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

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

2023.04.24

Professor: 박종혁

Presented by:

요사이 생텅 (YOTXAY SANGTHONG)

Seoul National University of Science and Technology, Seoul, South Korea.

Table Contents

Abstract

- In this paper, they introduce the architecture and promising applications of Cybertwin-driven 6G V2X.
- Analyze essential data security and privacy preservation requirements for Cybertwin-driven 6G V2X.
- They present the security reference architecture of Cybertwin-driven 6G V2X.
- As a case study, they 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, they discuss several open research directions for achieving more secure Cybertwin driven6G V2X.

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).
- 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.
- 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. 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.
- In addition, as an emerging intelligent computing technology, digital twin can realize the connection, interaction and integration between the physical world and cyberspace.
- 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.
- 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 .
- 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.

I. Introduction

- With the emerging research on digital twin, Cybertwin has been received widespread attentions from academia.
- 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.
- Vehicle-to-Everything (V2X) aims to share road information and to transmit collecting data between vehicles, infrastructures, pedestrians and cloud. 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 .
- The goal of 6G-V2X is to be a heterogeneous, dynamic, intelligent, autonomous, user driven connectivity and service platform for Intelligent Transportation System (ITS).
- As Intra-twin and Inter-twin communication in, 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. Cybertwin-to-Cybertwin communication, communicate other twin nodes to transfer data, share and improve information perception in cyberspace.

I. Introduction

- 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, they 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:**

➢ They 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.

➢ They summarize the security and privacy requirements and analyze the data security or privacy threats for Cybertwindriven 6G V2X network. Particularly, they 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, they design a handover authentication scheme based on proxy ring signature technique to achieve mutual authentication, key negotiation and Cybertwin migration between the moving vehicle and edge server.

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

A. Architecture for Cybertwin-Driven 6G V2X Network

- According to the definition and characteristics of Cybertwin, they 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:** This layer consists of vehicles, roadside infrastructures, pedestrians with wearable devices and other physical devices.

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

- **Access Layer:** This 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.

