BLA: Blockchain-Assisted Lightweight Anonymous Authentication for Distributed Vehicular Fog Services

Yingying Yao, Xiaolin Chang, *Member, IEEE*, Jelena Mišić, *Fellow, IEEE*,
Vojislav B. Mišić, *Senior Member, IEEE*, and Lin Li

***Abstract*—As modern vehicles and distributed fog services advance apace, vehicular fog services (VFSs) are being expected to span across multiple geo-distributed datacenters, which inevitably leads to cross-datacenter authentication. Traditional cross-datacenter authentication models are not suitable for the scenario of high-speed moving vehicles accessing VFS, because these models either ignored user privacy or ignored the delay requirement of driving vehicles. This paper proposes a blockchain-assisted lightweight anonymous authentication (BLA) mechanism for distributed VFS, which is provisioned to driving vehicles. BLA can achieve the following advantages: 1) realizing a flexible cross-datacenter authentication, in which a vehicle can decide whether to be reauthenticated or not when it enters a new vehicular fog datacenter; 2) achieving anonymity, and granting vehicle users the responsibility of preserving their privacy; 3) it is lightweight by achieving noninteractivity between vehicles and service managers (SMs), and eliminating the communication between SMs in the authentication process, which significantly reduces the communication delay; and 4) resisting the attack that the database governed by one center is tampered with. BLA achieves these advantages by effectively combining modern cryptographical technology and blockchain technology. These security features are demonstrated by carrying out security analysis. Meanwhile, extensive simulations are conducted to validate the efficiency and practicality of BLA.**

***Index Terms*—Anonymous, blockchain, cross-datacenter authentication, noninteractive, vehicular fog services (VFSs).**

I. Introduction

A VEHICULAR ad hoc network (VANET) is a subset of a mobile ad hoc network (MANET) which consists of mobile vehicles and roadside units (RSUs). Each vehicle is equipped with an on-board unit (OBU) and a group of sensors. VANETs have been depending primarily on cloud computing services for communication, computing, and storage facilities [1]. The tremendous rise in the number of connected vehicles and their ever-increasing mobility create the demand for low latency and uninterrupted services. Meeting the quality of service of users is an important challenge to vehicular cloud computing services that integrates cloud computing with VANETs [2]. Therefore, vehicular fog computing (VFC) [3] was proposed to overcome the challenges of efficient communication and computation with the emergence of latest and advanced vehicular applications [4]. VFC is considered as one of the most potential techniques to be highly beneficial for latency-sensitive applications which is ideal for high-speed moving vehicles. Thus, there are more and more attentions to the security and performance of vehicular fog services (VFSs) during its applications and popularizations.

There are several basic security and performance requirements of VFS, including authentication and privacy of vehicles' identities as well as real-time constraints and so on [5]. On one hand, each vehicle accessing VFS must be authenticated for subsequent authorization decisions. Meanwhile, the identity of a vehicle cannot be disclosed during the authentication process in order to ensure the privacy of vehicle users [6]. On the other hand, to accommodate the rapid movement of vehicles, the authentication is required to be lightweight.

Various anonymous authentication mechanisms have been proposed [7] for vehicle user privacy. They applied symmetric cryptography, public key infrastructure, identity-based signature, certificateless signature, or group signature. All of them relied on an administration center which created preset trust relationship with vehicles. But the relationship can fail when a vehicle moves to a new datacenter. To address this problem, researchers explored cross-datacenter authentication. The existing cross-datacenter/cross-region/cross-domain mechanisms [14]–[24] required multiple interactions among OBUs, RSUs, and trusted authority, causing high communication delays. Furthermore, their databases are managed by a single manager in these mechanisms, which cannot resist the attack which the database governed by one center is tampered with.

Recently, blockchain technology is attracting massive attention in both academia and industry [8]. A blockchain is

Manuscript received September 3, 2018; revised December 16, 2018; accepted December 25, 2018. Date of publication January 9, 2019; date of current version May 8, 2019. The work of Y. Yao was supported in part by the China Scholarship Council and in part by the National Natural Science Foundation of China under Grant 2018YJS023. The work of X. Chang was supported by the National Natural Science Foundation of China under Grant U183610024, Grant 61572066, and Grant 61502486. The work of J. Mišić and V. B. Mišić was supported by the National Science and Engineering Research Council of Canada through AQ1 Discovery Grants. *(Corresponding author: Xiaolin Chang.)*

Y. Yao, X. Chang, and L. Li are with the Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Beijing 100044, China (e-mail: 17112100@bjtu.edu.cn; xlchang@bjtu.edu.cn; lilin@bjtu.edu.cn).

