applied sciences

MDPI

Article

Secure Application of MIoT: Privacy-Preserving Solution for Online English Education Platforms

Jiming Yin [1,†] and Jie Cui [2,*,†]

[1] School of Foreign Studies, Anhui Jianzhu University, Hefei 230601, China; 080058@ahjzu.edu.cn
[2] School of Computer Science and Technology, Anhui University, Hefei 230039, China
* Correspondence: cuijie@mail.ustc.edu.cn; Tel.: +86-055163861263
† These authors contributed equally to this work.

Abstract: With the increasing demand for higher-quality services, online English education platforms have gained significant attention. However, practical application of the Mobile Internet of Things (MIoT) still faces various challenges, including communication security, availability, scalability, etc. These challenges directly impact the utilization of online English education platforms. The dynamic and evolving nature of the topology characteristics in Mobile Internet of Things networks adds complexity to addressing these issues. To overcome these challenges, we propose a software-defined MIoT model that effectively handles the dynamic and evolving network topology features, thereby enhancing the system's flexibility and adaptability. Additionally, our model can provide communication security and privacy protection, particularly in emergency situations. In our scheme, the control plane is responsible for computing routes for online learning devices (OLDs) and forward entries for switches. By utilizing the information collected from OLDs and facilities, the controller is able to effectively coordinate the overall system. To ensure the authenticity and reliability of messages sent by OLDs, we have proposed a new signature and authentication mechanism based on traditional encryption algorithms. Moreover, we introduce an emergency-handling system that integrates multicast technology into software-defined MIoT, generating a Steiner Tree among impacted nodes to promptly notify OLDs when there is an emergency. The security analysis proves that our scheme is able to ensure communication security in software-defined MIoT. A performance evaluation indicates that our scheme outperforms other existing schemes.

Keywords: MIoT; software-defined MIoT; security; signature; authentication; multicast; online English education

check for updates

Citation: Yin, J.; Cui, J. Secure Application of MIoT: Privacy-Preserving Solution for Online English Education Platforms. *Appl. Sci.* **2023**, *13*, 8293. https://doi.org/10.3390/app13148293

Academic Editors: Lip Yee Por and Abdullah Ayub Khan

Received: 13 June 2023
Revised: 14 July 2023
Accepted: 14 July 2023
Published: 18 July 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The Internet of Things (IoT) has drawn attention from both industry and academic fields for years due to its advantages, such as efficiency and providing more secure communication environments. Among the various applications of IoT, online education has emerged as a significant application of Mobile IoT (MIoT). IoT provides the necessary technological support and infrastructure for online education to be conducted on mobile devices and over the Internet. English, being a globally universal language, is widely learned and considered a core subject in schools across most countries. Consequently, the application of MIoT in online English education has rapidly become an important method and primary tool for individual learning and communication. This is a novel education model that puts students at the center and relies on software platforms to deliver personalized learning experiences [1,2]. Compared to traditional offline classroom education, online English education offers advantages such as higher efficiency [3,4] and freedom from geographical constraints [5]. Here, online learning devices (OLDs) have the capability to communicate with other devices and infrastructure, such as roadside units in certain models, enabling

access to the MIoT [6]. Thus, OLDs are allowed to report information and emergencies, which will be used to improve the quality of services [7,8]. However, if OLDs are allowed to broadcast messages without any verification or limitation, the communication mechanism will become vulnerable and easy to compromise [9–11]. For example, if messages sent in MIoT are not signed with an online learning device's unique identities, then a malicious user can broadcast fraud messages or sign them with fabricated identities to bypass a weak system. To solve problems in secure communication, some studies have been dedicated to designing privacy-preserving authentication schemes [12–14]. However, due to the feature of changing topology, it is hard to balance efficiency and security in conventional MIoT. Then, a brand-new technology came into researchers' sights.

Software-defined network (SDN) is an innovative technology that embodies a network structure distinct from traditional networks [15,16]. In SDN, controlling and forwarding are separated and work in different layers [17,18]. The control plane represents the centralized point as the brain of the whole architecture [19]. The data plane communicates with the control plane via southbound interfaces. It is mainly responsible for querying controllers for forwarding tables and forward packets. Using the programmability and scalability, the combination of VANETs and SDN offers a new approach to solve inherent problems in VANETs.

Software-defined MIoT has been proposed for years and there have been many research efforts demonstrating the advantages of this new combination [20,21]. Meanwhile, some schemes are proposed to cope with problems in quality of services (QoS) [22], heterogeneous network accessing [23], factory managing [24,25] and so many others in different fields by combining with SDN [26]. Inspired by [27], we design a scheme that uses multicast technology to solve the driving direction and secure communication problems in software-defined MIoT.

In traditional MIoT, OLDs mainly rely on broadcasting each other to receive network condition information, which lacks timeliness and overall planning [28–30]. By introducing multicast, the controller is allowed to manage OLDs and balance network throughputs more efficiently. In addition, some technology used not to be suitable for MIoT, like Steiner Tree, which is computation intense and scale sensitive [27]. But with SDN introduced, those algorithms can provide new methods for the development of MIoT [31,32].

Thus, we propose a new secure communicating and device movement path scheme in this paper. By using multicast [33] and privacy-preserving authentication technologies, we aim to design a secure and efficient model in software-defined MIoT. Concretely, the primary contributions of this paper can be outlined as follows.

Our Contribution

This work provides the following key contributions.

(1) We propose a novel software-defined MIoT-based model that provides security communication in the underlying data plane. The outstanding computing power of the control plane greatly relieves the overhead of the upper layer, which offers users higher-quality services.
(2) We design an authentication system to ensure the authenticity and reliability of messages, so that OLDs are encouraged to spread real information. Otherwise, they will be punished. In addition, an emergency-dealing scheme is offered to provide in-time services based on multicast, which not only takes current network situations into consideration, but also predictions of instantaneous changing.
(3) A security analysis demonstrates that the proposed scheme is capable of achieving the security objectives of software-defined MIoT. In addition, adopting elliptic curve cryptography avoids heavy overhead brought by bilinear pairing operations, which is demonstrated by the comparison results.

The structure of the remaining sections in this paper is as follows. Section 2 provides an overview of related works. Section 3 presents the system models and outlines our design objectives. In Section 4, we provide a comprehensive and elaborate explanation of the

proposed scheme. The security analysis is presented in Section 5, followed by a comparison of computation overhead in Section 6. Finally, Section 7 concludes the paper.

2. Related Works

Online education has a significant impact on the learning process by leveraging the IoT, cloud computing and big data. The key to integrating online educational resources lies in the storage of massive teaching data. Wei et al. [34] applied cloud storage technologies and methods to the construction of integrated online educational resources, which effectively saves educational resources for schools, enhances the utilization of online educational resources and thereby improves the teaching quality of subjects. Hui Tao [35] proposed an online English teaching system approach based on IoT technology. The author studied the English SPOC (Small Private Online Course) teaching mode, constructed a multimedia teaching system based on IoT technology, improved the teaching system and enhanced and learned the teaching mode, resulting in an improvement in the quality of English teaching.

Chen et al. [36] developed an IoT-oriented online English education platform with the aim of providing a conducive learning environment and enhancing students' overall English proficiency. To improve the ability to find optimal solutions, they incorporated a reverse learning (RL) mechanism into the grey wolf optimization (GWO) algorithm, resulting in the development of the RLGWO algorithm. They further constructed the RLGWO-BP model, which was utilized to assess the impact of the IoT-oriented online education platform on English language instruction. Gao et al. [37] utilized preliminary results obtained through the use of IoT to establish an interactive educational paradigm. They deployed numerous sensors with the aim of improving learners' English language correction by comparing learners' wording and speech with the software's standard wording and speech.

In the security in MIoT and the software-defined MIoT research field, a threshold anonymous authentication protocol using group signature technology was proposed by Shao et al. [9]. In this scheme, the decentralized group model is integrated. It achieved threshold authentication, anonymity, unforgeability, tracability and revocation of MIoT communication. However, the huge computation cost of bilinear pairing may create obstacles to implementation. Azees et al. [38] proposed a scheme that enabled roadside units to authenticate vehicles anonymously before providing certain messages to them. It also allowed vehicles to communicate with roadside units anonymously. The scheme reduced costs of certificate and signature verification and achieved privacy preserving and traceability in vehicular ad hoc networks. However, there were no timestamps attached to messages, which could be used by malicious parities to start replay attacks.