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

A. Architecture for Cybertwin-Driven 6G V2X Network

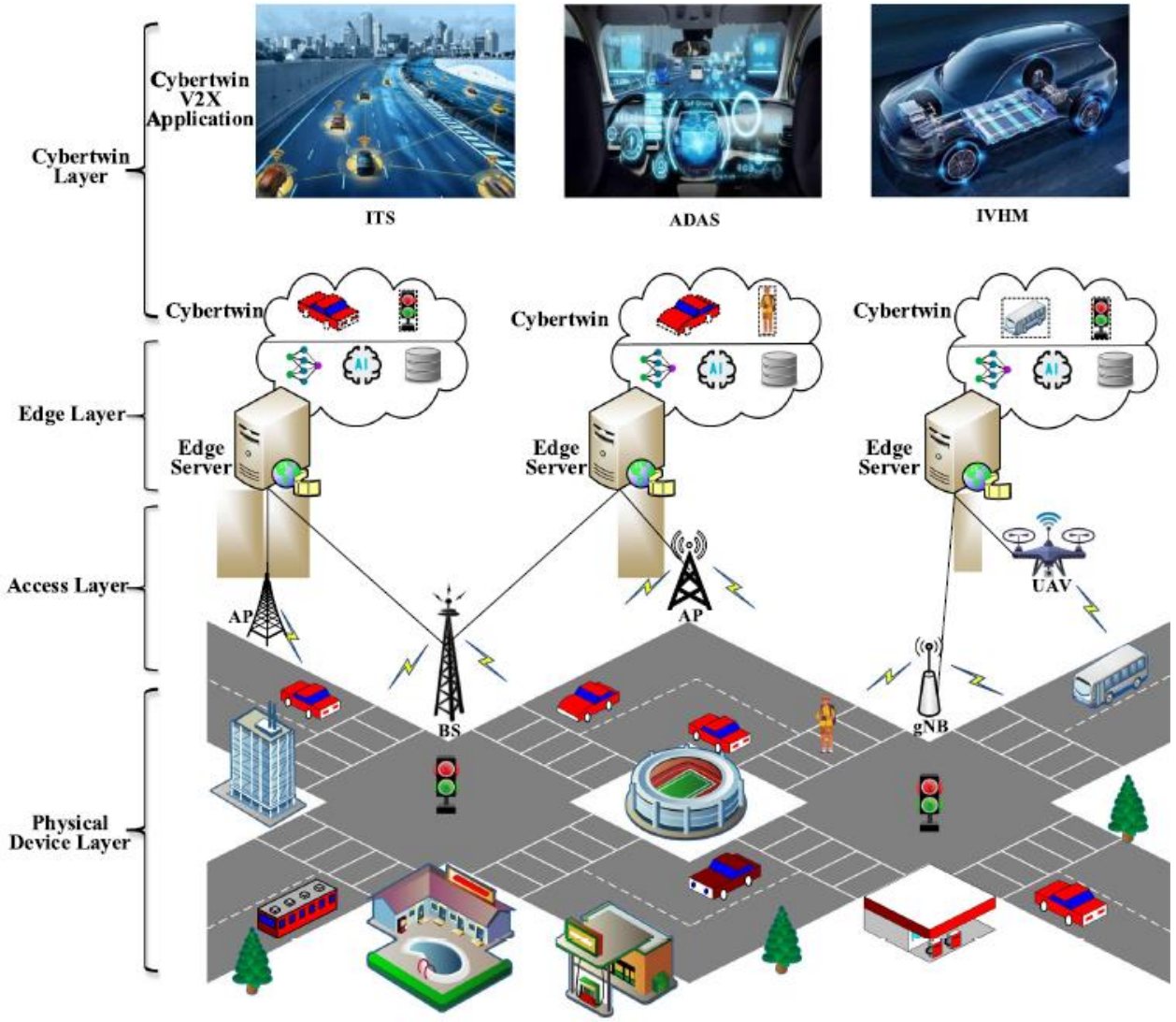

Fig. 1. Architecture of Cybertwin driven-6G V2X network.

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

A. Architecture for Cybertwin-Driven 6G V2X Network

- **Edge Layer:** In this 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.
- Cybertwin can communicate with other twins in the same or different edge servers, which can refer to as Cybertwin-to-Cybertwin communication.
- This communication mode improves the data acquisition ability and gets rid of the limitation of space for Cybertwin.

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

B. Applications of Cybertwin-Driven 6G V2X

- They summarize the state-of-art works relevant to V2X applications supported by digital twin.
- **1) Advanced Driver Assistant System:** Safe driving is the first priority and eternal goal for develop of V2X. ADAS is seen as a transitional stage for the realization of autonomous vehicles. 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.
- ADAS can prevent and avoid traffic accidents caused by human error to the greatest extent. But, ADAS still has several limitations. One of the issues is lack of road information interaction among vehicles on road, ADAS system cannot accurately prejudge the behavior of other vehicles.
- ADAS can effectively improve the above issues. **Wang et al. [25]** proposed ADAS based on the digital twin vehicle to provide driver with optimal driving speed when the vehicle enters the road ramp. The vehicle sends the driving information including speed, position and obstacles ahead to the digital twin which resides on the central server.
- **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 effect of decision to improve safe driving.
- **2) Intelligent Transportation System:** Several advanced technologies, such as communication, sense and artificial intelligent, have been applied to traffic management. 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 .
- The ITS is to improve traffic safety, optimize traffic flow, increase traffic throughput and facilitate traffic management. Cybertwin and digital twin can solve these challenges and make ITS even more powerful.
- 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.

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

B. Applications of Cybertwin-Driven 6G V2X

- **3) 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 and 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. 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.
- IVHM based on digital twin can bring more accurate and better performance for health monitoring and vehicle diagnosis.
- **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.
- **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.
- 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.

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

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

- They presented six security and privacy requirements of Cybertwin-driven 6G V2X network.
- **Confidentiality:** Since the physical device and its Cybertwin communicate over an open wireless channel, confidentiality requires the transmitted data can not be accessed by unauthorized third parties. 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.
- **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.
- **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.
- **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.
- **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.
- **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.

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

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 Cybertwindriven 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.

- **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. 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.
- 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.

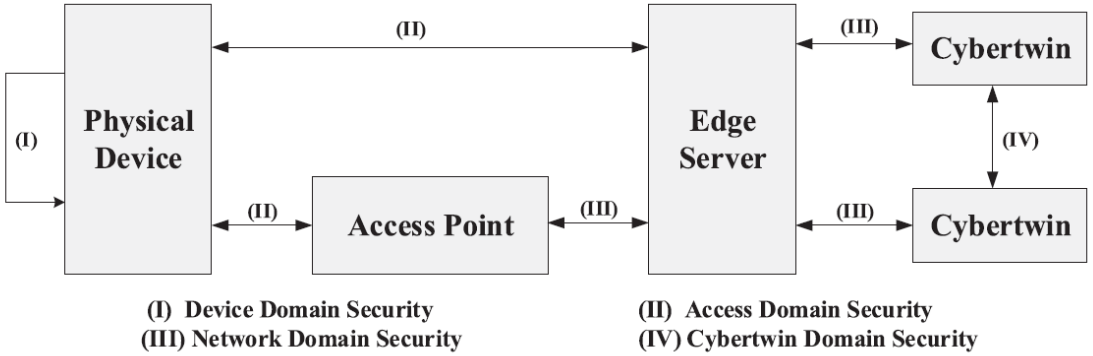

Fig. 2. Security reference architecture of Cybertwin-driven 6G V2X.

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

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

- **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.
- Its 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.
- 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.

- **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.

- **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 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.

- 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.

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

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

- The security solutions 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 wireless channel to improve the legal channel better than the eavesdropping channel, to reduce the information leakage.
- 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.
- **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 . On the one hand, 5G-AKA protocol provides the primary mutual authentication between physical device and access point against impersonation attack.
- **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.
- 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. 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. 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).

IV. A Case Study: Migration of CyberTwin

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.
- **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 theCybertwin V2X applications, which has been verified by the RTA to be legitimate and trusted.
- **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.
- **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.

