Blockchain-Based Pseudonym Management for Vehicle Twin Migrations in Vehicular Edge Metaverse

Jiawen Kang, *Senior Member, IEEE*, Xiaofeng Luo, Jiangtian Nie, *Member, IEEE*, Tianhao Wu, Haibo Zhou, *Senior Member, IEEE*, Yonghua Wang, *Senior Member, IEEE*, Dusit Niyato, *Fellow, IEEE*, Shiwen Mao, *Fellow, IEEE*, and Shengli Xie, *Fellow, IEEE*

***Abstract*—Driven by the great advances in metaverse and edge computing technologies, vehicular edge metaverses are expected to disrupt the current paradigm of intelligent transportation systems. As highly computerized avatars of vehicular metaverse users (VMUs), the vehicle twins (VTs) deployed in edge servers can provide valuable metaverse services to improve driving safety and on-board satisfaction for their VMUs throughout journeys. To maintain uninterrupted metaverse experiences, VTs must be migrated among edge servers following the movements of vehicles. This can raise concerns about privacy breaches during the dynamic communications among vehicular edge metaverses. To address these concerns and safeguard location privacy, pseudonyms as temporary identifiers can be leveraged by both VMUs and VTs to realize anonymous communications in the physical space and virtual spaces. However, existing pseudonym management methods fall short in meeting the extensive pseudonym demands in vehicular edge metaverses, thus dramatically diminishing the performance of privacy preservation. To this end, we present a cross-metaverse empowered dual pseudonym management framework. We utilize cross-chain technology to enhance management efficiency and data security for pseudonyms. Furthermore, we propose a metric to assess the privacy level and employ a multiagent deep reinforcement learning (MADRL) approach to obtain an optimal pseudonym generating strategy. Numerical results demonstrate that our proposed schemes are high-efficiency and cost-effective, showcasing their promising applications in vehicular edge metaverses.**

***Index Terms*—Cross-chain, deep reinforcement learning, pseudonym management, twin migration, vehicular metaverse.**

Manuscript received 22 March 2024; accepted 13 May 2024. Date of publication 23 May 2024; date of current version 24 October 2024. This work was supported in part by NSFC under Grant 62102099, Grant U22A205, and Grant 6197114; in part by the Pearl River Talent Recruitment Program under Grant 2021QN02S643; in part by the Guangzhou Basic Research Program under Grant 2023A04J1699; in part by the Guangdong Basic and Applied Basic Research Foundation under Grant 2023A1515011888; in part by the National Research Foundation, Singapore; in part by the Infocomm Media Development Authority under its Future Communications Research and Development Programme; in part by the Defence Science Organisation (DSO) National Laboratories under the AI Singapore Programme under Award AISG2-RP-2020-019 and Award FCP-ASTAR-TG-2022-003; and in part by the Singapore Ministry of Education (MOE) Tier 1 under Grant RG87/22. The work of Shiwen Mao work was supported in part by NSF under Grant CNS-2148382. *(Corresponding author: Yonghua Wang.)*

Please see the Acknowledgment section of this article for the author affiliations.

Digital Object Identifier 10.1109/JIOT.2024.3404559

I. Introduction

THE FAST evolution of Internet of Things (IoT) systems has paved the way for the novel paradigm of metaverse, which is considered a creative application of beyond 5G (B5G) networks to meet people's growing demands for hyper spatio-temporal and surreal digital services in the near future [1], [2]. By integrating the technologies of edge computing and intelligent transportation systems, metaverses can further transition into a distinct paradigm called vehicular edge metaverses [3]. Functioning as surreal realms that merge virtual spaces with the physical space at the network edge, vehicular edge metaverses can offer a range of remarkable metaverse services such as augmented reality (AR) navigation, to vehicular metaverse users (VMUs) (i.e., drivers and passengers within vehicles) with lower latency and higher fidelity [4]. These services can significantly increase VMUs' driving safety and on-board satisfaction throughout their journey [5]. Vehicle twins (VTs) as specific Al agents [6], are one of the core components of delivering metaverse services, which cover the entire life cycles of the vehicle and VMUs in vehicular edge metaverses. Embedded with versatile multimodal large language models (LLMs) [7], the VTs can process multimodal sensory inputs from their VMUs (e.g., gestures and speech) and the vehicle (e.g., sensing data collected by LiDAR and cameras) to enhance environmental perception and understanding. The VTs in virtual spaces are capable of continuously updating themselves through interacting with other VTs and their associated VMUs, thereby providing customized services back to the VMUs in the physical space [4].

Owing to the inherent limitations in computing and storage resources of vehicles, the memory and computation-intensive tasks of maintaining VTs and running LLMs should be offloaded to edge servers along the roadside, such as base stations and roadside units (RSUs) [4]. However, given the restricted communication coverage of edge servers, VTs often necessitate migrations among edge servers along the route of their associated VMUs to provide uninterrupted metaverse services [5]. Therefore, a substantial volume of communication takes place within vehicular edge metaverses. On one hand, vehicles with VMUs must broadcast safety messages including their current location information to nearby vehicles and edge servers, thereby enhancing mutual awareness of surrounding

traffic conditions and improving driving safety [8], [9]. On the other hand, VTs deployed in edge servers should connect with their VMUs in the physical space for real-time data synchronization and metaverse service provisioning, and interact with other VTs in virtual spaces for global information acquisition during VT migrations [4], [5]. These communication processes pose a potential risk of privacy leakages [10], as malicious attackers could exploit the background information (e.g., location) behind the messages to infer sensitive data, establishing mapping relationships between the identities of VMUs and VTs for constant tracking [5]. Fortunately, as temporary authorized identifiers issued by trusted entities, pseudonyms offer a credible solution for identity anonymization by hiding the true identities of both VMUs and VTs [11]. Through synchronous pseudonym changes, the VMUs and the VTs can increase their privacy levels collectively [5].

Although employing pseudonyms can improve privacy protection, incorporating the pseudonym scheme into vehicular edge metaverses remains several challenges that must be addressed before practical implementation. These challenges include: 1) On account of the large-scale use of VMU and VT pseudonyms in vehicular edge metaverses, the issue of pseudonym management becomes considerably more intractable. Traditionally, the trusted authority (TA) in the cloud layer is responsible for generating, distributing, and revoking pseudonyms throughout the vehicular networks [8]. However, this approach may incur an unprecedentedly overwhelming management overhead in the vehicular edge metaverses. 2) Since pseudonyms are typically stored in centralized storage devices within vehicular networks, the vulnerability of sensitive identity privacy to external violations is heightened. Unauthorized access by malicious attackers to these devices could result in the exposure of all identity information in the metaverse system, leading to severe privacy breaches [10], [12]. 3) To maximize utility, both VMUs and VTs need to know where and when to change pseudonyms is better. However, there still lacks a generalized metric to measure the level of privacy protection after pseudonym changes, which significantly hinders the application of privacy-preserving pseudonym schemes in vehicular edge metaverses.

With the above motivation, we resort to blockchain-based pseudonym management for VT migrations in vehicular edge metaverses in this article. The major contributions of this article are summarized as follows.

1) We design a novel cross-metaverse framework for vehicular edge metaverses, with its hierarchical architecture enabling pseudonym management and metaverse service provisioning in an efficient way. The global metaverse consists of multiple local metaverses collaborating to complete dual pseudonym management, thereby ensuring privacy protection for both VMUs and VTs.
2) To ensure the pseudonym unforgeability and metaverse robustness, we utilize the cross-chain technology combining the notary mechanism to facilitate decentralized and secure pseudonym distribution and revocation during VT migrations in vehicular edge metaverses.
3) Furthermore, we propose a new metric named Degree of Privacy Entropy (DoPE), to quantify the level of privacy protection after pseudonym changes for the VMUs and VTs. Based on DoPE and inventory theory, we formulate the optimization problem of pseudonym generation within the entire metaverse system.
4) Given the variability of pseudonym demands as multiple VMUs and VTs dynamically request pseudonyms within different local metaverses, we employ an multiagent deep reinforcement learning (MADRL) algorithm to derive the optimal pseudonym generating strategy in vehicular edge metaverses.

The rest of this article is organized as follows. We first review the related literature in Section II. In Section III, we examine the components and security requirements in vehicular edge metaverses. Then, the details of our cross-metaverse framework are presented in Section IV. Following that, the problem of pseudonym generation incorporating the DoPE metric and inventory theory is formulated in Section V. To address the problem, we leverage an MADRL algorithm based on edge learning technology in Section VI. The performance evaluations including security analyses and numerical results of our proposed framework are performed in Section VII. Finally, Section VIII concludes this article.

II. Related Work

A. Pseudonym Management Framework

Some research works have been conducted to explore pseudonym management in Internet of Vehicles (IoV). For instance, Khan et al. [13] proposed a privacy-preserving identity management scheme for vehicular social networking to enhance the security of vehicles by logging and monitoring malicious pseudonyms. However, their centralized architecture incurs significant communication overhead, posing a challenge for managing both VMU and VT pseudonyms in vehicular edge metaverses. To address this, Kang et al. [9] presented a three-layer (cloud-fog-user) architecture for pseudonym management, in which they harnessed pseudonym fogs dispersed at the network edge to reduce management overhead. Nevertheless, their approaches may lead to sensitive data disclosure or tampering, as the pseudonym fogs are vulnerable to external attackers. To resolve the problem of single point of failure, Cheng et al. [14] further proposed a blockchain-assisted pseudonym management scheme for multidomain IoV, which involves a blockchain network jointly maintained by TA and key generation authority to store pseudonym identities and status for vehicles. However, if the single blockchain network under their scheme fails, all identity privacy in the metaverses could still be divulged.

B. Cross-Chain for Metaverse

As an effective tool for data security, the cross-chain technology shows its unique advantages in enhancing the interoperability and scalability of blockchain networks [15]. For metaverse applications, Wang et al. [1] proposed to use cross-chain technology to assist transaction authentication across submetaverses, but they did not conduct experiments to demonstrate the practicability of their idea. Kang et al. [16]

presented a cross-chain empowered federated learning framework for secure data training in healthcare metaverses. More recently, Li et al. [17] proposed a cross-metaverse protocol, with the cross-chain technology serving as a key component to achieve metaverse interoperability. Supported by their proposed protocol, the users within different metaverses are capable of quickly interacting with each other. Although previous works have delved into the applications of cross-chain technology in metaverses, none of them explores its significant potential for pseudonym management, particularly in vehicular edge metaverses.

C. Privacy Metric

To better assess the effectiveness of privacy protection of pseudonym schemes, researchers have proposed various privacy metrics. For instance, Liu et al. [18] conducted a systematic study on location privacy, which is defined by three attributes of vehicle location information, namely, identity, position, and time. However, they did not provide a mathematical definition to quantify privacy levels. Building on this, Kang et al. [9] utilized a metric called privacy entropy to measure the uncertainty of mapping pseudonyms to real identities from the perspective of adversaries. Nevertheless, this metric fails to capture the impact of each pseudonym change on location privacy. Therefore, Liu et al. [19] utilized a metric named pseudonym age to measure privacy levels, defined as the time interval between the last pseudonym change and the current one. However, this metric solely takes the time dimension into account but ignores the strength factor. As each pseudonym change yields different degrees of privacy enhancement based on real-time traffic conditions [9], the pseudonym age does not reflect the location privacy well. Consequently, there is still a need for a generalized metric that can analytically quantify the degree of privacy protection after pseudonym changes, particularly in the context of pseudonym-based vehicular edge metaverses.