To solve the problems of insecurity of master keys, invalidity of PIDs in [12], and to cope with inherent problems in MIoT, Li et al. [39] proposed a certificate-less protocol and demonstrated the security of it. Xiang et al. [40] proposed a novel CLS (certificate-less signcryption) scheme to address critical issues such as data integrity and identity authentication in the IoT environment. The scheme eliminates the cumbersome certificate management in certificate-based signature systems and the key escrow problem in identity-based cryptography. Furthermore, it is designed to securely resist various attacks, such as public key-replacement attacks or malicious but passive key-generation center attacks. Garg et al. [31] proposed secure communication models by introducing SDN architecture. They enabled both mutual authentication among communicating entities and intrusion-detecting systems to detect potential attacks from the underling networks.

Hong et al. [41] proposed a time-limited secure attribute-based online/offline signature scheme (TS-ABOS-CMS) with a constant message length. The scheme achieves high efficiency by introducing online/offline signature methods while maintaining communication overhead at a constant level. Additionally, a key update mechanism is adopted to provide time-limited security protection for IoT terminals. Khashan et al. [42] proposed a blockchain-based hybrid centralized IoT system authentication architecture. Edge servers are deployed to provide centralized authentication for associated IoT devices. Subsequently, a blockchain network is established for the centralized edge servers to ensure decentralized

authentication and verification of IoT devices belonging to different and heterogeneous IoT systems. Wang et al. [43] adopted the low-energy distributed ledger technology IOTA to design a lightweight and scalable mechanism for managing the identity of IoT devices and access control of large-scale IoT data. This mechanism ensures the reliability of the source of IoT data and the security of data sharing.

In the multicast in the SDN research field, Zhou et al. [27] proposed the cost-efficient Degree-dependent Branch-node Weighted Steiner Tree (DBWST) problem in the SDN architecture. It solved the scalability problem of multicast by introducing Steiner Tree to span nodes. The scheme reduced the total cost and the number of branch nodes when generating the multicast tree T. Do et al. [26] proposed an architecture that allowed both multicast and broadcast services in the SDN-based mobile packet core. It had the advantages of programmability and flexibility of SDN and reduced the signaling cost compared with traditional network paradigms. However, the system may suffer certain security problems in terms of communication.

Lai et al. [44] proposed an integrated network architecture for secure group communication in SDN-based 5G vehicular ad hoc networks. The scheme was a group-oriented vehicular environment, in which vehicles are divided into groups based on their geographic positions. This also inspired us to manage vehicles by dividing them in a transaction-oriented way. Kim et al. [24] proposed a multicast scheme with Group Shared Tree (GST) switching in large-scale IIoT networks. To overcome inherent problems, such as transmitting multicast packets under congestions and configuring optimal paths dynamically, it adopted SDN-based architecture. They proved that the new architecture outperformed other models.

3. Models and Design Goals

3.1. System Model and Assumptions

According to [13], the layered control plane is thought to be more realistic in practical applications. Based on that, our system is composed of the following: the Global Controller (GC), many Local Controllers (LCs), many OpenFlow Switches (OF-Switches), Base Stations (BSs), Access Points (APs) and online learning devices (OLDs). GC and LCs are responsible for dealing with collected information and making optimal decisions. The others make up the data plane, which is mainly for transport packages and collecting road information. Figure 1 depicts the system model.

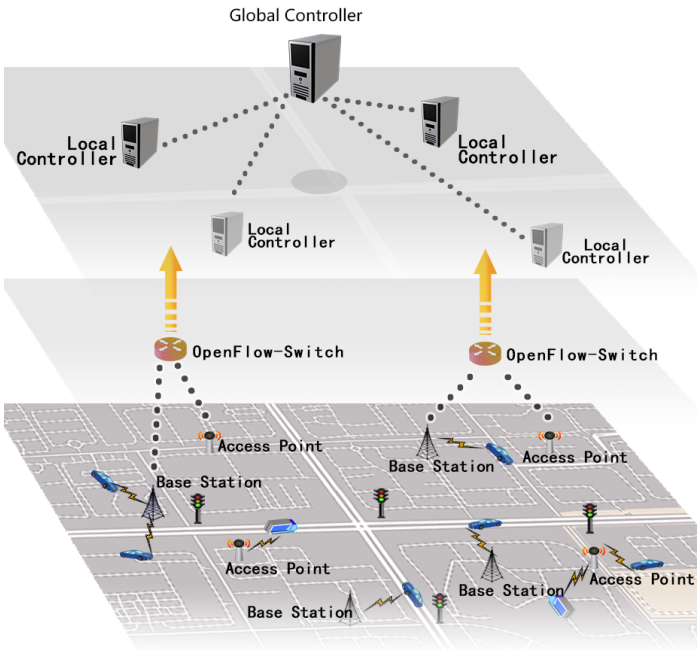


Figure 1. The system model.

(1) **GC:** This is the main controller of the control plane. In traditional SDN systems, the controller is a logically centralized point that has extremely outstanding storage and computing capabilities. Typically, it directs switches to deliver and forward packages by building routing rules. In our system, the GC assumes the primary responsibility of generating system parameters, calculating the device's movement path and constructing route tables for OF-Switches. When there are accidents or emergencies happening, it also selects impacted devices and forms a temporary multicast group. It generates a multicast tree for this group to inform them of conditions in time.

(2) **LCs:** These are distributed geographically and manage a specific small area. In our system, the LCs primarily serve the purpose of distributing the computation and storage loads of the GC. They can reduce realistic deployment costs as well. LCs set system parameters and communicate with OLDs. They can verify messages in their local areas and compute fine-grained navigation for OLDs. When there are road situations, they are also composed of multicast nodes to inform and direct OLDs in their areas.

(3) **OF-Switches:** Different from conventional switches, OF-Switches are OpenFlow-enabled data switches that communicate with external controllers over the OpenFlow channel. The OpenFlow protocol offers separation of programming network devices and underlying hardware [44]. In our system, OF-Switches perform package lookup and forwarding according to flow tables installed on them.

(4) **OLDs:** OLDs offer network access services via wireless communication capabilities, which have limited computing power and storage [45]. Also, tamper-proof equipment is embedded in each OLD that is robust and responsible for generating key cryptographical parameters and performing many encryption and decryption operations [46].

(5) **BSs and APs:** OLDs obtain access to the Internet via various ways. Cellular networks like 5G network via BSs and city WiFi via APs are both supported by our system. For software-defined MIoT, to balance heterogeneous networks and allow OLDs in different networks to communicate is much easier compared with conventional networks.

* The GC is absolutely trusted and will not suffer any compromise. It has ample computing power and storage space.
* LCs are trustworthy, but in cases in which they are compromised, we do not provide them capabilities of trace OLDs' real identities. LCs have sufficient computing and storage space.
* The parameters and data stored in OLDs are not available for others.

3.2. Multicast Subsystem

When an emergency occurs, impacted OLDs may request new movement paths rather than remaining stuck. Commonly, the conventional systems only replan new paths based on the present road conditions but do not take dynamically instantaneous changing into consideration. We design a multicast mechanism-based emergency system, which uses Stein Tree to compute a multicast tree between those nodes to inform affected OLDs in time.

3.2.1. Steiner Tree

In general, to connect n nodes, the Minimum Spanning Tree (MST) is the most commonly selected algorithm. But in networks, there are lots of factors that need to be taken into consideration, such as bandwidth, transport delay of networks and so on. Hence, Steiner Tree, a spanning tree algorithm with weights, is more suitable. The generation of Steiner Tree is thought to be computation intensive, so there are few applications in conventional multicast schemes. But as for SDN controller, it becomes feasible since the forwarding information is preloaded in network switches. In addition, the global visibility and programmability can also help to construct a better multicast tree more efficiently [21].