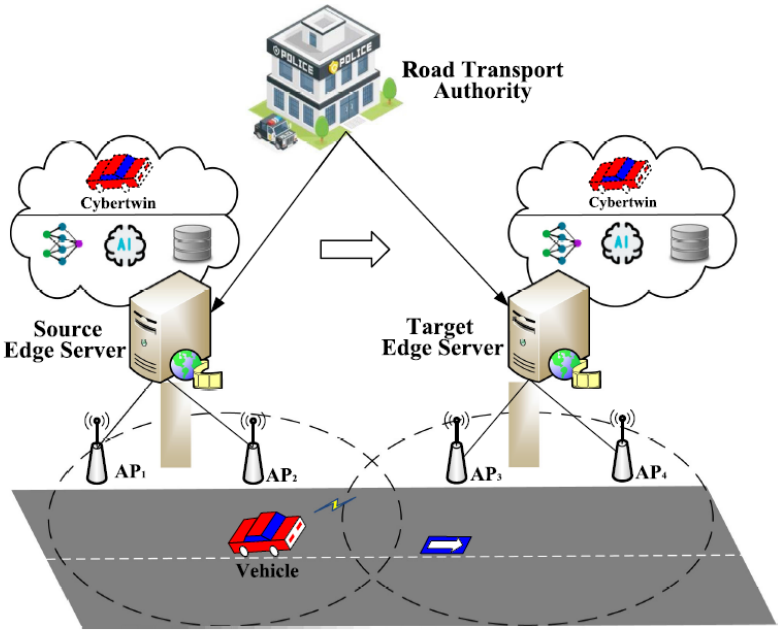

Fig. 3. System model.

IV. A Case Study: Migration of CyberTwin

B. Overview

- They 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.
- 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.

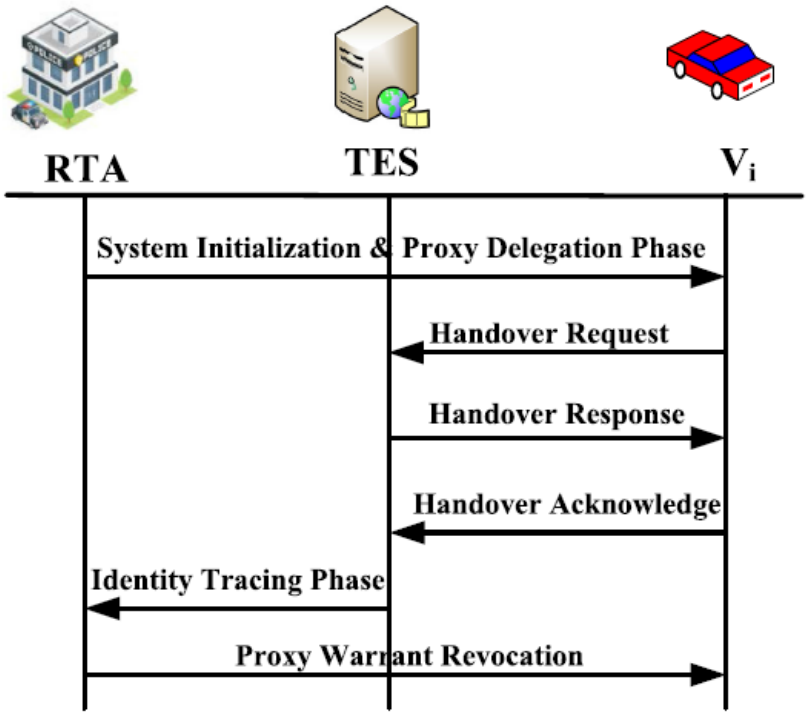

Fig. 4. Process in handover authentication.

IV. A Case Study: Migration of CyberTwin

C. The Proposed Scheme

- First, they 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, $G1$ be a cyclic addition group and $G2$ be a multiplicative cyclic group of order q ($q > 2\kappa$) with generator
  P, $e : G1 \times G1 \rightarrow G2$ be a bilinear pairing. The RTA executes system initialization.
- The RTA randomly selects $skrta \in Z*q$ as the system master key and computes $pkrta = skrta * P$ as the system public key.

- The vehicle V selects $skv \in Z*q$ as private key and computes the public key $pkv = skv * P$ for achieving secure communication. The edge server ES performs the same operations as the vehicle and finally generates the public and private key pairs (*skes, pkes*).

- Furthermore, the V sends identity information (*IDv, pkv*) to the RTA. On receiving *IDv* from the V, the RTA stores (*IDv, pkv*) in the local database.

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

IV. A Case Study: Migration of CyberTwin

C. The Proposed Scheme

- **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 asmore data is input.
- After verifying Cybertwin V2X applications on the ES, the RTA firstly generates an authorization proxy warrant wes = (IDRTA, IDES,APPESi ,ETStart,ETEnd), where IDRTA is the identity of the RTA, IDES is the identity of the ES, APPESi is the authorized Cybertwin V2X applications, ETStart and ETEnd are the authorization start time and end time for the ES respectively.
- Then, the RTA randomly selects res $\in$ Z$*$ q to compute the proxy delegation for ES. The proxy signature pair (yes, Res) of ES is computed as follows:

$$R_{es} = r_{es} * P$$

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

$$y_{es} = (r_{es} + h_{es} * sk_{rta}) \ mod \ q$$

- Finally, the proxy delegation σes = (wes, yes,Res) is sent to the ES from the RTA via secure channel. On receiving the σes, the ES first checks the contents of wes and determines whether the σes is correct by verifying the following equations.