D. Resource Optimization for Pseudonym Management

For the sake of cost-effective privacy preservation at the network edge, researchers have investigated optimization problems with regard to pseudonym management. For example, Artail and Abbani [20] developed an optimization algorithm to solve the pseudonym shuffling problem among RSUs in a distributed manner. Additionally, Chaudhary and Singh [21] leveraged the genetic algorithm to execute pseudonym generation, targeting the problem of location privacy preservation in vehicular ad hoc networks. Recently, Luo et al. [5] conducted a case study on pseudonym distribution formulated by the VMU utility with inventory theory. However, most existing research overlooks the intricate scenario of multiprovider multiconsumer pseudonym management, thereby constraining their performances in vehicular edge metaverses. Moreover, these studies typically rely on heuristics to solve the formulated problem, which lacks practicality in real-world applications. Therefore, it is urgent to develop a practical learning-based algorithm that can obtain an optimal pseudonym generating strategy in vehicular edge metaverses.

III. System Model

A. Network Model in Vehicular Edge Metaverses

1) *VTs:* The multimodal LLM-based VTs are one kind of powerful AI agents, which can evolve through engaging online in the vehicular edge metaverse, namely, synchronizing with their corresponding VMUs and interacting with other VTs [5]. In this way, VTs can better perform complex tasks by Chain-of-Thought (CoT) reasoning and planning in the edge layer, making more accurate decisions to enhance VMUs' driving safety and enrich on-board experience [6], [7]. However, the VT migrations may expose sensitive data (e.g., identity privacy) during dynamic communications within vehicular edge metaverses [10]. To mitigate potential privacy breaches, VTs can employ pseudonyms to effectively mask their true identities for anonymous communications [5].
2) *VMUs:* VMUs connect to edge servers to access vehicular edge metaverses through portable immersive devices, such as head-mounted displays (HMDs). To enjoy personalized services, the VMUs should continuously upload real-time sensing data collected by vehicular sensors to update their VTs [4]. In addition, their vehicles need to periodically broadcast safety messages to increase the contextual awareness of surrounding traffic conditions [9]. By synchronously changing pseudonyms with their VTs, VMUs can evade the continuous tracking by attackers during data synchronization and safety message broadcasting, thus safeguarding location privacy throughout the journeys [5].
3) *Edge Servers:* Vehicular edge metaverses are generally maintained by numerous edge servers geographically adjacent to VMUs to reduce service provisioning delays. With adequate computation, communication, and storage resources, the edge servers can perform latency-sensitive and computationally complicated tasks, such as VT simulation and visualization renderings [4]. Moreover, the edge servers expedite pseudonym management including pseudonym issuance, storage, allocation, and revocation [8], [9]. Combined with the blockchain technology, the edge servers function as miners to participate in consensus related to pseudonyms [16]. This integration fosters pseudonym security in vehicular edge metaverses.
4) *TA:* The TA can be a government agency equipped with anti-attack hardware to effectively thwart network attacks [9]. Located in the cloud layer, the TA with ample computing resources plays a pivotal role in overseeing pseudonym management operations as well as supervising VMUs, VTs, and edge servers within the entire metaverse. By synchronizing pseudonym information from edge servers on the blockchain network, the TA can verify pseudonym identities swiftly upon receiving messages related to pseudonyms, such as pseudonym renewals or misbehavior reports [14]. The pseudonym management is dominated by the fully trusted TA, thereby maintaining the pseudonym sustainability and accountability in vehicular edge metaverses [5].

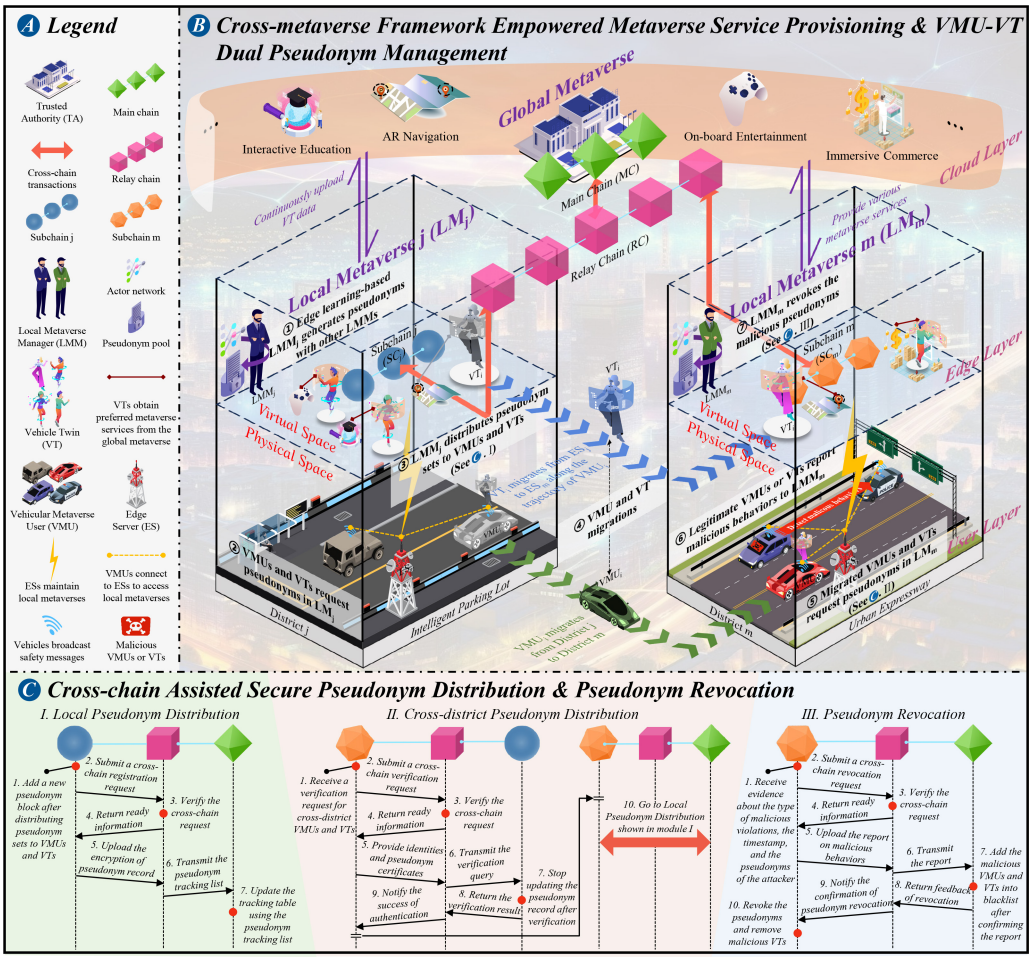


Fig. 1. Cross-metaverse paradigm integrated with cross-chain technology for twin migrations in vehicular edge metaverses. *Part. A* presents the element description in the vehicular edge metaverses. *Part. B* depicts the cross-metaverse framework in detail. *Part. C* provides the details of cross-chain transactions for pseudonym distribution and revocation in *Part. B*.

B. Security Requirements

The security threats in vehicular edge metaverses consist of purposeful behaviors and fatal attacks by malicious attackers. The attackers can be categorized into three main types: 1) Compromised VMUs, which eavesdrop basic safety messages from legitimate VMUs [9]; 2) Malicious VTs, which engage in intentional interactions with legal VTs to steal their sensitive privacy or disseminate fake news [5]; 3) Semi-trusted edge servers, which are curious about the data synchronization between legal VMUs and VTs [10], [22]. These edge servers are susceptible to hijacking by external attackers, affecting the normal pseudonym management in vehicular edge metaverses.

Considering the existence of the aforementioned attackers, to ensure normal operation in vehicular edge metaverses, the following security requirements must be strictly satisfied.

1) *Anonymity:* Anonymity is the foundation of vehicular edge metaverses, ensuring that the real identities of VMUs and their associated VTs remain undisclosed to other entities within the metaverse.
2) *Unlinkability:* Unlinkability ensures that colluding attackers cannot link the identities of VMUs with their associated VTs during vehicle and VT migrations, thus protecting location privacy for both VMUs and VTs.
3) *Immutability:* Immutability means that the sensitive pseudonym information should be guaranteed for data integrity and cannot be easily obtained or modified by external attackers.
4) *Conditional Traceability:* Conditional traceability grants the exclusive right to trace the true identities of VMUs and VTs and revoke the pseudonym use of malicious entities only to the creditable entities.
5) *Robustness:* Robustness is the ability of the blockchain network in vehicular edge metaverses to withstand external attacks and ensure on-chain data protection to a certain extent.
6) *Efficiency:* Due to ubiquitous communications in vehicular edge metaverses, the pseudonym management scheme should be highly efficient and cost-effective to ensure affordable and sustainable privacy protection.

IV. Cross-Metaverse Empowered VMU-VT Dual Pseudonym Management Framework

A. Overview of Hierarchical and Decentralized Architecture

To satisfy the security requirements mentioned above, we design a cross-metaverse empowered VMU-VT dual pseudonym management framework, as illustrated in Fig. 1.

The vehicular edge metaverse is regarded as a global metaverse encompassing multiple local metaverses to provide a variety of stunning metaverse services for VTs at the network edge, such as AR navigation and on-board entertainment [23], [24]. Afterwards, the associated VMUs in the user layer can obtain global traffic information while experiencing various kinds of metaverse services. This hierarchical architecture of our proposed framework expedites the metaverse service provisioning via cross-metaverse interactions. On one hand, the VTs within local metaverses continuously upload real-time data to the global metaverse, enabling it to render and offer customized services back to local metaverses. On the other hand, cross-metaverse interactions contribute to overcoming spatial limitations among different physical districts. For instance, if a traffic accident occurs in a certain local metaverse, the VMU witnessing the accident can notify its VT, and then the VT will forward this notification to the VTs in other local metaverses. In this way, the VMUs receiving the notification from their associated VTs can choose alternative routes, thus preventing the accident from escalating further.

In addition to facilitating metaverse service provisioning, the proposed cross-metaverse hierarchical architecture also plays a vital role in pseudonym management. Based on the above contents, we assume that the global metaverse is equipped with a TA in the cloud layer, and each local metaverse is equipped with a local metaverse manager (LMM) in the edge layer. Serving as regional trusted authorities, the LMMs are qualified to carry out the tasks of pseudonym management traditionally handled by the TA [9]. For instance, LMMs are capable of promptly generating and distributing pseudonyms to VMUs and VTs within local metaverses, substantially relieving the burdens of issuing, storing, transmitting, and recording pseudonyms in the cloud center.

Moreover, leveraging the blockchain technology to record pseudonym identities can ensure pseudonym confidentiality. However, in a single-chain system, the limited throughput and single-chain architecture become a constraint when handling massive pseudonymous transactions, potentially degrading the performance of the blockchain and causing irreversible damage to the metaverse [16]. Fortunately, the application of cross-chain technology can address the above challenges. As shown in Fig. 1, the hierarchical decentralized cross-chain architecture consists of a main chain, a relay chain, and multiple subchains. The main chain is maintained by the fully trusted nodes in the cloud layer (e.g., the TA), responsible for recording and verifying global pseudonyms and reports from various local metaverses. The relay chain facilitates the transmission of ciphertext, namely cross-chain requests between the main chain and subchains. Each local metaverse maintains a subchain in the edge layer, where edge servers function as miners using distributed consensus to add pseudonym blocks and LMMs serve as notaries to verify these blocks for cross-chain transactions [25].

In summary, the hierarchical cross-metaverse architecture enables efficient pseudonym management while the decentralized cross-chain architecture ensures sensitive privacy isolation. Consequently, our proposed framework effectively improves both management efficiency and data security for pseudonyms in vehicular edge metaverses.