3.2.2. Multicast Tree

In our scheme, we take the Degree-dependent Branch-node Weighted Steiner Tree (DBWST) proposed in [21] to construct our multicast tree. Algorithm 1 describes the specific procedure. Based on the DBWST, consider an undirected graph $G_v = \{V, L\}$, in which V denotes OLDs and other entities taking part in communication in software-defined MIoT, and L represents a collection of links. For example, the link $l = (v, w) \in L$ denotes the link from $v \in V$ and $w \in V$. Then the cost of link l is $Cst(l) : L \mapsto R^+$, where R^+ is nonnegative. Let s be the source of a multicast and $U \subset V - \{s\}$ be the set of destination nodes, which in our system is the affected OLDs. The size of this group corresponds to the quantity of $|R|$. Let $T = (s, U)$ denote the multicast tree whose source is s and spanning all nodes $OLD_i \in U, 1 < i < |U|$. According to the definition of branch node in Steiner Tree, if the degree of node OLD_i is no less than three, then OLD_i would be one. Let π_u represent that u is a branch node in T. Based on the above description, finally the cost of the tree T can be denoted as:

$$Cst(T) = \sum_{l \in T} Cst(e) + \sum_{u \in T} \pi_u \cdot Cst(u) \tag{1}$$

Based on the DBWST, it is computationally uncomplicated to find a tree $T = (s, U)$ which makes the $Cst(T)$ lowest. The constructed multicast tree can not only help to distribute messages more efficiently, but can also be applied to other fields, such as video conferences and streaming media subscribing.

Algorithm 1 Directing Process

Input: input departure, Dp; destination,Ds
Output: reach $Ds = 1$

1: OLD_i request path
2: control plane return path $C = \{LC_k\}^*$,$0 < k < n$
3: $LC_k : ST = ST + \{OLD_i\}$
4: **while** $C! = \emptyset$ **do**
5: OLD_i leaves LC_k
6: // OLD_i does:
7: $C = C - \{LC_k\}, 1 < k \leq n$
8: // LC_k does
9: $ST = ST - OLD_i, 0 \leq |ST| \leq n$
10: **if** LC_k unreachable = true **then**
11: $T = DBWST(d, n)$
12: // d represents the total number of affected OLDs
13: // $0 < d \leq m$
14: jump tp line 1
15: **end while**

3.2.3. Application Process

With the multicast tree having been constructed, the process can be described as follows. When an OLD starts driving, firstly it will request a path to the controller. Commonly, it tends to store all the forwarding entries in the control plane to program the routing process. However, given m OLDs and n LCs, the worst condition is that the spatial complexity will reach $O(n^m)$. Even the lowest will reach $O(n^2)$. So, we propose to only maintain a subscriber table in each LC. For example, an OLD_i gained a path passing through x consecutive LCs. Let C denote the set of x LCs, $|C| = x$. Then each LC will add OLD_i into its subscriber table ST. Every time OLD_i leaves an area, it will send a leaving packet to the control plane. After that, OLD_i and LCs will perform $C = C - \{LC_k\}$,$1 < k \leq n$ and $ST = ST - \{OLD_i\}, 0 \leq |ST| \leq m$, respectively. This step is designed to prevent OLDs that have passed through the area from being rearranged. By only maintaining subscriber

tables, the spatial complexity can be decreased to $O(m^n)$, where $n \ll m$. The process of subscribing is shown in Figure 2.

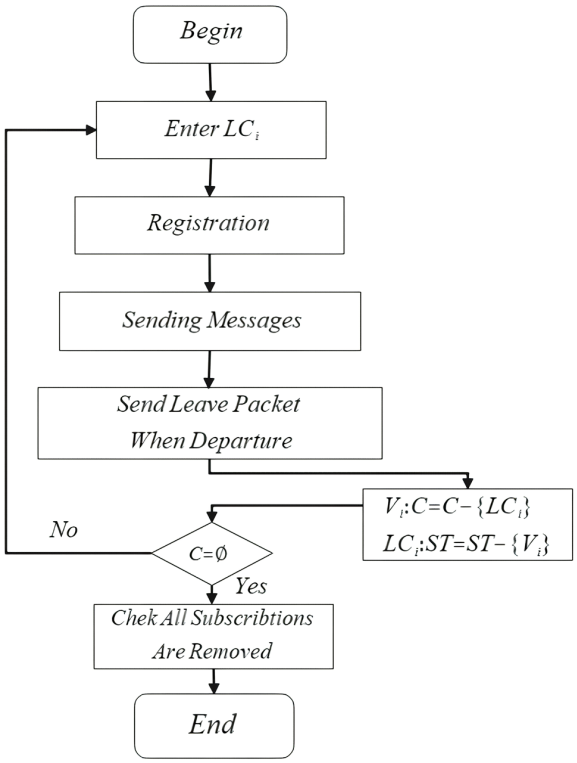


Figure 2. The process of subscribing.

3.3. Design Goals

Our objective is to create an efficient system to offer OLDs a secure environment to communicate and services such as avoiding risks. It will satisfy the following desirable properties. *Routing Plan*: Making use of the global ability, the control plane will generate the most suitable using plan for OLDs. *Emergency Handling*: When an emergency occurs, to avoid a second occurrence, the control system informs the impacted OLDs promptly via its multicast mechanism. Then it replans new routes for OLDs by balancing all network situations. *Secure Communication*: The most important factor is that all the messages sent by OLDs need to be trustworthy and factual. Considering that, the system should have the following security properties.

(1) Anonymity: OLDs in our system will not communicate with other entities with real identities. Based solely on the messages sent by OLDs and some public information, malicious users cannot ascertain the real identity of the sender. This way, OLDs are allowed to send messages without exposing sensitive privacy information.
(2) Authentication and Privacy: Each interactive party in our system can authenticate the others to ensure reliability and legitimacy. In particular, in different areas, messages sent by OLDs should reflect the present LC's information without exposing them to adversaries, which ensures location privacy would not be compromised.
(3) Traceability: We will not exclude the possibility of the existence of malicious entities. They aim to interrupt or interfere normal communications or spread false and deceptive messages to gain convenience and benefits for themselves. When misbehavior occurs, the controller plane should be able to trace the real identities and punish them by cutting services or submitting their information to related authorities.
(4) Unlinkability: The proposed scheme would not enable third parties to link scattered messages to the same OLDs. That is to say, no third party could know one specific OLD's activities by analysing those intercepted messages.

(5) Resistance to common attacks: The scheme must have the ability to effectively counter prevalent attacks that occur in conventional networks, including replay attacks, impersonation attacks, modification attacks and others.

4. Proposed Scheme

Here, we propose our secure communication scheme in software-defined MIoT. In our scheme, firstly messages should be signed and then distributed to ensure non-repudiation. Then, to prevent the privacy information of vehicles from being exposed, OLDs should communicate via pseudo identities, which include a rough location of their current LC area. All above information can only be derived via GC but not other third parties. When emergencies occur, GC will extract OLDs' locations from messages they sent. When malicious messages are found, GC will extract OLDs' real identities from those messages and take actions to punish them.

4.1. Control Plane Initialization

The scheme utilizes F_p as the finite field over a large prime number p, with p denoting the field's size. The parameters $(a, b) \in F_p$ define the elliptic curve $E : y^2 = x^3 + ax + b \ mod \ p$. A group G is generated from E in the system, where P serves as the generator and q represents the prime order of E. Table 1 presents additional notations and definitions employed in the scheme.

Table 1. Notations and definitions.

Notations	Definitions
GC	The Global Controller
LC_i	Local Controller i
OLD_i	The i-th online learning device
G	An additive cyclic group
P, q	The generator and order of G
p	The size of a field
P_{pub}, s	A public and private key of GC
NLC_i	The number of NLC_i
ID_i	The identity of OLD_i
PID_i	The pseudo identity of OLD_i
PK_i, sk_i	A public and private key of OLD_i
M	A message
msg	An encapsulated message
σ	The signature of a message
T_t	The time stamp

(1) **GC Initialization:** By randomly selecting the master key s from Z_q, the GC derives its public key as $P_{pub} = s \cdot P$ and computes $\alpha = s \cdot h(P_{pub})$. Subsequently, the GC chooses the hash function $h : G \rightarrow Z_q^*$, $H0 : G \times \{0,1\}^* \rightarrow Z_q^*$, $H1$: $\{0,1\}^* \rightarrow Z_q^*$, $H2 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times G \times G \rightarrow Z_q^*$. The value of α is transmitted to LCs, while $\{P_{pub}, p, q, a, b, P, H0, H1, H2\}$ is published as the system parameters. In order to ensure the overall security of the system, the GC must keep the hash function h confidential.

