ and for vehicle is $(3T_h + 4T_m)n\,ms$. Let's assume that the public key information for 15 vehicles is listed in the proxy warrant, namely $m = 15$, and the vehicle has already calculated the request message Req_{V_i} before entering the coverage area of TES, it can be seen from the Fig. 7(a) that the computation costs of the V_i side is much lower than that of the TES side. In addition, we also compare the computation costs on vehicle side in the related protocols. The computation costs of vehicle side in [57] is $(4T_m + T_a + 2T_e + 5T_h)n\,ms$, in [58] is $(3n+1)T_p + 2nT_e + 4nT_h + nT_m\ ms$, in 5G-AKA is $7nT_h\ ms$ and in EPS-AKA is $6nT_h\ ms$. From the Fig. 7(b), we can derive that our proposed scheme is better than [57] and [58] but weaker than 5G-AKA and EPS-AKA which adopt symmetric encryption and ignore the protection of identity information.

V. FUTURE RESEARCH DIRECTION

According to the characteristics of Cybertwin, security requirements and the security reference architecture proposed in Section III, we further put forward several promising research directions in order to achieve more secure Cybertwin-driven 6G V2X network in the future.

A. Secure and Flexible Data Migration

Cybertwin is fed not only on by real-time data, but also on historical data from the physical vehicle. The historical data includes the historical behavior of the vehicle and the results of previous edge server analysis. Considering the limited storage capacity of the vehicle, the historical data is often saved by edge servers. However, due to the mobility of the vehicles, Cybertwin also needs to be connected to and migrated to the new edge server along with the vehicles. In order to keep the Cybertwin operation accurately, the historical data should also be seamlessly and flexibly migrated to the new edge server. At the same time, the historical data stored on the source edge server also should be destroyed in order to prevent the leakage of vehicle data. During the migration of historical data phase, the authentication and integrity of the history data need to be protected against malicious attacks. Therefore, how to enable the secure migration of historical data to the new edge server with Cybertwin is a key issue in Cybertwin-driven 6G V2X network.

B. Secure and Lightweight Communication Protocol

A secure and efficient communication protocol is essential in Cybertwin-driven 6G V2X network. New communication and computation technology will be introduced to support operation of Cybertwin, which can inevitably lead to new communication security. In addition, dynamic topology and open wireless channel in the V2X is still more vulnerable to protocol attacks, such as sybil attack, man-in-the-middle attack, etc. Therefore, it is necessary to design a secure communication protocol, which should achieve secure communication, authentication, and resistance to various attacks between vehicle, edge server and Cybertwin. In addition, as oceans of devices applying for access to edge servers to create Cybertwin, the communication protocol should have low communication overhead to prevent signaling storms or outages of access edge server. Furthermore, for several time-sensitive V2X applications of Cybertwin, the communication protocol should also have low computational overhead to reduce latency.

C. Secure and Privacy-Preserving Data Processing

Cybertwin needs computing and storage resources provided by the edge server to operate, analyze and process the real-time raw data from its physical devices. However, as described in Section III, the outsourcing of raw data causes the physical device to lose ownership of the data. Curious edge servers may secretly record the data processed, resulting in a breach of privacy. In

addition, malicious servers can also corrupt data processing, resulting in the wrong operation of Cybertwin and physical devices. However, security and efficiency are contradictory. Although several cryptographic schemes, such as homomorphic encryption, can protect data confidentiality and privacy, it is not realistic for time-sensitive V2X applications due to the heavy computing overhead that would introduce intolerable delays. Therefore, it is essential to design a secure and efficient data processing protocol which can balance secure data processing and operation efficiency.

VI. Conclusion

In this paper, we first presented the four-layer architecture and several promising applications of Cybertwin-driven 6G V2X network. Then, we analyzed the requirements of security and privacy preservation in Cybertwin-driven 6G V2X network. Particularly, we proposed the security reference architecture of Cybertwin-driven 6G V2X network and analyzed the potential security solutions to solve exiting security and privacy issues. In addition, we investigated the migration of Cybertwin of moving vehicle as a case study, and proposed a handover authentication scheme to support Cybertwin migration between vehicle and edge server. We also performed security analysis and performance evaluation on the proposed scheme. Finally, we pointed out future research directions in achieving secure Cybertwin-driven 6G V2X network.

References

[1] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," *Comput. Netw.*, vol. 167, 2020, Art. no. 106984.

[2] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May/Jun. 2020.

[3] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?," *Nature Electron.*, vol. 3, no. 1, pp. 20–29, 2020.