J. Mišić and V. B. Mišić are with the Department of Computer Science, Ryerson University, Toronto, ON M5B 2K3, Canada (e-mail: jmisic@ryerson.ca; vmisic@ryerson.ca).

Digital Object Identifier 10.1109/JIOT.2019.2892009

2327-4662 © 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

a distributed system in which multiple network nodes maintain the same information without requiring a central authority. Therefore, this technology can not only alleviate the attack that the database governed by a central authority is tampered with, but also reduce communication overhead between datacenter/region/domain managers. This is especially suitable for delay-sensitive vehicular applications. These features motivate us to explore the application of blockchain technology to design the authentication mechanism.

In this paper, we propose a blockchain-assisted lightweight anonymous authentication (BLA) mechanism for distributed VFS to alleviate the above problems. BLA can achieve the following advantages.

1) Achieving a flexible cross-datacenter authentication. By flexible, we mean that a vehicle itself can decide to be reauthenticated or just send a VFS request directly when it moves to a new datacenter.
2) Realizing anonymity in order to preserve the privacy of vehicles. BLA grants vehicles the responsibility of preserving privacy, by allowing a vehicle to reauthenticate itself to change its pseudonym. Namely, a vehicle can determine the time and frequency of changing its pseudonym.
3) BLA is lightweight. First, cryptographical and blockchain technologies are combined to eliminate the interactivity between vehicles and service managers (SMs). A driving vehicle just needs to send one message which can be an authentication message or a VFS request message before accessing VFS. This can significantly reduce the time of authentication. In addition, the application of blockchain technology also eliminates the communication between SMs in the user authentication process. Because the records of all SMs are updated synchronously.
4) BLA can effectively resist the attack that the database governed by one center is tampered with, due to that the public ledger is maintained by all SMs.

BLA provides these advantages by combining cryptographical and blockchain technologies. To the best of our knowledge, we are the first to propose a noninteractive anonymous cross-datacenter authentication mechanism.

The rest of this paper is organized as follows. Section II presents related work and Section III presents background knowledge. Section IV introduces the system model, design goals, and mechanism details. Security analysis and performance evaluation are presented in Sections V and VI, respectively. Section VII concludes this paper and discusses the future work.

II. Related Work

Yao *et al.* [9] described how to construct a vehicular fog datacenter (VFD) and how to provide reliable and secure VFS in a VFD. This section focuses on the existing anonymous authentication mechanisms, cross-datacenter identity authentication mechanisms, and blockchain-related technologies.

A. Anonymous Authentication Mechanisms in Vehicular Networks

Anonymous authentication is a common technique to preserve privacy of vehicles in vehicular networks (VNs) [7]. Vijayakumar *et al.* [10] proposed dual authentication and key management mechanism for secure data transmission in VNs to provide a high-level of security in the vehicle side of VNs. Azees *et al.* [6] proposed an efficient anonymous authentication mechanism with conditional privacy preserving for VNs to reduce the storage overhead of the anonymous certificates of vehicles and roadsides. Karati *et al.* [11] introduced a new identity-based signcryption mechanism to be applicable for low-bandwidth communications. An efficient protocol called distributed aggregate privacy-preserving authentication was proposed in [12]. Islam *et al.* [13] proposed an efficient password-based conditional privacy preserving authentication and group-key generation protocol for VNs. But all of them relied on an administration center which created preset trust relationship with vehicles. Thus, the relationship will not exist when a vehicle moves to a new datacenter.

B. Cross-Datacenter Identity Authentication

In the recent years, several cross-datacenter authenticated protocols and models were proposed to solve the issue in Section II-A. Xu *et al.* [14] introduced a session authority to realize cross-datacenter authentication and the agreement of session keys, whereas the essential role of the session authority is equivalent to that of the bridge certificate authority. Zhang *et al.* [15] put forward a novel virtual bridge certificate authority trust model and introduced an efficient implementation mechanism, which achieved the cross-datacenter authentications in the distributed collaborative manufacturing systems. He *et al.* [16] proposed a cross-datacenter anonymous authentication scheme for wireless body area network. A new efficient cross-domain handshake scheme was proposed in [17] for mobile healthcare social network. Yang *et al.* [18] presented a novel cross-datacenter dynamic anonymous authenticated group key management protocol to realize the cross-datacenter secure group communication. Chen *et al.* [19] designed a cryptographic protocol specifically for privacy-preserving cross-datacenter routing optimization in software defined networking. What is more, a dynamic cross-datacenter authentication asymmetric group key agreement protocol was proposed in [20]. This protocol adopted cross-datacenter authentication mechanism to avoid the security risks of key escrow and reduce the complexity of certificate management.