TABLE I
KEY SYMBOLS USED IN THIS ARTICLE

Notation	Definition
$PID^k_{VMU_i}$	The k^{th} pseudonym of VMU_i. VMU_i requests a pseudonym set with w pseudonyms, $\{PID^k_{VMU_i}\}^w_{k=1} = \{PID^k_{VMU_i}\}$
$PID^l_{VT_i}$	The l^{th} pseudonym of VT_i. VT_i requests a pseudonym set with u pseudonyms, $\{PID^l_{VT_i}\}^u_{l=1} = \{PID^l_{VT_i}\}$
PK_{VMU_i}, SK_{VMU_i}	Public and private key pair of VMU_i
PK_{VT_i}, SK_{VT_i}	Public and private key pair of VT_i
$\{x\}$	A set with element x
$i \overset{(j)}{\rightarrow} k$	Entity i sends a message to entity k (through entity j)
$i \overset{(n)}{\Longrightarrow} c$	Entity i adds a new block to blockchain c (after the authentication of notary n)
$x\|\|y$	Element x concatenates to y
$E_{PK_i}(m)$	Encryption of message m using the public key of entity i
Ts	Timestamp of event

B. Cross-Chain Assisted Secure Pseudonym Management

Here, we provide a detailed description of cross-chain assisted pseudonym management processes in vehicular edge metaverses. For convenience, we list the symbols used in our proposed framework in Table I.

We adopt a lightweight Boneh-Boyen short signature scheme [26] for initial startup and key generation. When VMU_i with its true identity ID_{VMU_i} first joins the jth local metaverse, it sends an initial metaverse registration request to the nearest edge server. Then, the edge server will create VT_i for VMU_i after verifying ID_{VMU_i}, and both VMU_i and VT_i obtain its public/privacy key pairs and corresponding certificates (denoted as PK_{VMU_i}, PK_{VT_i}, SK_{VMU_i}, SK_{VT_i}, $Cert_{\text{VMU}_i}$, and $Cert_{VT_i}$) from the TA [9]. Afterwards, The TA notifies LMM_j to distribute a set of pseudonyms $\{PID^k_{\text{VMU}_i}\}^w_{k=1}$ and $\{PID^l_{VT_i}\}^u_{l=1}$ to VMU_i and VT_i, respectively. These pseudonyms are attached with the corresponding public/private key pairs and certificates (denoted as $PID^k_{\text{VMU}_i}$, $PID^l_{VT_i}$, $SK_{PID^k_{\text{VMU}_i}}$, $SK_{PID^l_{VT_i}}$, $Cert_{PID^k_{\text{VMU}_i}}$, and $Cert_{PID^l_{VT_i}}$). Following that, the TA creates a tracking table on the main chain MC, logging the true and pseudonym identities of VMU_i and VT_i as well as the pseudonym issuer LMM_j [9]. Meanwhile, the edge server adds a pseudonym registration block onto the subchain SC_j. Finally, the TA allocates a tracking list $\{PK_{\text{VMU}_i}, Cert_{\text{VMU}_i}, \text{LMM}_j, \{PID^k_{\text{VMU}_i}\}, \{Cert_{PID^k_{\text{VMU}_i}}\}\}$ to all local metaverses after encryption using LMMs' public keys. Here, we consider that all the LMMs are fully trusted while edge servers are semi-trusted [22]. The edge servers scattered across local metaverses link with each other via wired communications for better cooperation and mutual supervision [9]. The LMMs also supervise these edge servers and ban them from linking to the subchains for a specific period in case of detecting their misbehaviors during pseudonym management [13].

Protocol 1: Basic Operations of Pseudonym Management

1. LMM_j: generate G_j^t pseudonyms via the actor network trained by **Algorithm 1** and store them in the pseudonym pool
2. VMU_i: broadcast safety messages with VMU pseudonym $PID_{VMU_i}^k$ to neighboring VMUs and nearby ES_m
3. VT_i: interact with other VTs in virtual spaces and connect to VMU_i with VT pseudonym $PID_{VT_i}^l$
4. VMU_i & VT_i: change pseudonym synchronously
5. if VMU_i is (going to run out of pseudonyms issued by LMM_j)
5.1 if VMU_i is (within the coverage of the jth local metaverse)
VMU_i: Go to **Protocol 2**
else
VMU_i: Go to **Protocol 3**
endif
endif
6. LMM_j: Calculate the total pseudonym demand D_j^t within the jth local metaverse

1) Basic Operation: In our proposed scheme, the distributed LMMs are trained in parallel based on edge learning technology [2] to periodically generate pseudonyms and store them in pseudonym pools for subsequent allocation within local metaverses (see step ① in Fig. 1). When VMU_i moves within the jth local metaverse, the vehicle broadcasts safety messages with pseudonym $\{PID_{\text{VMU}_i}^k\}_{k=1}^w$ every 300 ms [9]. For simplicity, here we assume that both VMU_i and VT_i request the same number of pseudonyms [11]. VMU_i and VT_i can synchronously change their pseudonyms to prevent continuous tracking by attackers [5]. To ensure the validity of safety messages, VMU_i signs its messages with a timestamp to guarantee message freshness, in which pseudonym certificates are attached for identity verification [9]. Before depleting all available pseudonyms, VMU_i and VT_i request new pseudonyms from the local metaverse where they reside. Then, the local or cross-district pseudonym distribution protocol is correspondingly executed according to the VMU_i's current position. Further details can be found in Protocol 1.

2) Local Pseudonym Distribution: Before exhausting all pseudonyms, VMU_i and VT_i request new pseudonyms from the nearest edge server (denoted as ES_m) in the jth Local Metaverse (LM_j) where they previously conducted initialization (see step ② in Fig. 1). The request includes the number of requesting pseudonyms, the current location, the public key, the pseudonym being used, and corresponding certificates, all encrypted with LMM_j's public key [9]. After confirming that VMU_i and VT_i are in LM_j while verifying their identities on SC_j, LMM_j distributes the pseudonym set $\{PID_{\text{VMU}_i}^k\}$ and $\{PID_{\text{VMU}_i}^l\}$ to VMU_i and VT_i, respectively, (see step ③ in Fig. 1). Subsequently, ES_m generates a pseudonym registration block, which is added to SC_j with a distributed consensus algorithm [14]. Thereafter, SC_j submits a cross-chain registration request to the relay chain RC. After verifying by both LMM_j and RC, the block will finally forward to the main chain (*Module I* of *Part. C* in Fig. 1). More details are presented in Protocol 2.

Protocol 2: Local Pseudonym Distribution

1. $VMU_i \overset{ES_m}{\rightarrow} LMM_j$:
$request\_VMU = E_{PK_{LMM_j}}(Pseu\_request||PK_{VMU_i}||PID_{VMU_i}^n||Cert_{VMU_i}||Cert_{PID_{VMU_i}^n})$,
where $Pseu\_request = \{location_i||D_{j,i}^t||Ts\}$
2. $VT_i \rightarrow LMM_j$:
$request\_VT = E_{PK_{LMM_j}}(Pseu\_request||PK_{VT_i}||PID_{VT_i}^n||Cert_{VT_i}||Cert_{PID_{VT_i}^n})$
3. LMM_j: decrypt $request\_VMU$ and $request\_VT$ with SK_{LMM_j} to obtain VMU_i and VT_i's identities for verification
4. if LMM_j verified ($PID_{VMU_i}^n$, $PID_{VT_i}^n$, PK_{VMU_i} and PK_{VT_i} are on SC_j) and (VMU_i is within ES_m)
4.1 $LMM_j \overset{ES_m}{\rightarrow} VMU_i$:
$Reply\_VMU = E_{PK_{PID_{VMU_i}^n}}(\{PID_{VMU_i}^k, SK_{PID_{VMU_i}^k}, Cert_{PID_{VMU_i}^k}\}_{k=1}^w)||Ts$
4.2 $LMM_j \rightarrow VT_i$:
$Reply\_VT = E_{PK_{PID_{VT_i}^n}}(\{PID_{VT_i}^l, SK_{PID_{VT_i}^l}, Cert_{PID_{VT_i}^l}\}_{l=1}^u)||Ts$
4.3 $ES_m \overset{LMM_j}{\Longrightarrow} SC_j$:
$Record = (PK_{VMU_i}||\{PID_{VMU_i}^k, SK_{PID_{VMU_i}^k}, Cert_{PID_{VMU_i}^k}\}||Cert_{VMU_i})||Ts$
4.4 $SC_j \rightarrow RC$: cross-chain registration request
4.5 $RC \rightarrow SC_j$: ready information after authenticating SC_j
4.6 $SC_j \overset{RC}{\rightarrow} MC$:
$Tracking\_list = E_{PK_{TA}}(Record||Cert_{LMM_j})||Ts$
4.7 TA: download $Tracking\_list$ from MC and decrypt with SK_{TA} for information update
4.8 $TA \Longrightarrow MC$:
$Tracking\_table = \{ID_{VMU_i}||PK_{VMU_i}||PK_{VT_i}||Cert_{VMU_i}||Cert_{VT_i}||Cert_{LMM_j}||Ts||\{PID_{VMU_i}^k\}||\{PID_{VT_i}^l\}||\{Cert_{PID_{VMU_i}^k}\}||\{Cert_{PID_{VT_i}^l}\}\}$
else
LMM_j: do not reply
endif

3) Cross-District Pseudonym Distribution: Since VMU_i and its vehicle continuously migrate across different districts, the VT_i should be synchronously migrated among edge servers to access different local metaverses [4]. When VMU_i and VT_i have migrated from LM_j to LM_m (see step ④ in Fig. 1), they need to reapply for pseudonyms from ES_n using the last pseudonym $PID_{\text{VMU}_i}^{w-1}$ and $PID_{VT_i}^{u-1}$ issued by LMM_j (see step ⑤ in Fig. 1). In this case, cross-district pseudonym distribution will be executed. LMM_m audits VMU_i and VT_i's pseudonym identities through cross-chain verification

Protocol 3: Cross-district Pseudonym Distribution

1. $VMU_i \xrightarrow{ES_n} LMM_m$:
$request\_VMU = E_{PK_{LMM_m}}(Pseu\_request||PK_{VMU_i}||PID^{w-1}_{VMU_i}||Cert_{VMU_i}||Cert_{PID^{w-1}_{VMU_i}})$
2. $VT_i \rightarrow LMM_m$:
$request\_VT = E_{PK_{LMM_m}}(Pseu\_request||PK_{VT_i}||PID^{u-1}_{VT_i}||Cert_{VT_i}||Cert_{PID^{u-1}_{VT_i}})$
3. LMM_m: decrypt $request\_VMU$ and $request\_VT$ with SK_{LMM_j} to obtain VMU_i and VT_i's identities
4. if LMM_m verified ($PID^n_{VMU_i}$, $PID^n_{VT_i}$, PK_{VMU_i} and PK_{VT_i} are **not** on SC_m)
4.1 $SC_m \rightarrow RC$: cross-chain verification request
4.2 $RC \rightarrow SC_m$: ready information after verifying SC_m
4.3 $SC_m \xrightarrow{RC} SC_j$:
$Query = E_{PK_{LMM_j}}(PID^n_{VMU_i}||PID^n_{VT_i}||PK_{VMU_i}||PK_{VT_i}||Cert_{LMM_m})||Ts$
4.4 LMM_j: authenticate whether VMU_i and VT_i's identities are on SC_j via *record*
4.5 if both VMU_i and VT_i's identities are (verified on SC_j)
$SC_j \rightarrow SC_m$: $identity\ authenticated = True$
LMM_j: stop updating the record of VMU_i and VT_i
else
$SC_j \rightarrow SC_m$: $identity\ authenticated = False$
LMM_j: send this abnormal condition to TA
endif
4.6 if ($identity\ authenticated$)
LMM_m: execute pseudonym distribution following the processes of **4.1 - 4.9** in **Protocol 2**
else
pass
endif
else
LMM_m: do not reply
endif