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

[5] S. Zhang, H. Zhang, and L. Song, "Beyond D2D: Full dimension UAV-to-everything communications in 6G," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6592–6602, Jun. 2020.

[6] P. K. Padhi and F. Charrua-Santos, "6G enabled industrial internet of everything: Towards a theoretical framework," *Appl. Syst. Innov.*, vol. 4, no. 1, pp. 1–28, 2021.

[7] S. Nayak and R. Patgiri, "6G communication technology: A vision on intelligent healthcare," *Health Informatics: A Computational Perspective in Healthcare*. Singapore: Springer, 2021, pp. 1–18.

[8] H. X. Nguyen, R. Trestian, D. To, and M. Tatipamula, "Digital twin for 5G and beyond," *IEEE Commun. Mag.*, vol. 59, no. 2, pp. 10–15, Feb. 2021.

[9] W. Sun, H. Zhang, R. Wang, and Y. Zhang, "Reducing offloading latency for digital twin edge networks in 6G," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12 240–12 251, Oct. 2020.

[10] Y. Zheng, R. Lu, Y. Guan, S. Zhang, and J. Shao, "Towards private similarity query based healthcare monitoring over digital twin cloud platform," in *Proc. IEEE/ACM 29th Int. Symp. Qual. Serv.*, 2021, pp. 1–10.

[11] M. Pengnoo, M. T. Barros, L. Wuttisittikulkij, B. Butler, A. Davy, and S. Balasubramaniam, "Digital twin for metasurface reflector management in 6G terahertz communications," *IEEE Access*, vol. 8, pp. 114 580–114 596, 2020.

[12] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Low-latency federated learning and blockchain for edge association in digital twin empowered 6G networks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 5098–5107, Jul. 2021.

[13] Q. Yu, J. Ren, Y. Fu, Y. Li, and W. Zhang, "Cybertwin: An origin of next generation network architecture," *IEEE Wireless Commun.*, vol. 26, no. 6, pp. 111–117, Dec. 2019.

[14] Q. Yu, J. Ren, H. Zhou, and W. Zhang, "A cybertwin based network architecture for 6G," in *Proc. 2nd 6G Wireless Summit*, 2020, pp. 1–5.

[15] Y. Guan, R. Lu, Y. Zheng, S. Zhang, J. Shao, and G. Wei, "Toward privacy-preserving Cybertwin-based spatiotemporal keyword query for ITS in 6G era," *IEEE Internet Things J.*, vol. 8, no. 22, pp. 16 243–16 255, Nov. 2021.

[16] W. Shi, H. Zhou, J. Li, W. Xu, N. Zhang, and X. Shen, "Drone assisted vehicular networks: Architecture, challenges and opportunities," *IEEE Netw.*, vol. 32, no. 3, pp. 130–137, May/Jun. 2018.

[17] M. Mizmizi, D. Tagliaferri, D. Badini, C. Mazzucco, and U. Spagnolini, "Channel estimation for 6G V2X hybridsystems using multi-vehicular learning," 2021, *arXiv:2105.09689*.

[18] W. Xu *et al.*, "Internet of Vehicles in Big Data era," *IEEE/CAA J. Automatica Sinica*, vol. 5, no. 1, pp. 19–35, Jan. 2018.

[19] K. Fan *et al.*, "A secure and verifiable data sharing scheme based on blockchain in vehicular social networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5826–5835, Jun. 2020.

[20] T. H. Luan, R. Liu, L. Gao, R. Li, and H. Zhou, "The paradigm of digital twin communications," 2021, *arXiv:2105.07182*.

[21] Z. Su, Y. Hui, Q. Xu, T. Yang, J. Liu, and Y. Jia, "An edge caching scheme to distribute content in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 5346–5356, Jun. 2018.

[22] Y. Zhang and Z. Jiwen, "An efficient proxy ring signature without bilinear pairing," *Chin. J. Electron.*, vol. 28, no. 3, pp. 514–520, 2019.

[23] H. Zhou, N. Cheng, J. Wang, J. Chen, Q. Yu, and X. Shen, "Toward dynamic link utilization for efficient vehicular edge content distribution," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 8301–8313, Sep. 2019.

[24] R. Okuda, Y. Kajiwara, and K. Terashima, "A survey of technical trend of ADAS and autonomous driving," in *Proc. Tech. Papers Int. Symp. VLSI Des., Automat. Test*, 2014, pp. 1–4.