(2) **LC Initialization:** After receiving α via a secure channel in the control plane, LC_i computes $l_i = \alpha \cdot NLC_i$ as its secret key, where NLC_i is a unique number of each LC and a list of them is only stored in the GC. Since s is unknown to any third party and each NLC_i also stays secret, it is also difficult to compute l_i based on public parameters. Next, it calculates $L_i = l_i \cdot P$ to generate its public key, and adds L_i into the GC's system parameters. Finally, $\{P_{pub}, p, q, a, b, P, H0, H1, H2, L_i\}$ is the local system parameters of this specific area.

4.2. Online Learning Device Initialization

When an online learning device OLD_i enters into the area of LC_i and it is necessary to publish messages in the current environment, it loads parameters and randomly selects $sk_i \in Z_q$ as its private key and calculates $PK_i = sk_i \cdot P$ as the public key. Then $PID_{i,1} = ID_i \oplus H0(sk_i \cdot L_i \| T_t)$, $PID_{i,2} = (sk_i \cdot L_i) \oplus H1(T_t)$. It uses $PID_i = \{PID_{i,1}, PID_{i,2}\}$ as its pseudo name.

4.3. One-Time Key Generation and Message Signature

A message M_i could include status, emergency information or other related requests. When OLD_i tends to send message M_i, it will firstly select a number r_i randomly and compute $R_i = r \cdot P$. Let $w_i = H2(M_i \| PID_i \| T_t \| R_i \| PK_i)$, where T_t is the current timestamp. Then it signs M_i with $\sigma = sk_i + w_i \cdot r_i \ mod \ q$. Then, OLD_i will send encapsulated msg : $\{M_i, T_t, PK_i, R_i, PID_i\}$ to nearby communication-related entities.

4.4. Emergency Location Extraction

To ensure the basic location privacy of OLDs, the specific LC where it is located cannot be exposed in msg. Otherwise, by connecting and analysing several messages it has sent, it is feasible for malicious parties to draw rough activity areas of one OLD. But when an emergency occurs, the control plane needs to roughly locate affected OLDs. By fully balancing affected and unaffected areas' densities of OLDs, the control plane is able to construct a most efficient multicast tree with average lowest source consumption $Cst(T)$.

When there are abnormal conditions, OLDs around will broadcast a message msg to report. After receiving those msgs, the GC will perform the following computation to decide a rough location of LC.

$$\begin{aligned} PID_{i,2} &= (sk_i \cdot L_i) \oplus H1(T_t) \\ &= (sk_i \cdot \alpha \cdot NLC_i \cdot P) \oplus H1(T_t) \\ &= (PK_i \cdot \alpha \cdot NLC_i) \oplus H1(T_t) \\ &\Downarrow \\ NLC_i &= (PID_{i,2} \oplus H1(T_t)) \cdot (PK_i \cdot \alpha)^{-1} \end{aligned} \tag{2}$$

By locating the LC, the GC will handle this area's packets preferentially to deal with emergencies.

4.5. Message Authentication

To verify whether OLDs have sent false messages or packets have been modified, other entities can verify signatures of received messages. To enhance verification efficiency, the proposed scheme also provides the capability to simultaneously verify messages in a batch. The processes for verifying a single message and verifying messages in a batch are described below, respectively.

(1) **Single Verification**
After receiving a message $\{M_i, T_t, PK_i, R_i, PID_i\}$, to verify its validation, a receiver will perform the following steps in order with the system parameters $\{P_{pub}, p, q, a, b, P, H0, H1, H2, L_i\}$.

* Check if the timestamp T_t is fresh. If it is not, the received message is abandoned. If it is fresh, keep performing the operation.
* The receiver performs $\sigma \cdot P$ and $PK_i + w_i \cdot R_i$ and calculates whether they are equal. If they are not, the receiver chooses to abandon them. If they are equal, it admit the validation of this message.
  Since $P_{pub} = s \cdot P$, $w_i = H2(M_i \| PID_i \| T_t \| R_i \| PK_i)$, $R_i = r \cdot P$, $PK_i = sk_i \cdot P$ and $PID_i = \{PID_{i,1}, PID_{i,2}\}$, where $PID_{i,1} = ID_i \oplus H0(sk_i \cdot L_i \| T_t)$, $PID_{i,2} = (sk_i \cdot L_i) \oplus H1(T_t)$ and $\sigma = sk_i + w_i \cdot r_i \ mod \ q$, the following equations can be derived.

$$\begin{aligned} \sigma \cdot P &= (sk_i + w_i \cdot r_i) \cdot P \\ &= sk_i \cdot P + w_i \cdot r_i \cdot P \\ &= PK_i + w_i \cdot R_i \end{aligned} \tag{3}$$

(2) **Batch Verification**

Verifying each of the n messages individually consumes a significant amount of time and computing resources when a receiver receives a batch of messages within a short time interval. Therefore, our scheme incorporates batch verification to efficiently utilize resources. Firstly, to guarantee the non-repudiation of signatures using batch verification, we choose a vector comprising small random integers. Let the vector $\zeta = \{\zeta_1, \zeta_2, \zeta_3, ..., \zeta_n\}$, where $\zeta_i \in [1, 2^{\xi}]$ and ζ is a secure parameter. After receiving a message $\{M_1, T_{t,1}, PK_1, R_1, PID_1\}$, $\{M_2, T_{t,2}, PK_2, R_2, PID_2\}$, ..., $\{M_n, T_{t,n}, PK_n, R_n, PID_n\}$, to verify its validation, a receiver will perform the following steps in order with the system parameters $\{P_{pub}, p, q, a, b, P, H0, H1, H2, L_i\}$.

* Check if the timestamp $T_{t,1}, T_{t,2}, ..., T_{t,i}, ..., T_{t,n} (1 < i \leq n)$ are fresh. If they are not, the received message is abandoned. If they are fresh, keep performing the operation.
* The receiver performs (4) and calculates whether they are equal. If they are not equal, the receiver will find the malicious message via the invalid signature search algorithm and choose to abandon it. If they are equal, it admits the validation of this series of messages.

$$\begin{aligned} \sum_{i=1}^{n}(\zeta_i \cdot \sigma_i) \cdot P &= (\sum_{i=1}^{n} \zeta_i \cdot (sk_i + w_i \cdot r_i)) \cdot P \\ &= \sum_{i=1}^{n}(\zeta_i \cdot (sk_i \cdot P + w_i \cdot r_i \cdot P)) \\ &= \sum_{i=1}^{n}(\zeta_i \cdot PK_i + \zeta_i \cdot w_i \cdot R_i) \\ &= \sum_{i=1}^{n}(\zeta \cdot PK_i) + \sum_{i=1}^{n}(\zeta_i \cdot w_i \cdot R_i) \end{aligned} \tag{4}$$

By this, the validation of the batch verification of a series of message is proved. The interactions of the above parties are shown in Figure 3.

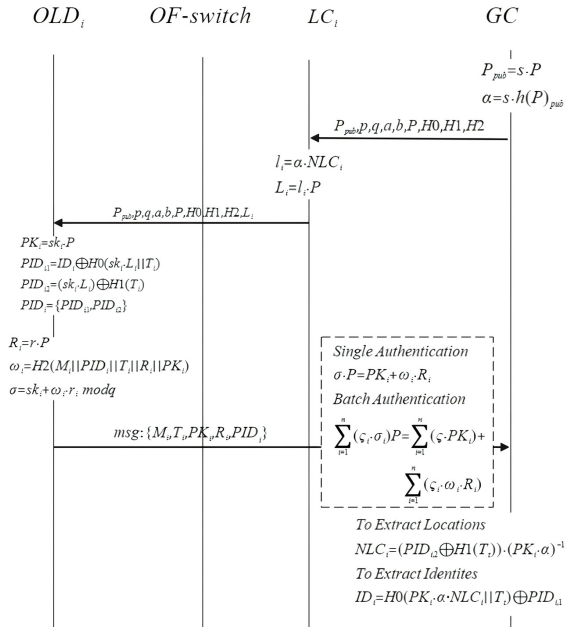


Figure 3. The interactions of parties.

5. Security Proof and Analysis

The communication security of the proposed scheme will be analyzed in this part. In Section 2, we presented some of our security goals and the threats that may be met. Here, firstly, we introduce the definition of the elliptic curve discrete logarithm problem (ECDLP) upon which the entire analysis is based.