However, the authentication of these mechanisms required multiple interactions between users and datacenter, which is an obstacle for mobile vehicle users to access VFS efficiently. In addition, these mechanisms assumed one trusted authority, leading to that the systems are vulnerable to the attack that the database kept and maintained by one center is damaged.

Blockchain-based cross-datacenter authentication mechanisms have been proposed. Fromknecht *et al.* [21] proposed a blockchain-based decentralized PKI authentication system to provide key querying and identity binding service,

TABLE I
COMPARISON OF CONSENSUS ALGORITHMS

Algorithm	PoS	dPoS	Ouroboros	Casper	PBFT	PoET
Capability	Middle	High	High	Middle	High	High
Decentralization	Complete	Complete	Complete	Complete	Semi	Semi
Max evil nodes	51%	51%	51%	51%	33%	51%
Token	Yes	Yes	Yes	Yes	No	No
Scenario	Public blockchain	Public blockchain	Public blockchain	Public blockchain	Consortium blockchain	Consortium blockchain
Technical maturity	Mature	Mature	Mature	Non application	Mature	Non application
Dedicated hardware	No	No	No	No	No	Yes

but it may leak user's privacy because the user's identity and public key are stored in the blockchain directly. Lei *et al.* [22] presented a blockchain-based dynamic key management for heterogeneous intelligent transportation systems. Wang *et al.* [23] put forward a blockchain-based cross-domain authentication model named BlockCAM to ensure the safety and efficiency to access resources in different domains. Fu *et al.* [24] proposed a location-aware authentication mechanism for cross-domain Internet of Thing (IoT) systems. Compared to traditional cross-datacenter authentication mechanisms, blockchain-based cross-datacenter authentication mechanisms can increase the efficiency of authentication and also can resist DDoS attacks [23], because even if one node fails, other nodes will not be affected. Expect that, they are easily scalable. Our proposed mechanism not only has these advantages, but also achieves the feature of noninteractivity which does not exists in the above blockchain-based cross-datacenter authentication mechanisms.

C. Blockchain Technology and Consensus Mechanism

The blockchain is a linear collection of data elements, where each data element is called a block. All blocks are linked in chronological order to form a chain and secured using cryptography [25]. Current blockchain systems are categorized roughly into three types: 1) public blockchain; 2) private blockchain; and 3) consortium blockchain [26]. In this paper, we concentrate on the consortium blockchain, which is constructed by several organizations. It is semidecentralized since only a small portion of nodes would be selected to determine the consensus. The consortium blockchain has the following features. First, about its consensus determination, a selected set of nodes are responsible for validating the block. Second, the read permission of records can be public or restricted. Third, it is semidecentralized and has high efficiency. What is more, not everyone in the world can join the consensus process of the consortium blockchain because it is permissioned.

During the past decade, the blockchain-based applications are constantly expanding, ranging from finance to IoT. In finance filed, the most representative are Bitcoin [27] and Ethereum [28], more altcoins and their distinct features we can refer to [29]. There are also blockchain-based applications in IoTs such as in [30] and [31]. But our extensive literature investigation shows that no one applies blockchain technology to the field of VFS cross-datacenter authentication. In this paper, we adopt the blockchain technology to improve the security and performance of BLA.

In distributed systems, there are a variety of consensus algorithms, referred to [32] and [33], such as proof of work (PoW), proof of stake (PoS), delegated PoS (dPoS), casper, practical Byzantine fault tolerance (PBFT), proof of elapsed time (PoET), and Ouroboros. Each consensus algorithm has its own advantages and disadvantages and adapts to different scenarios. For example, the consensus time of PoW is long, which does not suit for the vehicular systems with time-delay constraints. The comparison of these consensus algorithms is shown in Table I. Due to the high real-time requirements and no token required, the PBFT algorithm with relatively fixed number of nodes participating in the consensus process is more suitable for BLA according to Table I.

III. BACKGROUND KNOWLEDGE

BLA proposed in this paper is mainly based on two hard problems. The first is computational Diffie–Hellman problem (CDHP). Let G be an additive cycle consisting of points on the elliptic curve, and its order is prime number q. P is a generator of G. Given $xP, yP \in G(x, y \in Z_q^*)$, calculating xyP is a hard problem. The second is elliptic curve discrete logarithm problem (ECDLP). Let G be an additive cycle consisting of points on the elliptic curve, and its order is prime number q. P is a generator of G. It is noted that $xP \in G$, calculating x is hard.