[25] Z. Wang *et al.*, "A digital twin paradigm: Vehicle-to-cloud based advanced driver assistance systems," in *Proc. IEEE 91st Veh. Technol. Conf.*, 2020, pp. 1–6.

[26] X. Chen *et al.*, "Dynamic safety measurement-control technology for intelligent connected vehicles based on digital twin system," *Vibroengineering PROCEDIA*, vol. 37, pp. 78–85, 2021.

[27] H. Zhou, W. Xu, J. Chen, and W. Wang, "Evolutionary V2X technologies toward the Internet of Vehicles: Challenges and opportunities," in *Proc. IEEE*, vol. 108, no. 2, pp. 308–323, Feb. 2020.

[28] M. González, O. Salgado, J. Croes, B. Pluymers, and W. Desmet, "A digital twin for operational evaluation of vertical transportation systems," *IEEE Access*, vol. 8, pp. 114 389–114 400, 2020.

[29] G. Bhatti, H. Mohan, and R. R. Singh, "Towards the future of smart electric vehicles: Digital twin technology," *Renewable Sustain. Energy Rev.*, vol. 141, 2021, Art. no. 110801.

[30] C. M. Ezhilarasu, Z. Skaf, and I. K. Jennions, "The application of reasoning to aerospace Integrated Vehicle Health Management (IVHM): Challenges and opportunities," *Prog. Aerosp. Sci.*, vol. 105, pp. 60–73, 2019.

[31] V. Atamuradov, K. Medjaher, P. Dersin, B. Lamoureux, and N. Zerhouni, "Prognostics and health management for maintenance practitioners-review, implementation and tools evaluation," *Int. J. Prognostics Health Manage.*, vol. 8, no. 60, pp. 1–31, 2017.

[32] C. M. Ezhilarasu, Z. Skaf, and I. K. Jennions, "Understanding the role of a digital twin in integrated vehicle health management (IVHM)," in *Proc. IEEE Int. Conf. Syst., Man Cybern.*, 2019, pp. 1484–1491.

[33] Y. Ye, Q. Yang, F. Yang, Y. Huo, and S. Meng, "Digital twin for the structural health management of reusable spacecraft: A case study," *Eng. Fracture Mechanics*, vol. 234, 2020, Art. no. 107076.

[34] S. Venkatesan, K. Manickavasagam, N. Tengenkai, and N. Vijayalakshmi, "Health monitoring and prognosis of electric vehicle motor using intelligent-digital twin," *IET Electric Power Appl.*, vol. 13, no. 9, pp. 1328–1335, 2019.

[35] S. Khan, M. Farnsworth, R. McWilliam, and J. Erkoyuncu, "On the requirements of digital twin-driven autonomous maintenance," *Annu. Rev. Control*, vol. 50, pp. 13–28, 2020.

[36] J. Liu, S. Zhang, W. Sun, and Y. Shi, "In-vehicle network attacks and countermeasures: Challenges and future directions," *IEEE Netw.*, vol. 31, no. 5, pp. 50–58, Sept./Oct. 2017.

[37] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 993–1006, Apr. 2015.