Protocol 4: VMU-VT Dual Pseudonym Revocation

1. if VMU_i detects (VMU_k misbehaved in the physical space)
1.1 $VMU_i \xrightarrow{ES_n} LMM_m$:
$report_{VMU} = E_{PK_{LMM_j}}(Cert_{PID^n_{VMU_i}}||message_{VMU})$, where $message_{VMU} = \{Cert_{PID^m_{VMU_k}}||type||Ts\}$
elif VT_i detects (VT_k misbehaved in the virtual space)
1.2 $VT_i \rightarrow LMM_m$:
$report_{VT} = E_{PK_{LMM_j}}(Cert_{PID^n_{VT_i}}||message_{VT})$, where $message_{VT} = \{Cert_{PID^m_{VT_k}}||type||Ts\}$
endif
2. LMM_m: decrypt $report_{VMU}$ or $report_{VT}$ with SK_{LMM_m}
3. if LMM_m verified *message* ($message_{VMU}$ or $message_{VT}$) and the identity of reporter (VMU_i or VT_i) via SC_j
3.1 $ES_m \overset{LMM_j}{\Longrightarrow} SC_j$:
$report = E_{PK_{TA}}(PK_{VMU_k}||\{PID^m_{VMU_k}, SK_{PID^m_{VMU_k}}, Cert_{PID^m_{VMU_k}}\}||Cert_{LMM_m}||Cert_{VMU_k})||message||Ts$
3.2 $SC_j \rightarrow RC$: cross-chain revocation request
3.3 $RC \rightarrow SC_j$: ready information after verifying SC_j
3.4 $SC_j \xrightarrow{RC} MC$: *report*
3.5 *TA*: decrypt *report* with SK_{TA} and validate *message* with *Tracking_table* on *MC*
3.6 if *TA* confirmed (VMU_k or VT_k misbehaved)
TA: add VMU_k and VT_k into the blacklist and reveal the true identity ID_{VMU_k} to all edge servers
LMM_m: revoke the use of PID_{VMU_k} and PID_{VT_k} and remove VT_k from LM_j
else
TA: restrict the right of VMU_i and VT_i to report violation events
endif
else
LMM_m: do not reply
endif

(*Module II* of *Part. C* in Fig. 1). After the verification, LMM_m distributes pseudonyms following the processes of local pseudonym distribution. See the details in Protocol 3.

4) Dual Pseudonym Revocation: In the vehicular edge metaverses, both VMUs and VTs should mutually supervise their neighbors. Legitimate entities can accuse neighboring malicious individuals of engaging in misbehaviors (see step ⑥ in Fig. 1). For example, if the compromised VMU_k with $PID^m_{\text{VMU}_k}$ is perpetrating misbehaviors (e.g., spread fake traffic conditions) and is detected by VMU_i, VMU_i will record the pertinent violation information including the misbehavior type and timestamp, and report it to LMM_m via ES_n. Upon receiving the report, LMM_m first checks the validity of the report as well as the identity of VMU_i, and then ES_n adds the report onto the subchain SC_m. Then, SC_m will submit a cross-chain pseudonym revocation request (*Module III* of *Part. C* in Fig. 1). By auditing the complete identity information on the main chain *MC*, the TA can rapidly check the identities of entities involved in the report and validate the authenticity of the report [27]. If the misbehaviors are confirmed, TA will reveal the true identity of VMU_k to all edge servers in the metaverse, and then the LMM_m will revoke the use of both VMU and VT pseudonyms and remove VT_k from LM_m at once (see step ⑦ in Fig. 1) [9]. Eventually, The malicious VMU_k and VT_k are added to the blacklist, thereby banning them from communicating with other legal entities in vehicular edge metaverses. More details are described in Protocol 4.

V. Problem Formulation

A. Privacy Metric and VMU Utility

VMUs and VTs spread over local metaverses can synchronously change pseudonyms in groups with other entities to jointly increase their privacy levels [5]. Therefore, based on the definition of Age of Information (AoI) [28], [29] used

to characterize the latency in status updates, we propose a metric named DoPE to quantify location privacy levels for VMUs and VTs after pseudonym changes. Referring to [9], after each pseudonym change at time t_n^*, the DoPE can increase to privacy entropy, calculated by

$$H_n = -\log_2 p_i, \quad p_i \in [a, b]. \tag{1}$$

Here, the continuous random variable p_i represents the probability that attackers successfully track VMU$_i$ after VMU$_i$ changes a pseudonym [9], while a and b denote the reciprocal of the maximum and minimum number of vehicles at a social hotspot [9], respectively.

Without loss of generality, we consider that the autocorrelation of the pseudonym change processes is small because VMUs and VTs do not want their patterns of changing pseudonyms to be discovered by attackers. Therefore, an exponential DoPE is recommended to cope with this scenario [29]. As depicted in Fig. 2, the DoPE $H(t)$ declines exponentially over time, while increasing instantaneously when a VMU or VT replaces its current pseudonym with a new one at t_n^*. Note that $H(t)$ passes through the point (t_{i-1}, H_n), and thus the DoPE is defined as

$$H(t) = e^{-[t-t_{i-1}-\ln(1-\log_2 p_i)]} - 1. \tag{2}$$

We use the average DoPE in an observation time interval $(0, \mathcal{T})$ to study the global effect of pseudonym changes. Referring to [28], the time-average DoPE over $(0, \mathcal{T})$ is given as

$$H_{\mathcal{T}} = \frac{1}{\mathcal{T}} \int_0^{\mathcal{T}} H(t)dt. \tag{3}$$

To simplify, the area defined by the integral in (3) can be decomposed into a summation of multiple irregular geometric areas of the same type (i.e., $\widetilde{Q_1}$ and Q_i for $i \geq 2$). More specifically, the decomposition yields

$$\begin{aligned} H_{\mathcal{T}} &= \frac{\widetilde{Q_1} + \Sigma_{i=2}^{\mathcal{N}(\mathcal{T})} Q_i}{\mathcal{T}} \\ &= \frac{\widetilde{Q_1}}{\mathcal{T}} + \frac{1}{\mathcal{T}} \sum_{i=2}^{\mathcal{N}(\mathcal{T})} Q_i \end{aligned} \tag{4}$$

where $\mathcal{N}(\mathcal{T}) = \max\{n | t_n \leq \mathcal{T}\}$ denotes the number of pseudonym changes over a time interval $\mathcal{T}$. The term $(\widetilde{Q_1}/T)$ will vanish as $\mathcal{T} \to \infty$. Consequently, the time-average DoPE can be rewritten as

$$\overline{H} = \lim_{\mathcal{T}\to\infty} H_{\mathcal{T}} = \frac{\mathcal{N}(\mathcal{T})}{\mathcal{T}} \frac{1}{\mathcal{N}(\mathcal{T})} \sum_{i=2}^{\mathcal{N}(\mathcal{T})} Q_i. \tag{5}$$

Furthermore, for $i \geq 2$, the unit area can be obtained by

$$\begin{aligned} Q_i &= \int_{t_{i-1}}^{t_i} \left(e^{-[t-t_{i-1}-\ln(1-\log_2 p_i)]} - 1\right) dt \\ &= -e^{-[(t_i-t_{i-1})-\ln(1-log_2 p_i)]} + 1 - log_2 p_i - (t_i - t_{i-1}). \end{aligned} \tag{6}$$

For convenience, we define the elapsed time between the ith and $(i-1)$th pseudonym changes as

$$X_i = t_i - t_{i-1}. \tag{7}$$

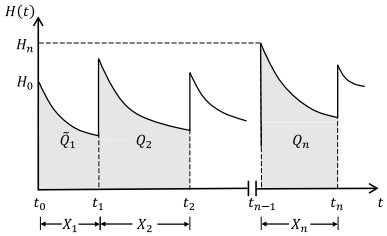


Fig. 2. Exponential DoPE for location privacy quantification.

Therefore, by substituting (7) into (6), the Q_i is converted into

$$Q_i = \left(1 - e^{-X_i}\right)(1 - log_2 p_i) - X_i. \tag{8}$$

Defining the steady pseudonym change frequency as $\lambda = \lim_{\mathcal{T}\to\infty} [\mathcal{N}(\mathcal{T})/\mathcal{T}]$, the time-average DoPE in (5) can be simplified as

$$\overline{H} = \lim_{\mathcal{T}\to\infty} H_{\mathcal{T}} = \lambda \mathbb{E}[Q_i] \tag{9}$$

where $\mathbb{E}[\cdot]$ represents the expectation operator.

The pseudonym changes of VMUs and VTs can be modeled as a Poisson process with rate λ [5]. Therefore, the elapsed times X_i are independent and identically distributed (iid) exponential random variables with $\mathbb{E}[X] = (1/\lambda)$ [29]. According to [9], the successful tracking probability p_i follows a uniform distribution, namely, $p_i \sim U(a, b)$. By substituting (8) into (9), the time-average DoPE can be obtained by

$$\overline{H} = \frac{\lambda}{\lambda + 1} \left(1 + \frac{1}{\ln 2} - \frac{b \log_2 b - a \log_2 a}{b - a}\right) - 1. \tag{10}$$

Guided by the time-average DoPE, the VMUs and VTs can assess their current privacy levels and decide whether to change pseudonyms. They can request pseudonyms from the local metaverse that they are in and continuously change pseudonyms for identity anonymization. Specifically, to quantify the surplus of privacy preservation through requesting and changing pseudonyms, we formulate VMU$_i$'s utility for consuming all requested pseudonyms over a time slot t in the jth local metaverse, represented as

$$u_{j,i}^t = -\varepsilon + \left(\beta \overline{H} - \delta\right) R_{j,i}^t \tag{11}$$

where ε, β, δ, and $R_{j,i}^t$ represent the basic cost of requesting new pseudonyms, the profit of improving privacy protection level by changing each pseudonym under unit DoPE, the additional cost of updating routing table of changing each pseudonym during VT migrations, and the number of pseudonyms that VMU$_i$ actually acquires in the jth local metaverse, respectively [5], [30]. Therefore, for the jth local metaverse with a set $\mathcal{I} = \{1, \ldots, i, \ldots, I\}$ of totally I VMUs, the VMU total utility can be obtained by

$$\mathcal{U}_j^t = \sum_{i\in\mathcal{I}} u_{j,i}^t = -I\varepsilon + \left(\beta \overline{H} - \delta\right) \mathcal{R}_j^t \tag{12}$$

where $\mathcal{R}_j^t = \min\{\mathcal{D}_j^t, G_j^t\}$ denotes the total number of pseudonyms that VMUs actually acquire at the beginning of time slot t in the jth local metaverse. D_j^t is the total pseudonym demand of VMUs and G_j^t is the number of pseudonyms generated by LMM$_j$ in the jth local metaverse.

B. Inventory Theory-Based Social Welfare Formulation

The LMM$_j$ periodically generates G_j^t pseudonyms based on the observed past pseudonym demands at the beginning of each time slot t and then distributes them to serve VMUs and VTs upon receiving pseudonym requests in the local metaverse. To better promote the privacy-preserving performance of this process within the whole metaverse, we jointly investigate the utilities of VMUs and the LMM in this article. The Newsvendor model [5] is a crucial component of stochastic inventory theory, which can help managers make informed decisions to maximize their surpluses. Therefore, we employ the Newsvendor model to investigate the optimization problem of pseudonym generation for the LMM. For LMM$_j$, during a time slot t, the pseudonym generation incurs generation costs due to computational consumption, while the pseudonym distribution yields provision profits for VMU privacy enhancement [5]. Moreover, if $G_j^t > D_j^t$, the redundant pseudonyms must be retained in the pseudonym pool for a specific duration, incurring storage costs. Conversely, if $D_j^t > G_j^t$, LMM$_j$ faces penalties because of not satisfying the pseudonym requirements of VMUs [5]. Specifically, the utility of LMM$_j$ is represented as

$$U_j^t = -gG_j^t + (p_0 - c)\mathcal{R}_j^t - h\max\left\{\left(G_j^t - \mathcal{D}_j^t\right), 0\right\} - r\max\left\{\left(\mathcal{D}_j^t - G_j^t\right), 0\right\} \tag{13}$$

where g, p_0, c, h, and r represent the cost of generating each pseudonym, the profit of supplying per pseudonym to VMUs, the communication overhead of distributing each pseudonym, the cost of storing each pseudonym, and the penalty for each unit of unmet pseudonym demand, respectively [5]. Note that p_0 is higher than c so that the LMM$_j$ can make profits through providing pseudonyms.