IV. BLA MECHANISM

In this section, we first describe the system model, then present the design goals and the details of BLA mechanism.

A. System Model

Fig. 1 shows the system considered in this paper, which consists of multiple regions. Each region includes a regional SM which manages multiple VFDs. There are five types of entities in the system.

1) *Audit Department (AD):* AD is a fully trusted authority, which is responsible for the registration of OBUs and SMs, and tracing illegal vehicles.
2) *SM:* Rather than maintaining a public ledger at each VFD, BLA establishes the role of SM to reduce the number of public leger managers in the *blockchain network* and then reduce the cost of infrastructure deployment. SM is the service manager of a region and needs to be registered at AD before establishing the system. An SM is mainly responsible for managing all VFDs

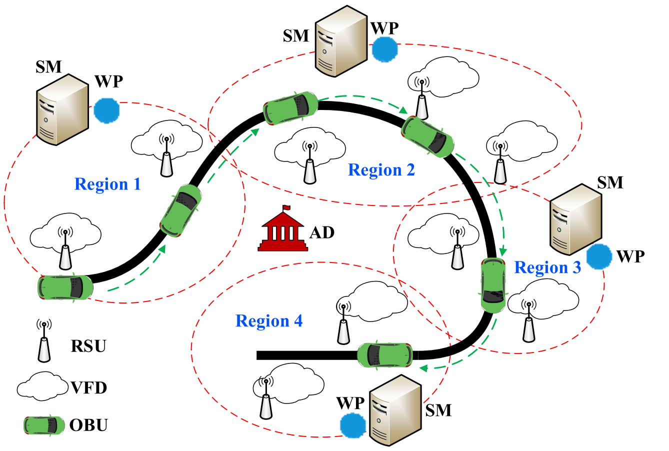


Fig. 1. System framework, including AD, SM, WP, RSU, OBU, and VFD.

and authenticating OBUs in its region. Each SM maintains a public ledger that contains all access records of vehicles. The public ledger only can be accessed by AD, SMs and WPs.

3) *Witness Peer (WP):* WP is a peer for writing authentication results to the public ledger through a consensus algorithm. There is a WP for each region. All WPs and SMs form a consortium blockchain.
4) *RSU:* RSU is the manager of a VFD and provisions VFS to legal OBUs. It belongs only to a region governed by an SM. Please refer to [9] for the details about how a RSU provisions VFS to an OBU.
5) *OBU:* OBU is a VFS user. It is equipped with computational and communication functions, such as embedded computer, wireless network interface, GPS receiver, vehicle navigation system, digital map, and so on. It needs to be registered at AD before accessing VFS.
6) *Consortium Blockchain Network (CBN):* It is made up of SMs and WPs of all regions. The infrastructure of CBN can refer to the blockchain infrastructure [34].

B. Design Goals

BLA for distributed VFS must achieve the following design goals concerning security and performance.

1) *Confidentiality:* Guarantee that an adversary cannot decrypt transmitted messages.
2) *Integrity:* Guarantee that an adversary cannot tamper with transmitted messages.
3) *Anonymity:* Allow each vehicle to use pseudonym, defined by itself. During its accessing VFS, a vehicle can change its pseudonym by reauthenticating itself, whenever necessary. By doing so, it is hard, if not impossible, for the adversary to track vehicles or count them.
4) *Noninteractivity:* Allow that a vehicle just needs to send one message, which could be an authentication message or accessing VFS message, before accessing VFS. No additional message is required to transmit.
5) *Traceability:* Guarantee that AD can trace illegal vehicles and refuse their access to VFS.