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

$$y_{es} * P = (r_{es} + h_{es} * sk_{rta}) * P$$

$$= R_{es} + h_{es} * pk_{rta}$$

- If the verification fails, the ES will request the valid proxy delegation from the RTA again. Otherwise, the ES receives proxy delegation σes which will be used to show the authority and legitimacy of the ES to the vehicleVi in handover authentication phase.

IV. A Case Study: Migration of CyberTwin

C. The Proposed Scheme

- **Between RTA and Vi:** 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 usersV = (V1,V2, . . .,Vn) who are applying for authorization from the RTA, each vehicle user sends (IDi,APPi) to the RTA via secure channel. On receiving (IDi,APPi), 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 wv = (IDRTA, L,APPVi ,VTStart,VTEnd) for these vehicle users who apply for the same application in the period, where L is the public key information string of these vehicles, APPVi is the Cybertwin V2X application that vehicle can create, VTStart andVTEnd are the authorization start time and end time for each vehicle user Vi. Then, the RTA selects random number rvi $\in$ Z$*$ q and computes the proxy delegation σvi for Vi. The proxy signature pair (yvi,Rvi) is generated as follows:

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

- Similarly, the RTA transmits the proxy delegation σvi = (wv, yvi,Rvi) to the applying vehicle users V = (V1,V2, . . .,Vn) via secure channel. After receiving the proxy delegation σvi = (wv, yvi,Rvi) from the RTA, each vehicle user reviews whether information in authorization warrant wv is correct and validates the received proxy delegation as follows:

$$y_{v_i} * P = (r_{v_i} + sk_{rta} * h_{v_i}) * P$$
$$= R_{v_i} + h_{v_i} * pk_{rta}$$

- If the verification is correct, the vehicle accepts σvi as proxy delegation.

IV. A Case Study: Migration of CyberTwin

C. The Proposed Scheme

- **3) Handover Authentication Phase:** Assuming that Vi has already accessed to a source edge server SES and created its Cybertwin. When the Vi is about to move from the coverage of SES to the coverage of target edge server TES, the Vi triggers handover authentication procedure with the TES in order to migrate new Cybertwin and to guarantee the QoE of Cybertwin V2X application.
- Step1: Vi → TES : HANDOVER REQUEST ReqVi
- The Vi first selects a random number ki ∈ Z∗ q to compute Kvi = ki ∗ P.
- Then, the Vi generates timestamp TS1 and randomly chooses λ ∈ Z∗ q , εj ∈ Z∗ q (j = 1, 2, . . ., i − 1, i + 1, . . ., n) to compute h2 and εi as follows where pkj 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 Vi computes proxy ring authentication signature pair (sv1, sv2) 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 wv and replay attack, the Vi generates a sequence number seq and selects αi ∈ Z∗ q to compute Ai, Ui and ciphertext Ci 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 Vi chooses tj ∈ Z∗ q (j = 1, 2, . . ., n) and computes tracking factors as follows:

$$TK_j = t_j * pk_j$$

$$T_j = t_j * P$$

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

IV. A Case Study: Migration of CyberTwin

C. The Proposed Scheme

- When the Vi enters the coverage area of the TES, the Vu sends the Handover Request message including ReqVi = (Ci,Ai,Rvi,Kvi, sv1, sv2, T,W, TS1) to the TES where W = (εj, TKj, j = 1, 2. . ., n).
- Step2:TES→Vi:HANDOVERRESPONSE Reptes,MAC1
- On receiving message from the Vi, the TES first verifies freshness of TS1. Then the TES uses private key sktes to compute Ui and to decrypt wv from Ci 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 wv and verifies legitimacy of the Vi 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 (wv, T, TKj) to the RTA in order to trace the true identity of Vi. Otherwise, the TES believes that the Vi has been legally authorized by the RTA and allows the Vi to access edge server and to create corresponding Cybertwin.
- The TES selects ktes ∈ 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 Vi.

$$K_{tes} = k_{tes} * P \quad (1)$$

$$AK = k_{tes} * K_{v_i} \quad (2)$$

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

IV. A Case Study: Migration of CyberTwin

C. The Proposed Scheme

- Then, the TES selects a random number ztes ∈ Z∗ q and generates TimestampTS2 to compute authentication signature stes and message authentication code MAC1 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 Reptes = (wtes, stes,Rtes, Ztes,Ktes, TS2) and MAC1. The TES sends Handover Response message to the Vi.
- Step3: Vi→TES: ACKNOWLEDGE MAC2, TS3 On receiving Reptes from the TES, the Vi checks the freshness of TS2 and recalculates htes, ntes. Then, the Vi 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 Vi quits authentication with TES and remains connected to the source edge server SES. Otherwise, the Vi can compute AK and PTK as follows:

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

- Then, the Vi recalculates MAC 1 and verifies Equation (4). If the verification is correct, the Vi can consider that the TES is authorized and can access the TES to create its Cybertwin.

$$MAC_1' = MAC_1 \qquad (4)$$

- Finally, the Vi generates Timestamp TS3 and sends Acknowledge message which includesMAC2 to the TES as handover authentication confirmation.