By considering the utilities of both VMUs and LMM$_j$, we can formulate the social welfare to study the network utilities that reflect the performance of privacy protection in the jth local metaverse. Covering a whole time period $\mathbf{T}$, the social welfare within the jth metaverse can be expressed by

$$SW_j^t = \left(\mathcal{U}_j^t + U_j^t\right), t \in \mathbf{T}. \tag{14}$$

Here, $\mathbf{T} = \{1, \ldots, t, \ldots, T\}$ means that the whole time period is divided into T equal time slots to recycle the pseudonym management processes [31]. Additionally, the number of pseudonyms generated by each LMM should not exceed the maximum $G_{\max}^t$ because of the computation limitations, and the total number within local metaverses cannot exceed the threshold as TA in the cloud layer can only register a specific number of pseudonym from the main chain within time slot t. Consequently, the optimization problem of pseudonym management can be transformed into maximizing the overall social welfare, formulated as

$$\textbf{Problem 1:} \sum_{j\in\mathcal{J}} \max\ SW_j^t$$
$$\text{s.t. } 0 \le G_j^t \le G_{\max}^t$$
$$\sum_{j\in\mathcal{J}} G_j^t \le \theta t$$
$$0 < c < p_0$$
$$0 < \delta < \beta\overline{H}. \tag{15}$$

The set $\mathcal{J} = \{1, \ldots, j, \ldots, J\}$ represents that the global metaverse consists of J local metaverses, while $G_{\max}^t$ and θ refer to the maximum number of pseudonyms that can be generated and the upper limit rate of registering pseudonym certificates by the TA within t, respectively.

Theorem 1: The independent social welfare in a certain local metaverse SW_j^t can reach its maximum.

Proof: The utility in (13) can be rewritten as $U_j^t = -gG_j^t + (p_0 - c)\min\{\mathcal{D}_j^t, G_j^t\} - h(G_j^t - \mathcal{D}_j^t)^+ - r(\mathcal{D}_j^t - G_j^t)^+$, where $x^+ = \max(x, 0)$. By exploiting the time-varying characteristic of U_j^t, we further transform the utility into

$$\begin{aligned} U_j^t &= (p_0 - c + r - g)G_j^t - (p_0 - c + r + h)\left(G_j^t - \mathcal{D}_j^t\right)^+ - r\mathcal{D}_j^t \\ &= (p_0 - c + r - g)G_j^t \\ &\quad -(p_0 - c + r + h)\int_0^{G_j^t}\left(G_j^t - \mathcal{D}_j^t\right)f\left(\mathcal{D}_j^t\right)d\mathcal{D}_j^t - r\mathcal{D}_j^t. \end{aligned} \tag{16}$$

Therefore, the social welfare in the jth local metaverse in time slot t is given by

$$\begin{aligned} SW_j^t &= \left[-I\varepsilon + \left(p_0 - c + r - g + \beta\overline{H} - \delta\right)\right]G_j^t \\ &\quad -\left(p_0 - c + r + h + \beta\overline{H} - \delta\right)\int_0^{G_j^t}\left(G_j^t - \mathcal{D}_j^t\right)f\left(\mathcal{D}_j^t\right)d\mathcal{D}_j^t - r\mathcal{D}_j^t. \end{aligned} \tag{17}$$

By taking the first-order and second-order derivatives of SW_j^t with respect to G_j^t, we can obtain

$$\begin{aligned} \frac{\partial SW_j^t}{\partial G_j^t} &= \left(p_o - c + r - g + \beta\overline{H} - \delta\right) \\ &\quad -\left(p_0 - c + r + h + \beta\overline{H} - \delta\right)F\left(G_j^t\right) \end{aligned} \tag{18}$$

$$\frac{\partial^2 SW_j^t}{\partial G_j^{t2}} = -\left(p_0 - c + r + h + \beta\overline{H} - \delta\right)f\left(G_j^t\right) < 0 \tag{19}$$

where $F(\cdot)$ denotes the cumulative distribution function (CDF) of $\mathcal{D}_j^t$. Notably, the first-order derivative has a unique zero point, and the second-order derivative is negative, indicating that the social welfare SW_j^t is strictly concave. According to the Newsvendor model, the maximum social welfare in the jth local metaverse is achieved when $(\partial SW_j^t/\partial G_j^t) = 0$, namely

$$G_j^{t*} = F^{-1}\left(\frac{p_o - c + r - g + \beta\overline{H} - \delta}{p_o - c + r + h + \beta\overline{H} - \delta}\right). \tag{20}$$

Here, G_j^{t*} is the optimal number of pseudonyms generated by LMM$_j$. Therefore, when LMM$_j$ generates G_j^{t*} at time slot t, the independent social welfare in the jth local metaverse can reach its maximum. ■

Although the independent social welfare in each local metaverse can reach its maximum, the constraint of pseudonym generation among LMMs complicates the problem of maximizing the overall social welfare. To be specific, the TA cannot register a large number of pseudonyms in a short time, and thus the total number of generated pseudonyms of LMMs in a given time slot should not exceed the predefined maximum.

Moreover, due to the variable pseudonym demands of VMUs and the uncertain communication overhead of transmitting pseudonyms within each local metaverse, determining how LMMs collaborate to achieve the optimal pseudonym generation set $\mathbb{G}^{t*} = \{G_j^{t*}\}$ still poses a considerable challenge.

VI. Solution: MADRL-Based Pseudonym Generating Strategy

To address the aforementioned challenges, we model the pseudonym generation by multiple LMMs as a partially observable Markov decision process (POMDP) [32]. According to the properties of POMDP, we adopt an MADRL algorithm based on edge learning technology [2] to resolve this problem, of which the details are presented as follows.

A. POMDP for Multiagent Pseudonym Generation

1) State Space: The entire period of pseudonym changes is segmented into equal time steps. At the beginning of time step t, the agent LMM_j generates G_j^t pseudonyms to satisfy the pseudonym requirements within the jth locals metaverse. After t, the VMUs distributed in each local metaverse consume all requested pseudonyms to enhance their respective location privacy, and then LMM_j regenerate pseudonyms to meet the following pseudonym demands. Since LMMs only make decisions according to the previous observations, we formulate the pseudonym generation as a POMDP. For each LMM_j, we define the observation o_j^t at the current decision step t as a union of past L-step observations, which is given by

$$o_j^t \triangleq \left\{c_j^{t-L}, Q_j^{t-L}, \mathcal{D}_j^{t-L}, \ldots, c_j^{t-1}, Q_j^{t-1}, \mathcal{D}_j^{t-1}\right\} \tag{21}$$

where c_j^t, Q_j^t, and $\mathcal{D}_j^t$ are the average communication overhead between LMM_j and VMUs, the periodic pseudonym overproduction, and pseudonym demands of VMUs at time step t in the jth local metaverse, respectively. $Q_j^t = G_j^t - \mathcal{D}_j^t (t \in \{t-L, \ldots, t-1\})$. Consequently, the observation space is defined as the aggregation of observations of all LMMs, denoted as $\boldsymbol{o}^t = \{o_1^t, \ldots, o_j^t, \ldots, o_J^t\}$.

2) Action Space: In vehicular edge metaverses, we define an action of LMM_j generating pseudonyms at the beginning of t within its local metaverse as $a_j^t = \{G_j^t\}$ [31]. Hence, the action space is a set containing the actions of each agent, represented by $\boldsymbol{a}^t = \{a_1^t, \ldots, a_j^t, \ldots, a_J^t\}$.

3) Reward: According to the current observation state o_j^t, the edge learning-based LMM_j selects an action a_j^t to gain the reward, and then o_j^t transitions to o_j^{t+1} [2]. The reward for pseudonym generation of each agent at time slot t can be defined as $R(o_j^t, a_j^t) = SW_j^t$. In the vehicular edge metaverses, maximizing social welfare is the common goal of LMMs. Therefore, the reward function is the sum of LMM's reward at time slot t, defined as

$$R\left(\boldsymbol{o}^t, a^t\right) = \begin{cases} \sum_{j\in\mathcal{J}} R\left(o_j^t, a_j^t\right), & \sum_{j\in\mathcal{J}} G_j^t \le \theta t \\ 0, & \text{otherwise.} \end{cases} \tag{22}$$

For convenience, we abbreviate $R(o_j^t, a_j^t)$ and $R(\boldsymbol{o}^t, a^t)$ as R_j^t and R^t, respectively.

B. Algorithm Details

We adopt the actor-critic framework and employ the multiagent proximal policy optimization (MAPPO) approach with centralized training and decentralized execution for policy iteration [33], [34]. The hyperparameters of LMM_j's policy π_{θ_j} and collective policy $\pi_{\boldsymbol{\theta}}$ are denoted as θ_j and $\boldsymbol{\theta}$, respectively. Here, $\boldsymbol{\theta} = \{\theta^1, \ldots, \theta^N\}$. Therefore, the objective of MAPPO can be formulated as

$$\max_{\boldsymbol{\theta}} \mathbb{E}_{\pi_{\boldsymbol{\theta}}^{\text{old}}} \left\{ \sum_{j\in\mathcal{J}} G\left[r\left(\theta_j\right), A_{\pi_{\boldsymbol{\theta}}^{\text{old}}}(\boldsymbol{o}, \boldsymbol{a})\right] \right\} \tag{23}$$

where the current policy of LMMs $\pi_{\boldsymbol{\theta}}^{\text{old}}$ is a differentiable function with hyperparameter $\boldsymbol{\theta}^{\text{old}}$ and $A_{\pi_{\boldsymbol{\theta}}^{\text{old}}}(\boldsymbol{o}^t, \boldsymbol{a}^t)$ is the advantage function [33]. To achieve feasible implementation of algorithm training, the objective function can be calculated by the expectation over a batch of samples. Specifically, the policy network of LMM_j is updated through gradient ascent [4], expressed as

$$\Delta\theta_j = \nabla_{\theta_j} \hat{\mathbb{E}}_t \left\{ G\left[r_t\left(\theta_j\right), A_j(\boldsymbol{o}_t, \boldsymbol{a}_t)\right] \right\}. \tag{24}$$

Here, $\mathbb{E}_t\{\cdot\}$ is the sample average and $r_t(\theta_j) = ([\pi_{\theta_j}(\boldsymbol{a}_t|\boldsymbol{o}_t)]/[\pi_{\theta_j^{\text{old}}}(\boldsymbol{a}_t|\boldsymbol{o}_t)])$ is the importance ratio [4]. $A_j(\boldsymbol{o}^t, \boldsymbol{a}^t)$ is the estimation of $A_{\pi_{\boldsymbol{\theta}}^{\text{old}}}(\boldsymbol{o}^t, \boldsymbol{a}^t)$, which can be calculated based on the generalized advantage estimation (GAE) method [4]. We also leverage a clip mechanism [33] to constrain the policy updates in (24), which can be further expressed by

$$G\left[r_t\left(\theta_j\right), A_j(\boldsymbol{o}_t, \boldsymbol{a}_t)\right] = \min \left\{ r_t\left(\theta_j\right) A_j\left(\boldsymbol{o}^t, \boldsymbol{a}^t\right), g_{\text{clip}}\left[\epsilon, A_j\left(\boldsymbol{o}^t, \boldsymbol{a}^t\right)\right] \right\} \tag{25}$$

where

$$g_{\text{clip}}(\epsilon, A) = \begin{cases} 1-\epsilon, & A < 0, \\ 1+\epsilon, & A \ge 0. \end{cases} \tag{26}$$

Note that $\epsilon \in [0, 1]$ is the clipping parameter [33].