Definition 1 (ECDLP). *Let P be the generator of group G, with $n \in Z_q$ and $N = nP \in G$. The ECDLP states that it is computationally infeasible to determine the value of n given $N = nP$. To establish the security model for the proposed scheme, a game is defined involving adversary $\mathcal{A}$ and challenger $\mathcal{C}$, leveraging the aforementioned network.*

5.1. Security Proof

In this game, the adversary $\mathcal{A}$ is allowed to execute the queries listed below.

- *Setup Oracle*: When $\mathcal{A}$ revokes the query, $\mathcal{C}$ sends the generated private key and the corresponding system parameters to $\mathcal{A}$.
- *H0 Oracle*: $\mathcal{C}$ randomly selects a point $d \in Z_q$ and includes $\{m, d\}$ in its list L_{H0}. Then it returns d to $\mathcal{A}$ when $\mathcal{A}$ revokes the query.
- *H1 Oracle*: $\mathcal{C}$ randomly selects a number $d \in Z_q$ and includes $\{m, d\}$ in its list L_{H1}. Then it returns d to $\mathcal{A}$ when $\mathcal{A}$ revokes the query.
- *H2 Oracle*: $\mathcal{C}$ randomly selects a point $d \in Z_q$ and includes $\{m, d\}$ in its list L_{H2}. Then it returns d to $\mathcal{A}$ when $\mathcal{A}$ revokes the query.
- *Sign Oracle*: Based on the M_i sent by $\mathcal{A}$, $\mathcal{C}$ computes a $msg : \{M_i, T_t, PK_i, R_i, PID_i\}$. Then $\mathcal{C}$ returns $\{M_i, T_t, PK_i, R_i, PID_i\}$ to $\mathcal{A}$ when $\mathcal{A}$ revokes the query.

If the adversary $\mathcal{A}$ has the ability to fabricate a legitimate login request message, it indicates a violation of the proposed secure communication scheme by $\mathcal{A}$. We define $\Phi(\mathcal{A})$ as the probability of $\mathcal{A}$ violating the scheme.

Definition 2. *For any polynomial adversary $\mathcal{A}$, our scheme is considered secure if the probability $\Phi(\mathcal{A})$ is negligible.*

By conducting a security evaluation of our scheme under the random oracle model, we establish the following theorem.

Theorem 1. *The proposed scheme exhibits security within the random oracle model.*

Proof. Suppose there is an adversary $\mathcal{A}$ who has the ability to forge a $msg : \{M_i, T_t, PK_i, R_i, PID_i\}$. Our signature scheme is executed by a challenger $\mathcal{C}$ that we construct. By performing the following queries revoked by $\mathcal{A}$, challenger $\mathcal{C}$ can leverage $\mathcal{A}$ as a subroutine to solve the ECDLP problem with a probability that is not negligible. □

Setup Oracle: First, a key parameter k is provided as input. Subsequently, $\mathcal{C}$ selects a random number s as its private key and calculates $P_{pub} = s \cdot P$. $\mathcal{C}$ then transmits $\{P_{pub}, p, q, a, b, P, H0, H1, H2\}$ to $\mathcal{A}$.

H0 Oracle: $\mathcal{C}$ maintains an initially empty list $L_{H0} : (sk_i, L_i, T_t, h_{0,i})$. When $\mathcal{A}$ makes a query with (sk_i, L_i, T_t), $\mathcal{C}$ verifies if $L_{H0} : (sk_i, L_i, T_t, h_{0,i})$ already exists in L_{H0}. If the entry exists, $\mathcal{C}$ provides the corresponding $h_{0,i}$. Otherwise, $\mathcal{C}$ generates a random $h_{0,i} = H0(sk_i \cdot L_i \| T_t)$, inserts $L_{H0} : (sk_i, L_i, T_t, h_{0,i})$ into the list and yields $h_{0,i}$ to $\mathcal{A}$.

H1 Oracle: $\mathcal{C}$ maintains an initially empty list $L_{H1} : (T_t, h_{1,i})$. When $\mathcal{A}$ makes a query with (T_t), $\mathcal{C}$ verifies if $L_{H1} : (T_t, h_{1,i})$ already exists in L_{H1}. If the entry exists, $\mathcal{C}$ provides the corresponding $h_{1,i}$. Otherwise, $\mathcal{C}$ generates a random $h_{1,i} = H1(T_t)$, inserts $L_{H1} : (T_t, h_{1,i})$ into the list and yields $h_{1,i}$ to $\mathcal{A}$.

H2 Oracle: $\mathcal{C}$ maintains an initially empty list $L_{H2} : (PID_i, L_i, T_t, R_i.PK_i, M_i, h_{2,i})$. When $\mathcal{A}$ makes a query with $(PID_i, L_i, T_t, R_i.PK_i, M_i)$, $\mathcal{C}$ verifies if $L_{H2} : (PID_i, L_i, T_t, R_i.PK_i, M_i)$ already exists in L_{H2}. If the entry exists, $\mathcal{C}$ provides the corresponding $h_{2,i}$. Otherwise, $\mathcal{C}$ generates

a random $h_{2,i} = H2(PID_i \| L_i \| T_t \| R_i \| PK_i \| M_i)$, inserts $L_{H2} : (PID_i, L_i, T_t, R_i.PK_i, M_i, h_{2,i})$ into the list and yields $h_{2,i}$ to $\mathcal{A}$.

Sign Oracle: When $\mathcal{A}$'s query with message M_i and pseudo identity PID_i is received, $\mathcal{C}$ checks if $(sk_i, L_i, T_t, h_{0,i})$ and $(T_t, h_{1,i})$ already exist in L_{H0} and L_{H1}, respectively. $\mathcal{C}$ gains $h_{0,i}$ from $(sk_i, L_i, T_t, h_{0,i})$ and $h_{1,i}$ from $(T_t, h_{1,i})$. Otherwise, $\mathcal{C}$ selects three random numbers $\sigma, w_i, PID_i \in Z_q$, where $PID_i = f1(h_{0,i}, h_{1,i})$, $\sigma = f2(w_i, PID_i)$. Then $\mathcal{C}$ sends $\{M_i, T_t, PK_i, R_i, PID_i\}$ to $\mathcal{A}$. It is feasible to verify that $\sigma \cdot P = PK_i + w_i \cdot R_i$ holds.

According to the Forking Lemma, assuming that $\mathcal{A}$ has produced two valid signatures, we have $\sigma \cdot P = PK_i + w_i \cdot R_i$ and $\widetilde{\sigma} \cdot P = PK_i + \widetilde{w}_i \cdot R_i$. To violate σ, $\mathcal{A}$ will perform the following steps.

$$\begin{aligned}(\sigma - \widetilde{\sigma}) \cdot P &= \sigma \cdot P - \widetilde{\sigma} \cdot P \\ &= (PK_i + w_i \cdot R_i) \cdot P - (PK_i + \widetilde{w}_i \cdot R_i) \cdot P \\ &= w_i \cdot Ri \cdot P - \widetilde{w}_i \cdot Ri \cdot P \\ &= (w_i - \widetilde{w}_i) \cdot r_i \cdot P^2\end{aligned} \tag{5}$$

By calculating $(\sigma - \widetilde{\sigma})((w_i - \widetilde{w}_i) \cdot P^2)^{-1}$, $\mathcal{C}$ demonstrates that $\mathcal{A}$ has effectively resolved the ECDLP problem within a polynomial time, thereby contradicting the principles defined in Definition 1. As a consequence, we reach the conclusion that the communication within our scheme remains impervious to adaptive chosen message attacks when operating within the random oracle model.

5.2. Security Analysis

We set several security goals in Section 2. Next, we delve into a detailed analysis of the security properties associated with the proposed scheme.

(1) Anonymity: OLDs in our system will not communicate with other entities with pseudo identities PID_i, where $PID_i = \{PID_{i,1}, PID_{i,2}\}$, $PID_{i,1} = ID_i \oplus H0(sk_i \cdot L_i \| T_t)$, $PID_{i,2} = (sk_i \cdot L_i) \oplus H1(T_t)$. Malicious users are not able to obtain the sender's privacy only via public parameters and messages sent. This way, vehicles are allowed to send messages without exposing their real identities.