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

IV. A Case Study: Migration of CyberTwin

C. The Proposed Scheme

- **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 wv 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 (wv, T, TKj) to the RTA via secure channel. Only the RTA has the right to ask each vehicle member Vj on the wv for tracing factor as follows:

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

- After receiving Tj from each vehicle Vj, the RTA verifies e(TKj, P) = e(Tj, pkj). If the validation fails, the RTA considers Tj to be invalid and suspects that the corresponding vehicle is dishonest. Otherwise, the RTA can obtain the public key pkvi and find (IDvi, pkvi) from local storage according to the Equations (5)-(6).
- Finally, the RTA further outputs the vehicle's true identity information IDvi. If the Vi does have malicious behavior, the RTA will eventually revoke the proxy warrant wv granted to the vehicle Vi.

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

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

- 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 Vi and TES according to the proxy warrant w issued by the TES during handover phase. The Vi sends the encrypted wv and proxy signature to the TES. After receiving the message, the TES can decrypt and obtain the wv by using the private key sktes.
- 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 Vi can determine the legitimacy of TES by verifying whether Equation (9) is correct.

IV. A Case Study: Migration of CyberTwin

D. Security Analysis

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

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

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

- **Key Agreement:** In the proposed scheme, the pairwise transient key PTK can be negotiated between the Vi and the TES based onAK,wv, wtes, 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 ktes ∗ P and ki ∗ P from public channel, it is difficult to calculate secret key AK = ktes ∗ ki ∗ P without ktes and ki. On the other hand, only the legal TES can obtain wv and seq by utilizing the private key sktes.

- **Withstanding Attacks**: First, the proposed scheme can resist replay attack by using the sequence number which has been encrypted by pktes. Second, the scheme can realize the integrity protection by using the message authentication code. Without knowing seq andAK, the malicious attacker cannot generate the tampered message intoMAC that can be verified by the vehicle.

- In addition, by using the timestamp, the proposed scheme is resistant to Man-in-Middle attacks. If theVi or the TES receives the timestamp attached to handover message that exceeds the time threshold, authenticationwill be quitted. Even if amalicious attacker tampers with the timestamp, the correct MAC cannot be generated.

- **Anonymity:** The proposed scheme can achieve unconditional anonymity for theVi during handover authentication phase. The TES just can infer that theVi is legal and belongs to set of proxy signers V = (V1,V2, . . .,Vn) by verifying the correctness of wV . The probability that the TES can conclude the true identity of the Vi is not more than 1 /n.

IV. A Case Study: Migration of CyberTwin

D. Security Analysis

- **Traceability:** When malicious or dispute behavior occurs, the RTA can reveal the true identity of the Vi. The RTA has the right to collect Tj from members of each vehicle listed on the wv. The RTA verifies the correctness of Tj as follows:

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

- If the verification is correct, the RTA can find pkvi according to Equation (10). The RTA can output the true identity information of vehicle based on (IDvi, pkvi) stored on the local server.

- **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: $\frac{P|\equiv P\overset{K}{\longleftrightarrow}Q,P\{X\}_K}{P|\equiv Q|\sim X}$

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

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

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

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

IV. A Case Study: Migration of CyberTwin

D. Security Analysis

- They prove that the proposed scheme can achieve mutual authentication and establish session key between TES and Vi according to the BAN logic as follows:

Since TES received ReqVi, we have:
S1: TES $\equiv$ *ReqVi*
According to Assumation2 and the fresh-promotion rule, they have:
S2: TES/$\equiv$ (*ReqVi*)
If Equations (7) and (8) are correct, according to S1, they have:
S3: ESt/$\equiv$ Vi/$\sim$ *ReqVi*
According to S2, S3 and the nonce-verification rule, they have:
S4: TES/$\equiv$ Vi/$\equiv$ *ReqVi*
According to S4 and the decomposition rule, we have:
S5: TES/$\equiv$ Vi/$\equiv$ $ki * P$, TES/$\equiv$ Vi/$\equiv$ (*wv, seq*)
According to S5, Assumption1 and jurisdiction rule, they have:
S6: TES/$\equiv$ $ki * P$, TES/$\equiv$ (*wv, seq*)
In the scheme, TES randomly selects $ktes \in Z*$ *q*, they have:
S7: TES/$\equiv$ *ktes*,
According to S6, S7 and the composition rule, they have:
S8: TES/$\equiv$ $AK = ktes * ki * P$
That is, TES/$\equiv$ TES $\leftarrow A \rightarrow K$ Vi
Since TES has already kept the *wtes*, according to S6, S8 and composition rule, theyhave:
S9: TES/$\equiv$ $PTK = H5(AK, wtes, wv, seq + 1)$
That is, TES/$\equiv$ TES $P \leftarrow T \rightarrow K$ Vi (Goal 2)
Since Vi received (*Reptes,MAC*1), they have
S10: Vi (*Reptes,MAC*1)