[38] R. Lu, L. Zhang, J. Ni, and Y. Fang, "5G vehicle-to-everything services: Gearing up for security and privacy," *Proc. IEEE*, vol. 108, no. 2, pp. 373–389, Feb. 2020.
[39] C. Lai, R. Lu, D. Zheng, and X. Shen, "Security and privacy challenges in 5G-enabled vehicular networks," *IEEE Netw.*, vol. 34, no. 2, pp. 37–45, Mar./Apr. 2020.
[40] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles," *Ad Hoc Netw.*, vol. 90, 2019, Art. no. 101823.
[41] Y. Yang, Z. Wei, Y. Zhang, H. Lu, K.-K. R. Choo, and H. Cai, "V2X security: A case study of anonymous authentication," *Pervasive Mobile Comput.*, vol. 41, pp. 259–269, 2017.
[42] R. Soua, I. Turcanu, F. Adamsky, D. Führer, and T. Engel, "Multi-access edge computing for vehicular networks: A position paper," in *Proc. IEEE Globecom Workshops*, 2018, pp. 1–6.
[43] G. Potrino, F. De Rango, and P. Fazio, "A distributed mitigation strategy against DoS attacks in edge computing," in *Proc. Wireless Telecommun. Symp.*, 2019, pp. 1–7.
[44] D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, "A survey on secure data analytics in edge computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4946–4967, Jun. 2019.
[45] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.
[46] X. S. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2013.
[47] *3rd Generation Partnership Project*, "Technical specification group service and system aspects," *3GPP Standard TS 33.501*, Secur. Architecture Procedures 5G Syst. (Rel. 15) V15.3.1, Dec. 2018.
[48] C. Cremers and M. Dehnel-Wild, "Component-based formal analysis of 5G-AKA: Channel assumptions and session confusion," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2019, pp. 1–5.
[49] S. R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, and E. Bertino, "5greasoner: A property-directed security and privacy analysis framework for 5G cellular network protocol," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2019, pp. 669–684.
[50] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5G authentication," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2018, pp. 1383–1396.
[51] S. Ravidas, A. Lekidis, F. Paci, and N. Zannone, "Access control in Internet-of-Things: A survey," *J. Netw. Comput. Appl.*, vol. 144, pp. 79–101, 2019.
[52] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Comput. Surv.*, vol. 51, no. 4, pp. 1–35, 2018.
[53] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: A survey," *IEEE Commun. Surv. Tut.*, vol. 22, no. 1, pp. 746–789, Jan.–Mar. 2020.
[54] R. R. Al-Dahhan, Q. Shi, G. M. Lee, and K. Kifayat, "Survey on revocation in ciphertext-policy attribute-based encryption," *Sensors*, vol. 19, no. 7, pp. 1695–1717, 2019.
[55] 3rd Generation Partnership Project, "Technical specification group service and system aspects," 3GPP Standard TS 33.401, *3GPP Syst. Architecture Evol. (SAE) Secur. Architecture* (Rel 16), V16.1.0, Dec. 2019.
[56] R. Ma, J. Cao, D. Feng, H. Li, and S. He, "FTGPHA: Fixed-trajectory group pre-handover authentication mechanism for mobile relays in 5G high-speed rail networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 2126–2140, Feb. 2020.
[57] D. W. Q. X. K. C. Debiao HE, "Anonymous handover authentication protocol for mobile wireless networks with conditional privacy preservation," *Sci. China*, vol. 60, no. 5, pp. 113–129, 2017.
[58] Z. Haddad, A. Alsharif, A. Sherif, and M. Mahmoud, "Privacy-preserving Intra-MME group handover via MRN in LTE-A networks for repeated trips," in *Proc. IEEE 86th Veh. Technol. Conf.*, 2017, pp. 1–5.

Guanjie Li received the B.S. degree in communication engineering and the M.S. degree in electronics and communication engineering from the Xi'an University of Posts and Telecommunications, Xi'an, China, in 2016 and 2021, respectively. He is currently working toward the Ph.D. degree in cyberspace security with the School of Cyber Engineering, Xidian University, Xi'an, China. His research interests include vehicular network and digital twin.

Chengzhe Lai (Member, IEEE) received the B.S. degree in information security from the Xi'an University of Posts and Telecommunications, Xi'an, China, in 2008, and the Ph.D. degree from Xidian University, Xi'an, China, in 2014. From 2012 to 2014, he was a Visiting Ph.D. Student with the Broadband Communications Research (BBCR) Group, University of Waterloo, Waterloo, ON, Canada. He is currently with the Xi'an University of Posts and Telecommunications and National Engineering Laboratory for Wireless Security, Xi'an, China. His research interests include wireless network security and privacy preservation.

Rongxing Lu (Fellow, IEEE) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, in 2012. From 2013 to 2016, he was an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. Since 2016, he has been an Associate Professor with the Faculty of Computer Science (FCS), University of New Brunswick (UNB), Fredericton, NB, Canada. From 2012 to 2013, he was a Postdoctoral Fellow with the University of Waterloo. He was the recipient of Governor Generals Gold Medal for his Ph.D. degree, 8th IEEE Communications Society (ComSoc) AsiaPacific Outstanding Young Researcher Award in 2013, and the 2016 to 2017 Excellence in Teaching Award from FCS, UNB. He is currently the Vice Chair (Publication) of the IEEE ComSoc CIS-TC.

Dong Zheng received the M.S. degree in mathematics from Shaanxi Normal University, Xi'an, China, in 1988, and the Ph.D. degree in communication engineering from Xidian University, Xi'an, China, in 1999. He was a Professor with the School of Information Security Engineering, Shanghai Jiao Tong University, Shanghai, China. He is currently a Professor with the Xi'an University of Posts and Telecommunications and is also connected with the National Engineering Laboratory for Wireless Security, Xi'an, China. His research interests include provable security and new cryptographic technology.