In this article, we calculate the advantage estimation in the form of state-action value function [33]. To tackle the problem of not knowing the impact that LMM_j generates a certain number of pseudonyms on the total reward (i.e., the multiagent credit assign problem), we also use a counterfactual baseline [35] to calculate the estimates, given by

$$A_j\left(\boldsymbol{o}^t, \boldsymbol{a}^t\right) = \hat{Q}_j\left(\boldsymbol{o}^t, \boldsymbol{a}^t\right) - b\left(\boldsymbol{o}^t, \boldsymbol{a}_{-j}^t\right). \tag{27}$$

Here, $b(\boldsymbol{o}^t, \boldsymbol{a}_{-j}^t) = \sum_{a_j^t} \pi_{\theta_j}^{\text{old}}(a_j^t|o_j^t) Q_{\omega_j}[\boldsymbol{o}^t, (\boldsymbol{a}_{-j}^t, a_j^t)]$ is the counterfactual baseline, and $\boldsymbol{a}_{-j}^t$ is the joint action of other agents except LMM_j [33]. $\hat{Q}_j(\boldsymbol{o}^t, \boldsymbol{a}^t)$ is the estimation of state-action value function, calculated by

$$\hat{Q}_j\left(\boldsymbol{o}^t, \boldsymbol{a}^t\right) = Q_{\tilde{\omega}_j}\left(\boldsymbol{o}^t, \boldsymbol{a}^t\right) + \delta_t + \left(\gamma\lambda_{\text{gae}}\right)\delta_{t+1} + \cdots + \left(\gamma\lambda_{\text{gae}}\right)^T \delta_T \tag{28}$$

where the TD error $\delta_t = R_t + \gamma Q_{\tilde{\omega}_j}(\boldsymbol{o}^{t+1}, \boldsymbol{a}^{t+1}) - Q_{\tilde{\omega}_j}(\boldsymbol{o}^t, \boldsymbol{a}^t)$, $Q_{\tilde{\omega}_j}(\boldsymbol{o}^t, \boldsymbol{a}^t)$ is the centralized critic of LMM_j. γ is the discount factor, and λ_{gae} is the decay factor [33].

Algorithm 1: MAPPO Algorithm for Pseudonym Generation in Vehicular Edge Metaverses

Initialize maximum episodes E, maximum time steps T in an episode, maximum epochs K, and batch size B ;
Initialize actor π_{θ_j}, $\pi_{\theta_j}^{old}$ and critic Q_{ω_j}, $Q_{\overline{\omega}_j}$;
for *Episode* $e = 1, 2, \ldots, E$ **do**
  Reset Pseudonym Generation Environment *PGEnv* and replay buffer $\mathcal{BF}$;
  for *Time step* $t = 1, 2, \ldots, T$ **do**
    Each agent LMM_j observes o_j^t and selects an action a_j^t according to its current actor policy $\pi_{\theta_j}^{old}$;
    Get the reward r_t and update $\boldsymbol{o}^t$ into $\boldsymbol{o}^{t+1}$;
  end
  Each agent LMM_j obtains a trajectory $\tau_j = \{o_j^t, a_j^t, R_j^t, o_j^{t+1}\}_{t=1}^T$;
  Compute $\{\hat{Q}_j(\boldsymbol{o}^t, \boldsymbol{a}^t)\}_{t=1}^T$ according to Eq. (28);
  Compute advantages $\{A_j(\boldsymbol{o}^t, \boldsymbol{a}^t)\}_{t=1}^T$ according to Eq. (27);
  Store data $\{\{o_j^t, a_j^t, \hat{Q}_j[\boldsymbol{o}^t, \boldsymbol{a}^t], A_j[\boldsymbol{o}^t, \boldsymbol{a}^t]\}_{j=1}^J\}_{t=1}^T$ into replay buffer $\mathcal{BF}$;
  for *Epoch* $k = 1, 2, \ldots, K$ **do**
    Shuffle the data order in $\mathcal{BF}$;
    for $l = 1, 2, \ldots, \frac{T}{B} - 1$ **do**
      Sample a mini-batch of data d_l with a size B from $\mathcal{BF}$, where $d_l = \{[o_j^m, a_j^m, \hat{Q}_j[\boldsymbol{o}^m, \boldsymbol{a}^m], A_j[\boldsymbol{o}^m, \boldsymbol{a}^m]_{j=1}^J\}_{m=1+Bl}^{B(l+1)}$ **for** $j = 1, 2, \ldots, J$ **do**
        $\Delta\theta_j = \frac{1}{B}\sum_{m=1}^{B}\{\nabla_{\theta_j} G[r_m(\theta_j), A_j(\boldsymbol{o}_m, \boldsymbol{a}_m)]\}$
        $\Delta\omega_j = \frac{1}{B}\sum_{m=1}^{B}\{\nabla_{\omega_j}(\hat{Q}_j(\boldsymbol{o}_m, \boldsymbol{a}_m) - Q_{\omega_j}(\boldsymbol{o}_m, \boldsymbol{a}_m))^2\}$
        Apply gradient ascent to update actor parameter θ_j using $\Delta\theta_j$;
        Apply gradient descent to update critic parameter ω_j using $\Delta\omega_j$;
      end
    end
  end
  Update $\theta_j^{(old)} \leftarrow \theta_j$ and $\overline{\omega}_j \leftarrow \omega_j$ for each LMM_j;
end

The complete pseudo-code of the MAPPO algorithm for pseudonym generation is presented in Algorithm 1. During the collecting process, each agent LMM_j continually interacts with the pseudonym generation environment to select an action with the current policy $\pi_{\theta_j^{(old)}}$ to obtain the trajectories. Then, the Q-function and advantage estimation are calculated by the target critic $Q_{\bar{\omega}_j}$. After that, the data $\{\{o_j^t, a_j^t, \hat{Q}_j(\boldsymbol{o}^t, \boldsymbol{a}^t), A_j(\boldsymbol{o}^t, \boldsymbol{a}^t)\}_{\text{j=1}}^J\}_{t=1}^T$ will be stored in the replay buffer. During the training process, the optimizer randomly samples experiences from the replay buffer to update the network parameters [4] in each epoch. Then, the network parameters $\theta_j^{(old)}$ and $\overline{\omega}_j$ are updated to θ_j and ω_j, respectively. For each agent LMM_j, the critic parameter ω_j is updated by minimizing the loss function $L(\omega_j) = (\hat{Q}_j(\boldsymbol{o}^t, \boldsymbol{a}^t) - Q_{\omega_j}(\boldsymbol{o}^t, \boldsymbol{a}^t))^2$. The time complexity of the employed MAPPO algorithm hinges on the multiplication operations within multiple fully-connected deep neural networks [4], [32]. This complexity is denoted by $\mathcal{O}(\sum_{f=1}^{F+1} \xi_f \xi_{f-1})$, where ξ_f signifies the number of neural units in the f^{th} layer and F represents the total number of hidden layers.

VII. Performance Evaluation

A. Security Analysis

The cross-metaverse empowered dual pseudonym management framework has a positive effect on privacy protection, satisfying the following anticipated security requirements.

1) *Reliable Privacy Protection:* The proposed framework ensures *anonymity* in vehicular edge metaverses by allowing both VMUs and VTs quickly acquire pseudonyms in the local metaverse to conceal their true identities [5], [11]. The VMUs and VTs can utilize the DoPE to evaluate their current privacy levels and decide whether to change pseudonyms. Even if attackers have eavesdropped a safety message including a VMU pseudonym identity, they cannot link it to the associated VT. This is because when VMU and VT change pseudonyms synchronously, attackers will confuse the identity of the target VMU with that of other VMUs in the same local metaverse [5], meaning that the security requirement *unlinkability* is well satisfied.
2) *Data Integrity and Immutability:* To improve management efficiency and pseudonym security, we utilize a consortium blockchain and practical byzantine fault tolerance (PBFT) consensus algorithm in the cross-chain system [3], [36]. Given the nature of integrity of hash-based blocks, the subchain in the local metaverse cannot be easily cracked by attackers, thereby guaranteeing pseudonym *immutability*. Furthermore, combined with the notary mechanism, only the authenticated edge servers are permitted to make cross-chain transactions. Hence, only the fully trusted TA, notaries (i.e., LMMs) and verified nodes can access data on the relay chain and other subchains, thus ensuring the *conditional traceability* in vehicular edge metaverses. Moreover, even though a certain subchain in a local metaverse crashes due to a disastrous attack, the relay chain and other subchains can continue to operate because the on-chain data are partially isolated among subchains. This demonstrates the *robustness* of our proposed framework.
3) *Efficient Pseudonym Management:* With the aid of the hierarchical cross-metaverse architecture, the pseudonym management is accelerated by LMMs in the edge layer, significantly reducing the communication delay compared to traditional centralized schemes [9]. Moreover, the MADRL algorithm based on edge learning technology enables multiple LMMs to generate pseudonyms swiftly [2]. Therefore, we achieve high *Efficiency* in pseudonym management.

B. Performance Analysis of the Cross-Chain Assisted Pseudonym Management Scheme

To evaluate the proposed cross-chain assisted pseudonym management, we conduct simulation experiments w.r.t. blockchains on the FISCO BCOS platform integrated with a

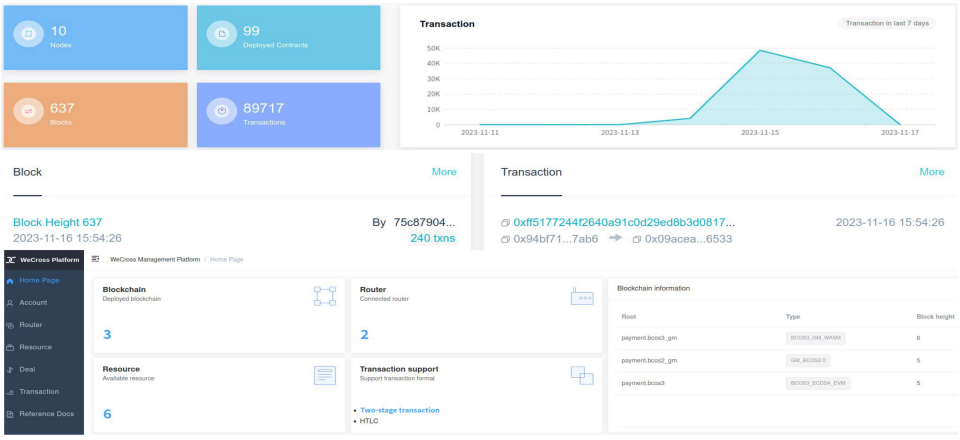


Fig. 3. Blockchain system building on FISCO BCOS and WeCross platforms. The figure shows the status of the single-chain and cross-chain system with block and transaction information.

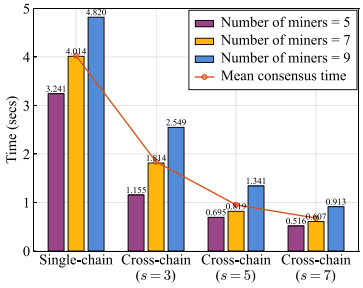


Fig. 4. Consensus time comparison between single-chain and cross-chain system.

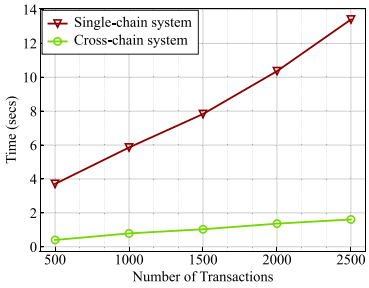


Fig. 5. Consensus time corresponding to different numbers of transactions under different system types.

cross-chain platform called WeCross [16], as shown in Fig. 3. The simulations are run on an Ubuntu 22.04 system with an Intel Core i7-12700 CPU @2.10 GHz, including 8 GB RAM. By default, the number of pseudonym-related transactions is set to 1000, and the data size per transaction is set to 1 KB [13]. Meanwhile, We employ five subchains in our cross-chain system as the default setting.