IV. A Case Study: Migration of CyberTwin

D. Security Analysis

According to Assumption5 and the fresh-promotion rule, they have:
S11: Vi/≡ (*Reptes*)
If Equation (9) is correct, according to S10, they have:
S12: Vi/≡ TES/~*Reptes*
According to S11, S12 and the nonce-verification rule, they have:
S13: Vi/≡ TES/≡*Reptes*
According to S13 and the decomposition rule, they have:
S14: Vi/≡ TES/≡*ktes* ∗ *P*, Vi/≡ TES/≡ *wtes*
According to S14, Assumption 4 and the jurisdiction rule, they have:
S15: Vi/≡*ktes* ∗ *P*, Vi/≡*wtes*
Since Vi randomly selects *ki*, they have:
S16: Vi/≡*ki*
According to S15, S16 and the composition rule, we have:
S17: Vi/≡ *AK* = *ki* ∗ *ktes* ∗ *P*
That is, Vi/≡ Vi
←*A*→*K* TES
Since Vi has already kept the *wv* and *seq*, according to S15, S17 and composition rule, they have:
S18: Vi/≡ *PTK* = *H*5(*AK,wtes, wv, seq* + 1)
That is, Vi/≡ Vi
P←*T*→*K* TES (Goal 1)
Since TES received *MAC*2 they have:
S19: TES *MAC*2,
According to to S8, S19 and the message-meaning rule, they have:
S20: TES/≡ Vi/ ~ (*PTK,TS*3, *seq* + 2)
According to Assumption3 and the fresh-promotion rule, they have:
S21: TES/≡ (*PTK,TS*3, *seq* + 2)
According to S20, S21 and the nonce-verification rule, they have:
S22: TES/≡ Vi/≡ (*PTK,TS*3, *seq* + 2)
According to S22 and the decomposition rule, they have: S23: TES|≡ Vi|≡ PTK
That is, TES|≡ Vi|≡ Vi P←T→K TES (Goal 4)
Since Vi received MAC1, they have:
S24: Vi MAC1
According to S17, S24 and message meaning rule, they have:
S25: Vi|≡ TES| ~ (PTK,TS2, seq + 1)
According to Assumption5 and fresh promotion rule,wehave:
S26: Vi|≡ (PTK,TS2, seq + 1) According to S25, S26 and the nonce-verification rule, they have:
S27: Vi|≡ TES|≡ (PTK,TS2, seq + 1)
According to S27 and the decomposition rule, they have: S28: Vi|≡ TES|≡ PTK That is, Vi|≡ TES|≡ TES P←T→K Vi (Goal 3)

IV. A Case Study: Migration of CyberTwin

D. Security Analysis

- **E. Performance Evaluation**
- In this subsection, They 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, They compare our proposed scheme with the standard mechanisms: 5G-AKA [47], EAPAKA' [47] and EPS-AKA [55]. The transmission costs consumed in 5G-AKA and EAP-AKA' is 3 + 4b + 2c and in EPSAKA 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,** they can obtain that transmission costs of our proposed scheme is better than other protocols.