(2) Authentication and Privacy: All messages sent by communicating parties should sign these messages before sending. They compute $\sigma = sk_i + w_i \cdot r_i \ mod \ q$, where $w_i = H2(M_i \| PID_i \| T_t \| R_i \| PK_i)$. Then encapsulated messages $msg = \{M_i, T_t, PK_i, R_i, PID_i\}$ are broadcasted. Thus, all interactive parties in our system can authenticate each other to ensure reliability and legitimacy. In addition, an encapsulated message msg includes no LC NLC_i explicitly, which will keep the basic location privacy of OLDs. But when needed, the GC can derive the rough location of v_i by computing $(PID_{i,2} \oplus H1(T_t)) \cdot (PK_i \cdot \alpha)^{-1}$ from the msg.

(3) Traceability: When malicious messages are detected, the GC will extract vehicles' real identities by computing $ID_i = H0(PK_i \cdot \alpha \cdot NLC_i \| T_t) \oplus PID_{i,1}$, since $sk_i \cdot L_i = sk_i \cdot \alpha \cdot NLC_i \cdot P = PK_i \cdot \alpha \cdot NLC_i$ and $NLC_i = (PID_{i,2} \oplus H1(T_t)) \cdot (PK_i \cdot \alpha)^{-1}$ can be easily derived via messages.

(4) Unlinkability: Every time, to generate a message $msg : \{M_i, T_t, PK_i, R_i, PID_i\}$, a random number $r_i \in Z_q$ will be reselected and a new $w_i = H2(M_i \| PID_i \| T_t \| R_i \| PK_i)$ will be recomputed. Due to the randomness of r_i and the variability of w_i, a malicious party is unable to link messages sent by one OLD to itself. Therefore, the proposed scheme offers unlinkability in interactive communications.

(5) Resistance to common attacks: Our scheme is capable of countering common attacks present in traditional networks, such as the following:

    * *Replay Attack*: By encapsulating the timestamp T_t within the message, it prevents the message from being forwarded again in the future. Upon receiving the message, receivers first check the timestamp to verify its freshness. If it is still

fresh, the receiver will start to verify the validation of these messages. Otherwise, messages will be abandoned.

* *Impersonation Attack*: An adversary needs to generate a signature for the message msg that satisfies $\sigma \cdot P = PK_i + w_i \cdot R_i$ in order to impersonate a legitimate vehicle. However, based on Theorem 1, no adversary can forge such a signature in polynomial time, which proves that our scheme is capable of resisting impersonation attacks.
* *Modification Attack*: A signature $\sigma = sk_i + w_i \cdot r_i \; mod \; q$ is a digital signature related to M_i since $w_i = H2(M_i \| PID_i \| T_t \| R_i \| PK_i)$. If M_i is modified by a malicious party, then w_i will change consequently, which makes σ change as well. Hence, the modification can be easily detected if the message itself is modified. This way, our scheme is able to resist modification attacks.
* *Sybil Attack*: To start a sybil attack, the adversary must generate multiple identities to play multiple roles. However, the pseudo identities are computed by a tamper-proof device. An adversary must violate the device first to generate those identities, which is infeasible via current technologies. Hence, our scheme successfully defends against sybil attacks.

6. Performance Analysis

In this analysis, we evaluate the performance of our scheme in comparison to the schemes proposed by Pournaghi et al. [47], Li et al. [6] and Tzeng et al. [48]. The evaluation is conducted on a system equipped with an Intel Core CPU i7-6700 operating at 3.40 GHz and 8 GB RAM, running the Windows 7 operating system. Firstly, we adopt a bilinear pairing denoted $E : G_1 \times G_1 \rightarrow G_T$, which ensures a security level equivalent to 80 bits, where P' serves as the generator of G_1. And G_1 is defined as a super singular elliptic curve $E' : y^2 = x^3 + x \; mod \; p'$, where p' is a 512-bit prime number and q' represents its order, which is a prime number of 160 bits. Let q denote the order of the group G on the super elliptic curve $E : y^2 = x^3 + ax + b \; mod \; p, (a, b \in Z_p^*)$; in this context, both q and p are 160-bit prime numbers. The symbols used throughout this section are as follows:

- T_{bp}: The duration of executing a bilinear pairing operation $e(Q', R'), \; Q', R' \in G_1$.
- T_{bm}: The duration of the scale multiplication operation $x' \cdot P'$ of bilinear pairing, where $x' \in Z_{q'}, P' \in G_1$.
- T_{ba}: The duration of the point addition operation $Q' + R'$ of bilinear pairing, where $Q', R' \in G_1$.
- T_{mtp}: The duration of a MapToPoint hash operation of bilinear pairing.
- T_{em}: The duration of the scale multiplication operation $x \cdot P$, where $x \in Z_q, P \in G$.
- T_{ea}: The duration of a point addition operation $Q + R$, where $Q, R \in G$.
- T_h: The duration of an one-way hash function operation.

The time taken for each operation is presented in Table 2.

Table 2. Running time of operations.

Operations	Running Time (ms)
T_{bp}	5.086
T_{bm}	0.694
T_{ba}	0.0018
T_{mtp}	0.0992
T_{em}	0.3218
T_{ea}	0.0024
T_h	0.001

6.1. Computation Cost Analysis

In the scheme proposed by Pournaghi et al. [47], when signing a single message, the bilinear pairing scale multiplication operation is performed four times, the bilinear pairing addition operation is performed once, the bilinear pairing MapToPoint function is performed once and the hash function is performed twice. The total time required for these operations is approximately 2.8790 ms, calculated as $4T_{bm} + T_{ba} + T_{mtp} + 2T_h$. And when the batch verification is implemented, the bilinear pairing addition operation is performed $3(n-1)$ times, the bilinear pairing scalar multiplication operation is performed n times, the bilinear pairing operation is performed three times, the MapToPoint operation is performed n times and the one-way hash function is performed n times. The total approximate time for these operations can be expressed as $3(n-1)T_{ba} + nT_{bm} + 3T_{bp} + nT_{mtp} + nT_h \approx 0.7996n + 15.2598$ ms.

In the scheme proposed by Tzeng et al. [48], when signing a single message, the bilinear pairing scale multiplication operation is performed three times and the hash function operation is performed twice, resulting in approximately 2.0840 *ms*, calculated as $3T_{bm} + 2T_h$. During batch verification, the bilinear pairing addition operation and the bilinear pairing scalar multiplication operation are both performed $(2n+1)$ times, the bilinear pairing operation is performed twice and the one-way hash function is performed n times, resulting in approximately $1.3926n + 10.8678$ ms, calculated as $(2n+1)T_{ba} + (2n+1)T_{bm} + 2T_{bp} + nT_h$.

In the scheme proposed by Li et al. [6], when signing a single message, the scale multiplication operation is performed once and the one-way hash function is performed twice, resulting in approximately 0.3238 ms, calculated as $T_{em} + 2T_h$. During batch verification, the scale multiplication operation is performed $(2n+2)$ times, the point addition operation is performed n times and the one-way hash function is performed $(2n)$ times, resulting in approximately $0.648n + 0.6436$ ms, calculated as $(2n+2)T_{em} + nT_{ea} + (2n)T_h$.

In our scheme, when signing a single message, the scale multiplication operation is performed once and the one-way hash function is executed twice, resulting in approximately 0.3228 ms, calculated as $T_{em} + T_h$. During batch verification, the scale multiplication operation is performed $2n$ times, the point addition operation is performed n times and the one-way hash function is performed n times, resulting in approximately $0.647n$ ms, calculated as $2nT_{em} + nT_{ea} + nT_h$.

As Figure 4 shows, to sign a message, our scheme costs lower computation power than the other three schemes. In Figure 5, we conducted a comparison of the execution time for batch verifications and the result indicates that our scheme demonstrates superior performance.