Fig. 4 shows the consensus time for adding new blocks (e.g., pseudonym registration information) in the single-chain system and the cross-chain system. Focusing on the red solid line, we find that the single-chain system takes the longest mean consensus time to complete 1000 transactions. In contrast, our cross-chain system with the PBFT consensus significantly reduces the consensus time [37]. As the number of subchains s increases from 3 to 7, the average consensus time in our cross-chain system decreases from 1.839 s to 0.679 s, indicating that the consensus efficiency of our cross-chain system is nearly 6× higher than that of the single-chain system when the number of subchains exceeds 7. Additionally, as the number of miners increases, the time for adding blocks increases because there are more nodes participating in the consensus.

Fig. 5 shows the effects of the number of transactions on consensus time. It is evident that as the number of transactions increases, both the single-chain system and cross-chain system undergo incremental block delays. Nonetheless, the consensus time in our cross-chain system increases smoothly, whereas the single-chain system experiences a much sharper increase. Compared with the single-chain scheme, our proposed schemes exhibit a notable reduction in consensus time by 87.973% when processing 2500 transactions, showcasing their capability to handle high-throughput scenarios of pseudonym management in vehicular edge metaverses.

TABLE II
PSEUDONYM REQUESTING DELAY (MILLISECONDS) COMPARISON

System type	Cryptographic operation time	Communi-cation delay	Blockchain verification time	
			local	*cross-district*
Single-chain	19	60	28	
Cross-chain	7	50	21	806

Table II shows a comparison of pseudonym requesting delay, which encompasses cryptographic operation time, communication delay, and blockchain verification time. According to [9], the cryptographic operation time includes the time of asymmetric encryption and decryption, the time of signature generation and verification, and the time of certificate verification, which are set to 1.86 ms, 0.94 ms, 0.93 ms, 1.11 ms, 5.42 ms, respectively. The communication delay comprises the delays between the VMU and edge server, edge server and LMM, and edge server and TA, set to 20 ms, 5 ms, and 10 ms, respectively [9]. We can see that for local pseudonym distribution (denoted as *local*) in our cross-chain system, all three types of time are lower compared

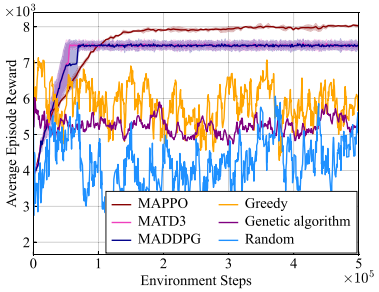


Fig. 6. Comparison of average episode reward curves of MAPPO and benchmarks for the pseudonym generation task.

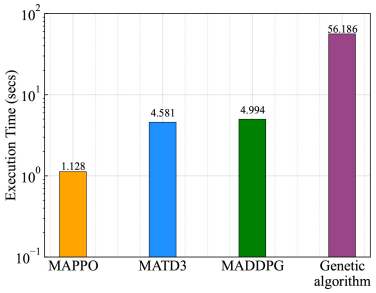


Fig. 7. Execution time of obtaining optimal strategy for pseudonym generation under different schemes.

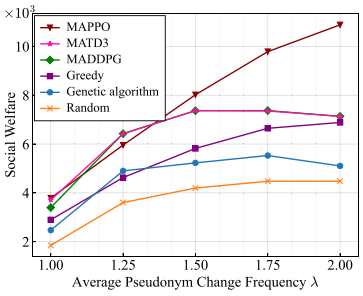


Fig. 8. Social welfare under different average pseudonym change frequencies.

to the single-chain system. This is because the distributed LMMs close to VMUs can reduce operational complexity and communication latency, and there are fewer workers participating in consensus on the subchain, which can improve verification efficiency. Despite the slightly higher verification time for cross-district pseudonym distribution (denoted as *cross-district*), our proposed scheme is still practical. Under acceptable time overhead, the pseudonyms are only recorded on original subchains when VMUs and VTs migrate among local metaverses in our cross-chain scheme, thus partially isolating sensitive data to enhance secure pseudonym management.

C. Performance Analysis of the Proposed Pseudonym Generation Method

1) Parameter Setting: To evaluate the performance of the MAPPO algorithm for pseudonym generation, we investigate a scenario where multiple LMMs generate pseudonyms to meet the pseudonym demands of VMUs in simulation experiments. Specifically, We consider that there are three LMMs and the number of VMUs in each local metaverse $\mathcal{I}$ is set to $[80, 70, 60]$. We assume that the varying pseudonym demands in each local metaverses follow a Poisson distribution with mean $[80, 90, 100]$ per minute, since generally the fewer VMUs in a district, the more pseudonyms are needed for privacy preservation. For simplicity, we consider that the communication overhead follows a uniform distribution, namely, $c_j^t \sim U[0, 0.2]$. Meanwhile, we set default values $\varepsilon = 0.1$, $\beta = 0.2$, $\delta = 0.5$, and $p_0 = 1.5$. The length of a time slot t is set to 60 s, the maximum number of generated pseudonyms of each LMM $G_{\max}^t$ is set to 120, and the upper limit rate for registering pseudonyms in the global metaverse θ is set to 5 per second. The minimum and maximum number of vehicles in a local metaverse are set to 10 and 160, respectively. Regarding the configuration of learning-based algorithms, we set $T = 120$, $L = 3$, $K = 15$, and $B = 16$. The learning rate of actor and critic is set to 0.001. The clip parameter g_{clip} is set to 0.2. The discount factor γ is set to 0.99, and the decay factor λ_{gae} is set to 0.95. Finally, ξ_f and F are set to 64 and 1, respectively.

2) Convergence Analysis: As shown in Fig. 6, we compare the convergence performance of our proposed MAPPO-based scheme with several benchmark approaches, including 1) *multiagent deep deterministic policy gradient* (MADDPG), 2) *multiagent twin delayed deep deterministic policy gradient* (MATD3), 3) *genetic algorithm* [21], 4) *random*, and 5) *greedy*. The MADDPG and MATD3 are learning-based algorithms [34], while the genetic algorithm is a classical heuristic algorithm. In the random scheme, the LMM randomly determines the number of pseudonyms to generate, while in the greedy scheme, the LMM determines the number based on the maximum utility achieved in previous time steps. We can see that the proposed scheme can converge on the maximum reward, outperforming MATD3, MADDPG, genetic algorithm, greedy, and random by 8.7%, 8.8%, 37.1%, 53.3%, and 92.9%, respectively. Since the pseudonym demands are time-varying, traditional heuristic algorithms fail to reach the convergence value. In Fig. 7, we compare the execution time of each algorithm over 1000 episodes. The proposed MAPPO-based scheme is found to be four times faster than other learning-based algorithms and nearly 50× faster than the heuristic. Consequently, our MAPPO-based solution requires less training time and performs better, highlighting its competence in pseudonym generation for vehicular edge metaverses.

3) Utility Analysis: Fig. 8 shows the impact of pseudonym change frequency on social welfare. From (10) we know that the time-average DoPE is positively correlated with average pseudonym change frequency λ. It is observed that our MAPPO-based scheme achieves the highest social welfare under different λ, except for 1.25. Furthermore, with the λ ranging from 1.75 to 2, the social welfare decreases under the methods of MATD3, MADDPG, and the genetic algorithm. This phenomenon implies that these baseline schemes are not well-suited for the complex vehicular edge metaverse with ever-changing pseudonym demands. Therefore, our proposed method exhibits greater feasibility when applied in metaverses.

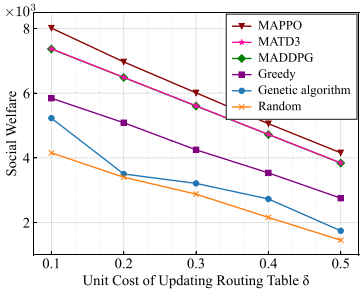


Fig. 9. Social welfare under different unit costs of updating routing table.

Fig. 9 shows the effect of different unit costs of updating routing table on the social welfare under various schemes. On account of the dynamic migrations in vehicular edge metaverses, changing both VMU and VT pseudonyms can incur a heterogeneous cost of updating routing table within different local metaverses [30]. We find that our proposed scheme consistently achieves maximum social welfare under each unit cost of updating routing table δ. Therefore, the proposed schemes exhibit greater adaptability to the fluctuating network condition within vehicular edge metaverses.

VIII. Conclusion

In this article, we examined the transformative potential of privacy-preserving pseudonym management in vehicular edge metaverses. Considering the dynamic nature of VMU and VT migrations, we presented a cross-metaverse empowered dual pseudonym management framework, in which the global metaverse consists of multiple local metaverse collaborating for efficient VMU and VT pseudonym management. Then, we integrated the cross-chain technology into our framework, with its decentralized architecture facilitating secure pseudonym distribution and revocation. Furthermore, we proposed an analytical metric named DoPE to assess the degree of privacy protection after pseudonym changes for VMUs and VTs. Combining DoPE with inventory theory, we formulated the optimization problem of pseudonym generation in vehicular edge metaverses. Additionally, due to the ever-changing pseudonym demands within multiple local metaverses, we employed an MADRL algorithm based on edge learning technology to achieve high-efficiency and cost-effective pseudonym generation. Finally, numerical results demonstrated the effectiveness and feasibility of our proposed framework in vehicular edge metaverses. For future work, we will further explore the applications of advanced optimization tools and the proposed metric across various domains in vehicular metaverses, such as pseudonym changes and exchanges, among others.

Acknowledgment

Jiawen Kang is with the School of Automation and the Guangdong Basic Research Center of Excellence for Ecological Security and Green Development, Key Laboratory for City Cluster Environmental Safety and Green Development of the Ministry of Education, Guangdong University of Technology, Guangzhou 510006, China (e-mail: kavinkang@gdut.edu.cn).

Xiaofeng Luo is with the School of Automation and the Guangdong-HongKong-Macao Joint Laboratory for Smart Discrete Manufacturing, Guangdong University of Technology, Guangzhou 510006, China (e-mail: gdutxiaofengluo@163.com).

Jiangtian Nie and Dusit Niyato are with the College of Computing and Data Science, Nanyang Technological University, Singapore 639798 (e-mail: jnie001@e.ntu.edu.sg; dniyato@ntu.edu.sg).

Tianhao Wu is with the School of Automation and the Key Laboratory of Intelligent Information Processing and System Integration of IoT, Ministry of Education, Guangdong University of Technology, Guangzhou 510006, China (e-mail: wutianhao32@163.com).

Haibo Zhou is with the School of Electronic Science and Engineering, Nanjing University, Nanjing 210093, China (e-mail: haibozhou@nju.edu.cn).

Yonghua Wang is with the School of Automation and the Key Laboratory of Intelligent Detection and IoT in Manufacturing, Ministry of Education, Guangdong University of Technology, Guangzhou 510006, China (e-mail: wangyonghua@gdut.edu.cn).

Shiwen Mao is with the Department of Electrical and Computer Engineering, Auburn University, Auburn, AL 36849 USA (e-mail: smao@ieee.org).

Shengli Xie is with the School of Automation and the 111 Center for Intelligent Batch Manufacturing Based on IoT Technology, Guangdong University of Technology, Guangzhou 510006, China (e-mail: shlxie@gdut.edu.cn).

References

[1] Y. Wang et al., "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 319–352, 1st Quart., 2022.

[2] W. Xu, Z. Yang, D. W. K. Ng, M. Levorato, Y. C. Eldar, and M. Debbah, "Edge learning for B5G networks with distributed signal processing: Semantic communication, edge computing, and wireless sensing," *IEEE J. Sel. Topics Signal Process.*, vol. 17, no. 1, pp. 9–39, Jan. 2023.