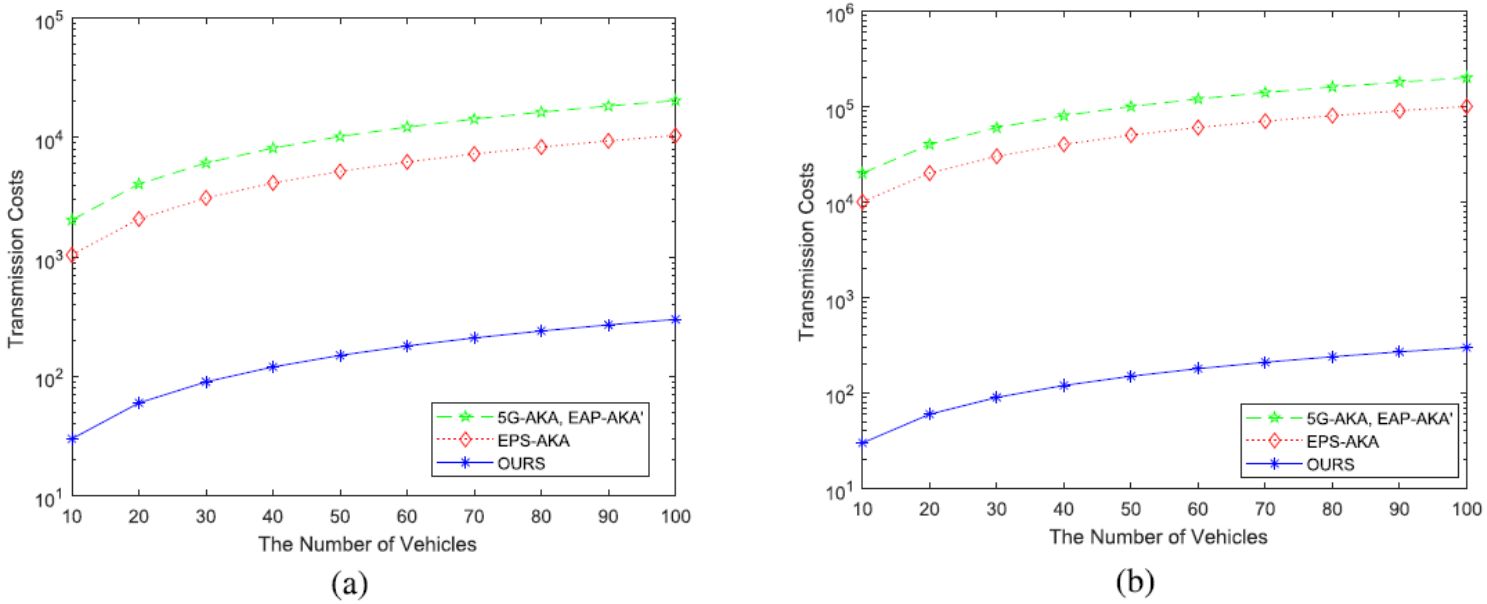

Fig. 5. Comparison of the transmission costs. (a) b = 50 and c = 0.4. (b) b = 500 and c = 0.4.

IV. A Case Study: Migration of CyberTwin

D. Security Analysis

- **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 mis number of public keys listed in proxy warrant.
- As shown in **Fig. 6,** with the number of mincreases, 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**.

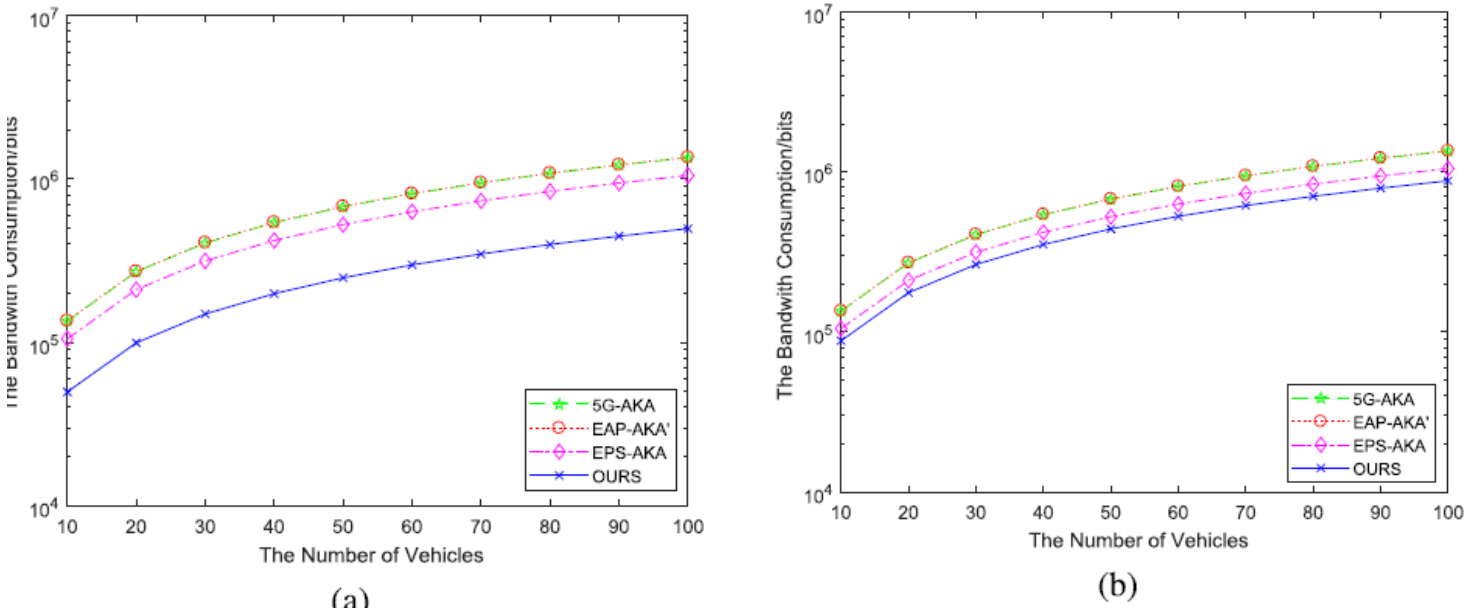

Fig. 6. Comparison of bandwidth consumption. (a) m = 15 and t = 15. (b) m = 30 and t = 15.

IV. A Case Study: Migration of CyberTwin

D. Security Analysis

- **3) Computation Costs:** They only consider the computation costs for the cryptographic primitive operation during the authentication process, in terms of hash function Th, the point addition operation Ta, the modular exponentiation operation Te, the bilinear pairing operation Tp and point multiplication operation Tm.