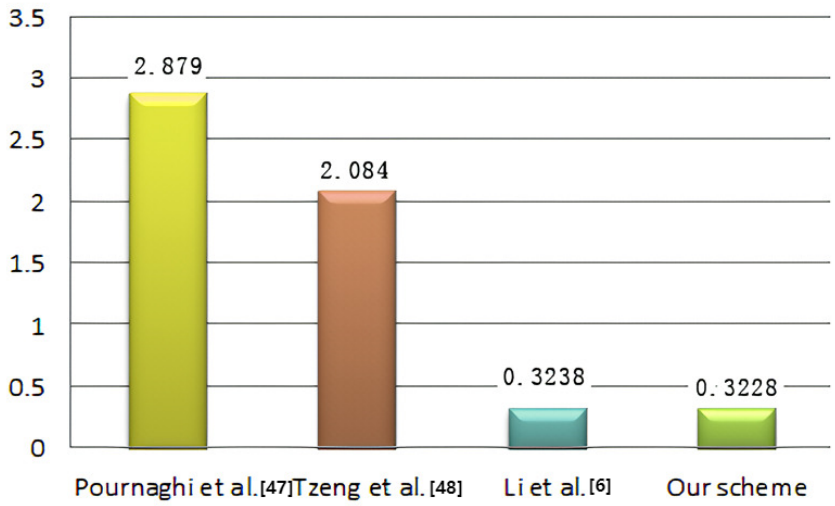


Figure 4. The time consumed for signing.

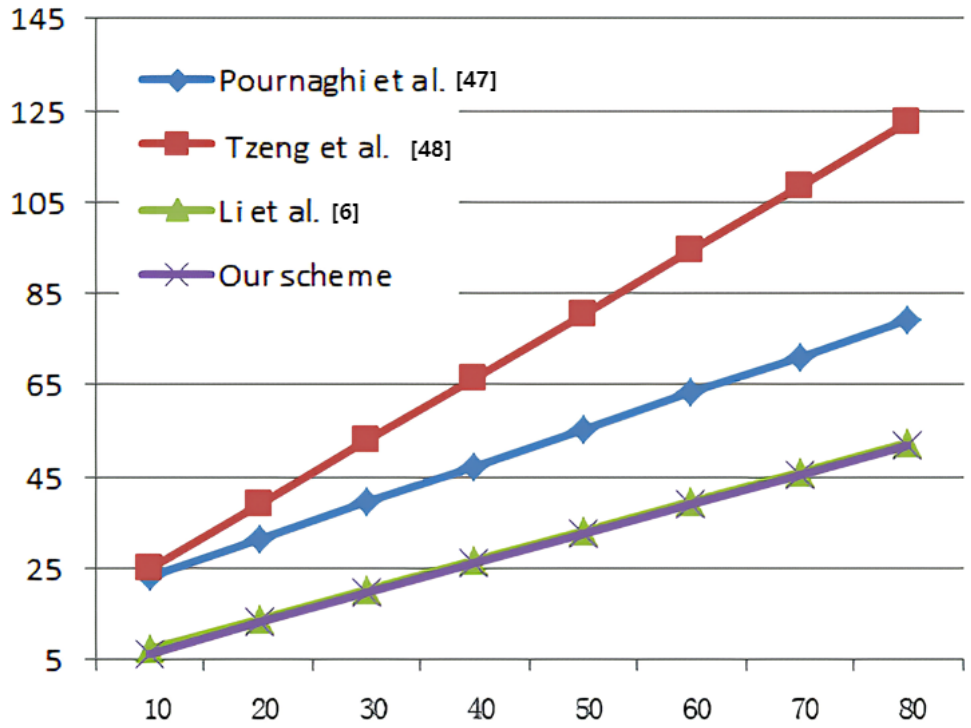


Figure 5. The time consumed for batch verifications.

6.2. Communication Cost Analysis

We only analyze our scheme in detail since the analyzing process is the same. In our scheme, the online learning devices will send the anonymous identity and signature $\{M_i, T_t, PK_i, R_i, PID_i\}$, in which $PID_i = \{PID_{i,1}, PID_{i,2}\} \in G, \sigma \in Z_q$ and T_t is the timestamp. Therefore, in our scheme, the communication cost is $40 \times 4 + 20 + 4 = 184$ bytes, while the scheme proposed by Pournaghi et al. [47] requires 296 bytes, the scheme by Tzeng et al. [48] requires 388 bytes and the scheme by Li et al. [6] requires 144 bytes.

Table 3 provides a summary of the comparison among the different schemes in terms of computation costs and communication costs.

Table 3. Comparison of computational and communication costs.

	Signature	Batch Authentication	Communication Cost
[47]	$4T_{bm} + T_{ba} + T_{mtp} + 2T_h$	$(n+2)T_m + (3n-1)T_a + 2nT_h$	296 bytes
[48]	$3T_{bm} + 2T_h$	$(2n+1)T_{ba} + (2n+1)T_{bm} + 2T_{bp} + (n)T_h$	388 bytes
[6]	$1T_{em} + 2T_h$	$(2n+2)T_{em} + (n)T_{ea} + (2n)T_h$	144 bytes
Our	$1T_{em} + T_h$	$2nT_{em} + (n)T_{ea} + (n)T_h$	184 bytes

7. Conclusions

This paper proposes a secure communication scheme based on a multicast mechanism in software-defined MIoT. Firstly, we designed a multicast tree protocol based on DBWST. This protocol incorporates multicast mechanisms to quickly establish a multicast tree among affected online learning devices after the occurrence of emergencies. Secondly, an adaptive signature authentication scheme is devised to ensure the security of multi-party communication, enabling the system to meet security requirements such as anonymity, privacy preservation and traceability. Additionally, our scheme supports batch authentication, effectively saving resources. Furthermore, a security proof conducted under the

random oracle model demonstrates that the proposed scheme satisfies the security requirements for secure communication in software-defined MIoT. The performance comparison of the scheme indicates its superior performance in both computing and communication. However, our system does not consider the actual distribution of online learning devices and does not achieve optimal efficiency. In the future, we will focus on how to group online learning devices based on the proposed scheme, which will help in managing online learning devices more efficiently in device-intensive areas.

Author Contributions: In this research paper, J.Y. conceived, designed, and wrote the cryptographic protocol; J.C. performed the experiments and analyzed the collected experimental data. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Foundation of Anhui Educational Committee grant number 2020jyxm0326, 2022sx020, 2022jy55; National Natural Science Foundation of China grant number 62272002.

Institutional Review Board Statement: Not applicable

Informed Consent Statement: Not applicable

Data Availability Statement: Due to restrictions on user privacy, we cannot make the data publicly available. If readers require access to the data, they can contact the authors via email to obtain it.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Gómez, J.; Huete, J.F.; Hoyos, O.; Perezc, L.; Grigorid, D. Interaction system based on Internet of Things as support for education. *Procedia Comput. Sci.* **2013**, *21*, 132–139. [CrossRef]
2. Gul, S.; Asif, M.; Ahmad, S.; Yasir, M.; Majid, M.; Malik M.S.A. A survey on role of Internet of Things in education. *Int. J. Comput. Sci. Netw. Secur.* **2017**, *17*, 159–165.
3. Konan M, Wang W. A secure mutual batch authentication scheme for patient data privacy preserving in WBAN. *Sensors* **2019**, *19*, 1608–1621. [CrossRef]
4. Vasile, R.; Olivares, S.; Paris, M.G.A.; Maniscalco, S. Continuous-variable quantum key distribution in non-Markovian channels. *Phys. Rev. A* **2011**, *83*, 042321. [CrossRef]
5. Pei, X.L.; Wang, X.; Wang, Y.F.; Li, M.K. Internet of Things based education: Definition, benefits and challenges. *Appl. Mech. Mater.* **2013**, *411*, 2947–2951. [CrossRef]
6. Li, J.L.; Choo, K.K.R.; Zhang, W.; Kumari, S.; Joel J.P.C.R.; Khan, M.K.; Hogrefe, D. EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *Veh. Commun.* **2018**, *13*, 104–113. [CrossRef]
7. Liu, Y.; Wang, Y.; Chang, G. Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2740–2749. [CrossRef]
8. Phoenix, S.; Khan, F.; Teklu, B. Preferences in quantum games. *Phys. Lett. A*, **2020**, *384*, 126299. [CrossRef]
9. Shao, J.; Lin, X.; Lu, R.; Zuo, C. A threshold anonymous authentication protocol for VANETs. *IEEE Trans. Veh. Technol.* **2015**, *65*, 1711–1720. [CrossRef]
10. Trapani, J.; Teklu, B.; Olivares, S.; Paris, M.G.A. Quantum phase communication channels in the presence of static and dynamical phase diffusion. *Phys. Rev. A* **2015**, *92*, 012317. [CrossRef]
11. Wang, M.; Liu, D.; Zhu, L.; Xu, Y.; Wang, F. LESPP: Lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication. *Computing* **2016**, *98*, 685–708. [CrossRef]
12. He, D.; Zeadally, S.; Xu, B.; Huang, X. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *J. Abbr.* **2015**, *10*, 2681–2691. [CrossRef]
13. Huang, J.; Qian, Y.; Hu, R.Q. Secure and Efficient Privacy-Preserving Authentication Scheme for 5G Software Defined Vehicular Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 8542–8554. [CrossRef]
14. Cui, J.; Zhang, X.; Zhong, H.; Zhang, J.; Liu, L. Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 1654–1667. [CrossRef]
15. Li, H.; Dong, M.; Ota, K. Control plane optimization in software-defined vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 7895–7904. [CrossRef]
16. Rosati, M.; Mari, A.; Giovannetti, V. Coherent-state discrimination via nonheralded probabilistic amplification. *Phys. Rev. A* **2016**, *93*, 062315. [CrossRef]
17. Duan, P.; Peng, C.; Zhu, Q.; Shi, J.; Cai, H. Design and analysis of software defined Vehicular Cyber Physical Systems. In Proceedings of the 2014 20th IEEE International Conference on Parallel and Distributed Systems (ICPADS), Hsinchu, Taiwan, 16–19 December 2014; pp.412–417