[3] L. Liu, J. Feng, C. Wu, C. Chen, and Q. Pei, "Reputation management for consensus mechanism in vehicular edge metaverse," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 4, pp. 919–932, Apr. 2024.

[4] J. Zhang et al., "Learning-based incentive mechanism for task freshness-aware vehicular twin migration," in *Proc. IEEE 43rd Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW)*, 2023, pp. 103–108.

[5] X. Luo et al., "Privacy attacks and defenses for digital twin migrations in vehicular metaverses," *IEEE Netw.*, vol. 37, no. 6, pp. 82–91, Nov. 2023.

[6] Z. Durante et al., "Agent AI: Surveying the horizons of multimodal interaction," 2024, *arXiv:2401.03568*.

[7] C. Cui et al., "A survey on multimodal large language models for autonomous driving," in *Proc. IEEE/CVF Winter Conf. Appl. Comput. Vis.*, 2024, pp. 958–979.

[8] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, 1st Quart., 2015.

[9] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-preserved pseudonym scheme for Fog computing supported Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 8, pp. 2627–2637, Aug. 2018.

[10] Y. Wang, Z. Su, S. Guo, M. Dai, T. H. Luan, and Y. Liu, "A survey on digital twins: Architecture, enabling technologies, security and privacy, and future prospects," *IEEE Internet Things J.*, vol. 10, no. 17, pp. 14965–14987, Sep. 2023.

[11] J. Xu, C. He, and T. H. Luan, "Efficient authentication for vehicular digital twin communications," in *Proc. IEEE 94th Veh. Technol. Conf. (VTC2021-Fall)*, 2021, pp. 1–5.

[12] H. Fang, X. Wang, N. Zhao, and N. Al-Dhahir, "Lightweight continuous authentication via intelligently arranged pseudo-random access in 5G-and-beyond," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 4011–4023, Jun. 2021.

[13] S. Khan et al., "A privacy-preserving and transparent identity management scheme for vehicular social networking," *IEEE Trans. Veh. Technol.*, vol. 71, no. 11, pp. 11555–11570, Nov. 2022.

[14] G. Cheng et al., "Conditional privacy-preserving multi-domain authentication and pseudonym management for 6G-enabled IoV," *IEEE Trans. Inf. Forensics Security*, early access, Sep. 11, 2023, doi: 10.1109/TIFS.2023.3314211.

[15] H. Huang, W. Kong, S. Zhou, Z. Zheng, and S. Guo, "A survey of state-of-the-art on blockchains: Theories, modelings, and tools," *ACM Comput. Surveys*, vol. 54, no. 2, pp. 1–42, 2021.

[16] J. Kang et al., "Blockchain-empowered federated learning for healthcare metaverses: User-centric incentive mechanism with optimal data freshness," *IEEE Trans. Cogn. Commun. Netw.*, vol. 10, no. 1, pp. 348–362, Feb. 2024.

[17] T. Li et al., "Metaopera: A cross-metaverse interoperability protocol," *IEEE Wireless Commun.*, vol. 30, no. 5, pp. 136–143, Oct. 2023.
[18] B. Liu, W. Zhou, T. Zhu, L. Gao, and Y. Xiang, "Location privacy and its applications: A systematic study," *IEEE Access*, vol. 6, pp. 17606–17624, 2018.
[19] Z. Liu, L. Zhang, W. Ni, and I. B. Collings, "Uncoordinated pseudonym changes for privacy preserving in distributed networks," *IEEE Trans. Mobile Comput.*, vol. 19, no. 6, pp. 1465–1477, Jun. 2020.
[20] H. Artail and N. Abbani, "A pseudonym management system to achieve anonymity in vehicular ad hoc networks," *IEEE Trans. Depend. Secure Comput.*, vol. 13, no. 1, pp. 106–119, Feb. 2016.
[21] B. Chaudhary and K. Singh, "Pseudonym generation using genetic algorithm in vehicular ad hoc networks," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 4, pp. 661–677, 2019.
[22] J. Li, H. Lu, and M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 938–948, Apr. 2015.
[23] J. Kang et al., "Adversarial attacks and defenses for semantic communication in vehicular metaverses," *IEEE Wireless Commun.*, vol. 30, no. 4, pp. 48–55, Aug. 2023.
[24] P. Li et al., "Filling the missing: Exploring generative AI for enhanced federated learning over heterogeneous mobile edge devices," *IEEE Trans. Mobile Comput.*, early access, Feb. 29, 2024, doi: 10.1109/TMC.2024.3371772.
[25] J. Du et al., "Resource pricing and allocation in MEC enabled blockchain systems: An A3C deep reinforcement learning approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 1, pp. 33–44, Feb. 2022.
[26] D. Boneh and X. Boyen, "Short signatures without random oracles," in *Proc. Int. Conf. Theory Appl. Cryptogr. Techn.*, 2004, pp. 56–73.
[27] J. Liang, Z. Qin, S. Xiao, L. Ou, and X. Lin, "Efficient and secure decision tree classification for cloud-assisted online diagnosis services," *IEEE Trans. Depend. Secure Comput.*, vol. 18, no. 4, pp. 1632–1644, Aug. 2021.
[28] S. Kaul, R. Yates, and M. Gruteser, "Real-time status: How often should one update?" in *Proc. IEEE INFOCOM*, 2012, pp. 2731–2735.
[29] A. Kosta, N. Pappas, A. Ephremides, and V. Angelakis, "Age and value of information: Non-linear age case," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2017, pp. 326–330.
[30] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "On non-cooperative location privacy: A game-theoretic analysis," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, 2009, pp. 324–337.
[31] T. Zhang, C. Xu, B. Zhang, X. Li, X. Kuang, and L. A. Grieco, "Towards attack-resistant service function chain migration: A model-based adaptive proximal policy optimization approach," *IEEE Trans. Depend. Secure Comput.*, vol. 20, no. 6, pp. 4913–4927, Dec. 2023.
[32] T. Zhang, C. Xu, J. Shen, X. Kuang, and L. A. Grieco, "How to disturb network reconnaissance: A moving target defense approach based on deep reinforcement learning," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 5735–5748, 2023.
[33] J. Chen et al., "Multiagent deep reinforcement learning for dynamic avatar migration in AIoT-enabled vehicular metaverses with trajectory prediction," *IEEE Internet Things J.*, vol. 11, no. 1, pp. 70–83, Jan. 2024.
[34] J. Du et al., "MADDPG-based joint service placement and task offloading in MEC empowered air–ground integrated networks," *IEEE Internet Things J.*, vol. 11, no. 6, pp. 10600–10615, Mar. 2024.
[35] J. Foerster, G. Farquhar, T. Afouras, N. Nardelli, and S. Whiteson, "Counterfactual multi-agent policy gradients," in *Proc. AAAI Conf. Artif. Intell.*, 2018, pp. 2974–2982.
[36] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, "A scalable multi-layer PBFT consensus for blockchain," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 5, pp. 1146–1160, May 2021.
[37] C. Feng, Z. Xu, X. Zhu, P. V. Klaine, and L. Zhang, "Wireless distributed consensus in vehicle to vehicle networks for autonomous driving," *IEEE Trans. Veh. Technol.*, vol. 72, no. 6, pp. 8061–8073, Jun. 2023.

Jiawen Kang (Senior Member, IEEE) received the Ph.D. degree from Guangdong University of Technology, Guangzhou, China, in 2018.

He was a Postdoctoral Fellow with Nanyang Technological University, Singapore, from 2018 to 2021. He is currently a Professor with Guangdong University of Technology. His research interests mainly focus on blockchain, security, and privacy protection in wireless communications and networking.

Xiaofeng Luo received the B.Eng. degree from Guangdong University of Technology, Guangzhou, China, in 2023, where he is currently pursuing the M.S. degree with the School of Automation.

His research interests include privacy protection, edge intelligence, and metaverse.

Jiangtian Nie (Member, IEEE) received the B.Eng. degree (with Hons.) in electronics and information engineering from Huazhong University of Science and Technology, Wuhan, China, in 2016, and the Ph.D. degree from ERI@N, Interdisciplinary Graduate School, Nanyang Technological University (NTU), Singapore, in 2021.

She was a visiting student with Princeton University, Princeton, NJ, USA, and the University of Waterloo, Waterloo, ON, Canada. She is currently with NTU. Her research interests include network economics, game theory, wireless blockchain, and crowd sensing and learning.

Tianhao Wu received the B.Eng. degree from Southwest Petroleum University, Chengdu, China, in 2022. He is currently pursuing the M.S. degree with the School of Automation, Guangdong University of Technology, Guangzhou, China.

His research interests include blockchain and metaverse.

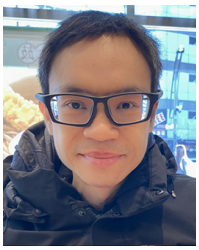
Haibo Zhou (Senior Member, IEEE) received the Ph.D. degree from Shanghai Jiao Tong University, Shanghai, China, in 2014.

He is currently a Full Professor with the School of Electronic Science and Engineering, Nanjing University, Nanjing, China. His research interests include resource management and protocol design in B5G/6G networks, vehicular ad hoc networks, and space–air–ground integrated networks.

Prof. Zhou was a recipient of the 2019 IEEE Com Soc Asia–Pacific Outstanding Young Researcher Award, the 2023–2024 IEEE Com Soc Distinguished Lecturer, and the 2023–2025 IEEE VTS Distinguished Lecturer.

Yonghua Wang (Senior Member, IEEE) received the B.S. degree in electrical engineering and automation from Hebei University of Technology, Tianjin, China, in 2001, the M.S. degree in control theory and control engineering from Guangdong University of Technology, Guangzhou, China, in 2006, and the Ph.D. degree in communication and information system from Sun Yat-sen University, Guangzhou, China, in 2009.

He is currently an Associate Professor with the School of Automation, Guangdong University of Technology. His current research interests include machine learning, intelligent control, and cognitive radio networks.



Dusit Niyato (Fellow, IEEE) received the B.Eng. degree from King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand, in 1999, and the Ph.D. degree in electrical and computer engineering from the University of Manitoba, Winnipeg, MB, Canada, in 2008.

He is a Professor with the College of Computing and Data Science, Nanyang Technological University, Singapore. His research interests are in the areas of sustainability, edge intelligence, decentralized machine learning, and incentive mechanism design.

Shiwen Mao (Fellow, IEEE) received the Ph.D. degree in electrical and computer engineering from Polytechnic University, Brooklyn, NY, USA, in 2004.

He is a Professor, an Earle C. Williams Eminent Scholar Chair, and the Director of the Wireless Engineering Research and Education Center, Auburn University, Auburn, AL, USA. His research interests include wireless networks, multimedia communications, and smart grid.

Prof. Mao was the recipient of the IEEE ComSoc TC-CSR Distinguished Technical Achievement Award in 2019, the NSF CAREER Award in 2010, the IEEE Vehicular Technology Society 2020 Jack Neubauer Memorial Award, and the 2004 IEEE Communications Society Leonard G. Abraham Prize in the Field of Communications Systems.

Shengli Xie (Fellow, IEEE) received the B.S. degree in mathematics from Jilin University, Changchun, China, in 1983, the M.S. degree in mathematics from Central China Normal University, Wuhan, China, in 1995, and the Ph.D. degree in control theory and applications from South China University of Technology, Guangzhou, China, in 1997.

He is currently a Full Professor and the Head of the Institute of Intelligent Information Processing, Guangdong University of Technology, Guangzhou. He has coauthored two books and more than 150 research papers in refereed journals and conference proceedings. His research interests include blind signal processing, machine learning, and the Internet of Things.

Prof. Xie was awarded the Highly Cited Researcher in 2020. He was awarded the Second Prize of National Natural Science Award of China in 2009. He is an Associate Editor for IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS. He is a Foreign Full Member (Academician) of the Russian Academy of Engineering.