- The above operations have been investigated in [56] by using OpenSSL with Intel m3-6Y30 CPU@0.9 GHz as Vi and Intel i7-7500 U CPU @2.70 GHz as TES. The details of the computation cost are listed in **Table II.**

TABLE II
COMPUTATION COSTS OF THE PRIMITIVE CRYPTOGRAPHY OPERATIONS

Time (ms) / User	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

IV. A Case Study: Migration of CyberTwin

C. The Proposed Scheme

- They compare the computation costs used for the vehicle Vi side and target edge server the TES side during handover authentication phase. The computation costs for edge server is (4Th + (7 + m)Tm)nms and for vehicle is (3Th + 4Tm)nms.
- Let's assume that the public key information for 15 vehicles is listed in the proxy warrant, namelym = 15, and the vehicle has already calculated the request message ReqVi before entering the coverage area of TES, it can be seen from the **Fig. 7(a)** that the computation costs of theVi side is much lower than that of the TES side.
- In addition, they also compare the computation costs on vehicle side in the related protocols. The computation costs of vehicle side in [57] is (4Tm + Ta + 2Te + 5Th)nms,
- in [58] is (3n + 1)Tp + 2nTe + 4nTh + nTm ms, in 5G-AKA is 7nTh ms and in EPS-AKA is 6nTh 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.

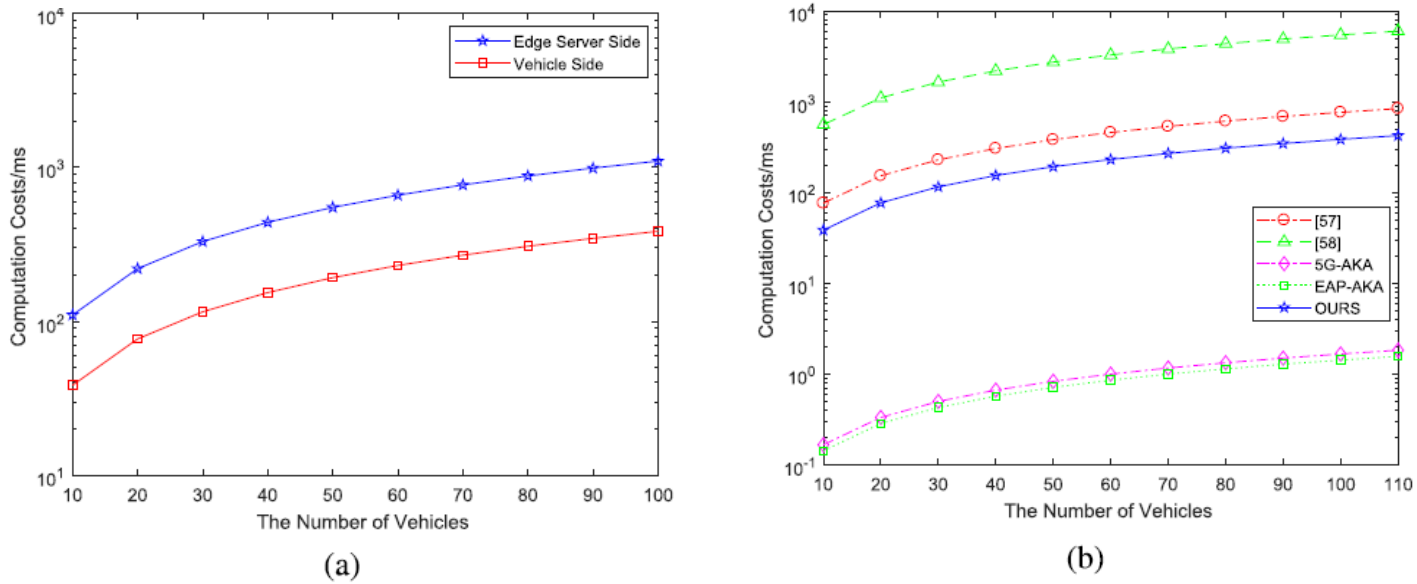

Fig. 7. Comparison of computation costs. (a) Between vehicle side and edge side of our proposed scheme (b) Between our proposed scheme and other protocols on vehicle side.

V. Future Research Direction

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 themobility of the vehicles, Cybertwin also needs to be connected to and migrated to the newedge server along with the vehicles.
- In order to keep theCybertwin operation accurately, the historical data should also be seamlessly and flexibly migrated to the new edge server.

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.

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 rawdata 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.

VI. Conclusion

- In this paper, They presented the four-layer architecture and several promising applications of Cybertwin-driven 6G V2X network.

- Then, they analyzed the requirements of security and privacy preservation in Cybertwin-driven 6G V2X network.
- Particularly, proposed the security reference architecture of Cybertwin-driven 6G V2X network and analyzed the potential security solutions to solve exiting security and privacy issues.

- They 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.
- a security reference architecture is a useful tool for ensuring the security of complex systems such as cybertwin-driven 6G V2X. By providing a structured approach to security, it can help to identify potential vulnerabilities and mitigate risks before they can be exploited.

My opinion for this paper

- This paper proposed architecture include security measures such **as secure communication protocols, access control mechanisms, data protection, and threat detection and response.**

- It also address specific security challenges associated with cybertwin-driven 6G V2X.

- The paper provide a structured approach to designing, implementing, and maintaining security controls and policies for cybertwin-driven 6G V2X, with the aim of mitigating potential security risks and ensuring the safety and reliability of this emerging technology.

Thank You

For your Attention!

연락처: yotxaysangthong@seoultech.ac.kr
+82 10-8999-3151