18. Teklu, B.; Bina, M.; Paris, M.G.A. Noisy propagation of Gaussian states in optical media with finite bandwidth. *Sci. Rep.* **2022**, *12*, 11646. [CrossRef] [PubMed]
19. de Oca, E.M.; Mallouli, W. Security Aspects of SDMN. In *Software Defined Mobile Networks (SDMN) beyond LTE Network Architecture*; IEEE: Piscataway, NJ, USA, 2015, pp. 331–357.
20. Nkenyereye, L.; Nkenyereye, L.; Islam, S.M.R.; Choi, Y.H.; Bilal, M.; Jang, J.W. Software-defined network-based vehicular networks: A position paper on their modeling and implementation. *Sensors* **2019**, *19*, 3788. [CrossRef]
21. Zhu, M.; Cao, J.; Pang, D.; He, Z.; Xu, M. SDN-based routing for efficient message propagation in VANET. In *Wireless Algorithms, Systems and Applications: 10th International Conference, Qufu, China, 10–12 August 2015*; Springer International Publishing: Berlin/Heidelberg, Germany, 2015; pp. 788–797.
22. Karakus, M.; Durresi, A. Quality of service (QoS) in software defined networking (SDN): A survey. *J. Netw. Comput. Appl.* **2017**, *10*, 2681–2691. [CrossRef]
23. Lai, C.; Lu, R.; Zheng, D. Achieving secure and seamless IP Communications for group-oriented software defined vehicular networks. *Wirel. Algorithms Syst.* **2017**, *10*, 356–368.
24. Kim, H.S.; Yun, S.; Kim, H.; Shin, H.; Kim, W.T. An efficient SDN multicast architecture for dynamic industrial IoT environments. *Mob. Inf. Syst.* **2018**, *2018*, 8482467. [CrossRef]
25. Teklu, B. Continuous-variable entanglement dynamics in Lorentzian environment. *Phys. Lett. A* **2022**, *432*, 128022. [CrossRef]
26. Do, T.X.; Nguyen, V.G.; Kim, Y. SDN-based mobile packet core for multicast and broadcast services. *Wirel. Netw.* **2018**, *24*, 1715–1728. [CrossRef]
27. Zhou, S.; Wang, H.; Yi, S.; Zhu, F. Cost-efficient and scalable multicast tree in software defined networking. In Proceedings of the Algorithms and Architectures for Parallel Processing: 15th International Conference, ICA3PP 2015, Zhangjiajie, China, 18–20 November 2015; pp. 592–605.
28. Lecompte, D.; Gabin, F. Evolved multimedia broadcast/multicast service (eMBMS) in LTE-advanced: Overview and Rel-11 enhancements. *IEEE Commun. Mag.* **2012**, *50*, 68–74. [CrossRef]
29. Chen, J.; Yan, F.; Li, D.; Chen, S.; Qiu, X. Recovery and Reconstruction of Multicast Tree in Software-Defined Network: High Speed and Low Cost. *IEEE Access* **2020**, *8*, 27188–27201. [CrossRef]
30. Teklu, B.; Trapani, J.; Olivares, S.; Paris, M.G.A. Noisy quantum phase communication channels. *Phys. Scr.* **2015**, *90*, 074027. [CrossRef]
31. Garg, S.; Kaur, K.; Kaddoum, G.; Ahmed, S.H.; Jayakody, D.N.K. SDN-based secure and privacy-preserving scheme for vehicular networks: A 5G perspective. *IEEE Trans. Veh. Technol.* **2019**, *68*, 8421–8434. [CrossRef]
32. Adnane, H.; Teklu, B.; Paris, M.G.A. Quantum phase communication channels assisted by non-deterministic noiseless amplifiers. *JOSA B* **2019**, *36*, 2938–2945. [CrossRef]
33. Moulierac, J.; Guitton, A.; Molnár, M. Multicast tree aggregation in large domains. In *Networking Technologies, Services and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems: 5th International IFIP-TC6 Networking Conference, Coimbra, Portugal, 15–19 May 2006*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 691–702.
34. Li, W.; Guo, Y. A Secure Private Cloud Storage Platform for English Education Resources Based on IoT Technology. *Comput. Math. Methods Med.* **2022**, *2022*, 8453470 . [CrossRef]
35. Tao, H. Online English Teaching System Based on Internet of Things Technology. *J. Sens.* **2022**, *2022*, 7748067 . [CrossRef]
36. Chen, D. Application of IoT-Oriented Online Education Platform in English Teaching. *Math. Probl. Eng.* **2022**, *2022*, 9606706. [CrossRef]
37. Gao, W. Designing an interactive teaching model of English language using Internet of Things. *Soft Comput.* **2022**, *26*, 10903–10913. [CrossRef]
38. Azees, M.; Vijayakumar, P.; Deboarh, L.J. EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. *IEEE Trans. Intell. Transp.* **2017**, *18*, 2467–2476. [CrossRef]
39. Li, J.; Ji, Y.; Choo, K.K.R.; Hogrefe, D. CL-CPPA: Certificate-less conditional privacy-preserving authentication protocol for the Internet of Vehicles. *IEEE Internet Things J.* **2019**, *6*, 10332–10343. [CrossRef]
40. Xiang, D.; Li, X.; Gao, J.; Zhang, X. A secure and efficient certificateless signature scheme for Internet of Things. *Ad Hoc Netw.* **2022**, *124*, 102702. [CrossRef]
41. Hong, H.; Sun, Z. TS-ABOS-CMS: Time-bounded secure attribute-based online/offline signature with constant message size for IoT systems. *J. Syst. Archit.* **2022**, *123*, 102388. [CrossRef]
42. Khashan, O.A.; Khafajah, N.M. Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems. *J. King Saud Univ.-Comput. Inf. Sci.* **2023**, *35*, 726–739. [CrossRef]
43. Wang, S.; Li, H.; Chen, J.; Wang, J.; Deng, Y. DAG blockchain-based lightweight authentication and authorization scheme for IoT devices. *J. Inf. Secur. Appl.* **2022**, *66*, 103134. [CrossRef]
44. Lai, C.; Zhou, H.; Cheng, N.; Shen, X.S. Secure group communications in vehicular networks: A software-defined network-enabled architecture and solution. *IEEE Veh. Technol. Mag.* **2017**, *12*, 40–49. [CrossRef]
45. Cui, J.; Zhang, X.; Zhong, H.; Ying, Z.; Liu, L. RSMA: Reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks. *IEEE Internet Things J.* **2019**, *6*, 6417–6428. [CrossRef]
46. Cui, J.; Wu, D.; Zhang, J.; Xu, Y.; Zhong, H. An efficient authentication scheme based on semi-trusted authority in VANETs. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2972–2986. [CrossRef]

47. Pournaghi, S.M.; Zahednejad, B.; Bayat, M.; Farjami, Y. NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET. *Comput. Netw.* **2018**, *134*, 78–92. [CrossRef]
48. Tzeng, S.F.; Horng, S.J.; Li, T.; Wang, X.; Huang, P.H.; Khan, M.K. Enhancing security and privacy for identity-based batch verification scheme in VANETs. *IEEE Trans. Veh. Technol.* **2015**, *66*, 3235–3248. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.