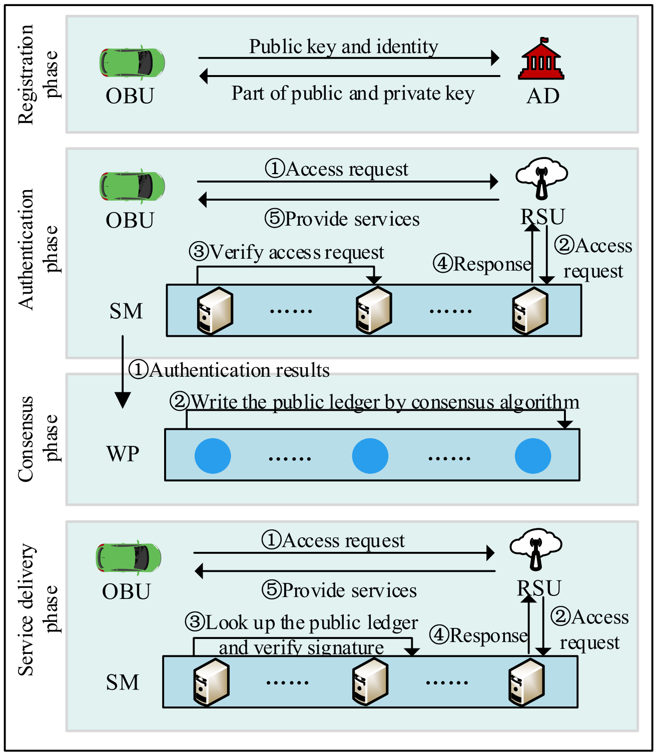


Fig. 2. Workflow of the proposed mechanism.

TABLE II
NOTATIONS

Notation	Description
PK_X	The public key of X
SK_X	The private key of X
ID_X	The unique identity of X
$Enc_X\{M\}$	Encrypt M with key X
$Sig_X\{M\}$	Sign M with key X
pid_x	A randomly selected pseudonym
tst	Timestamp

6) *Nonrepudiation:* Guarantee that when an illegal vehicle is reported, its misbehaviors cannot be denied.
7) *Lightweight:* Guarantee that the computation and communication overhead is low.

C. BLA Description

This section presents BLA, including five phases, namely *Initialization*, *Registration*, *Authentication*, *Consensus*, and *Service-delivery* phases (see Fig. 2). Since *Initialization* phase is just executed once by AD during the system establishment, Fig. 2 only shows the last four phases. The notations used in this paper are presented in Table II.

1) Initialization Phase: In this phase, AD performs the following operations to initialize a set of system parameters.

1) Set a system security parameter η to generate a large secure prime number q.
2) Choose an elliptic curve additive cyclic group G with order q and generator P of G.

3) Define the following secure Hash functions:

$$H_0 : \{0, 1\}^* \times G \times G \to Z_q^*, H_1 : G \times \{0, 1\}^* \times G \to Z_q^*$$
$$H_2 : G \to \{0, 1\}^*, H_3 : \{0, 1\}^* \to Z_q^*.$$

4) Randomly choose an integer $\mathrm{SK_{AD}} \in Z_q^*$ as its private key and calculate its public key $\mathrm{PK_{AD}} = \mathrm{SK_{AD}} \cdot P$.
5) Keep $\mathrm{SK_{AD}}$ secret and publish the system parameters $(q, \mathrm{PK_{AD}}, H_0, H_1, H_2, H_3)$.

2) Registration Phase: This phase completes the registration of SMs and OBUs. It is just executed once during the BLA lifecycle. The SM registration process executes the following operations.

1) SM_i randomly chooses an integer $\mathrm{SK}^1_{\mathrm{SM}_i} \in Z_q^*$ as the first part of its private key, calculates $\mathrm{PK}^1_{\mathrm{SM}_i} = \mathrm{SK}^1_{\mathrm{SM}_i} \cdot P$, and sends AD the encrypted first part of public key and its identity $\mathrm{Enc}_{\mathrm{PK_{AD}}}(\mathrm{PK}^1_{\mathrm{SM}_i}||\mathrm{ID}_{\mathrm{SM}_i})$.
2) After receiving $\mathrm{Enc}_{\mathrm{PK_{AD}}}(\mathrm{PK}^1_{\mathrm{SM}_i}||\mathrm{ID}_{\mathrm{SM}_i})$, AD decrypts it and checks the identity. Then it randomly chooses an integer $d_i \in Z_q^*$, and calculates $\mathrm{PK}^2_{\mathrm{SM}_i}$ and $\mathrm{SK}^2_{\mathrm{SM}_i}$ by $\mathrm{PK}^2_{\mathrm{SM}_i} = d_i \cdot P$ and $\mathrm{SK}^2_{\mathrm{SM}_i} = d_i + \mathrm{SK_{AD}} \cdot H_0(\mathrm{ID}_{\mathrm{SM}_i}, \mathrm{PK}^2_{\mathrm{SM}_i}, \mathrm{PK}^1_{\mathrm{SM}_i})$. After that, AD returns $\mathrm{SK}^2_{\mathrm{SM}_i}||\mathrm{PK}^2_{\mathrm{SM}_i}$ to SM_i through a secure channel.
3) SM_i extracts the second part $\mathrm{SK}^2_{\mathrm{SM}_i}$ of the private key from the received $\mathrm{SK}^2_{\mathrm{SM}_i}||\mathrm{PK}^2_{\mathrm{SM}_i}$ to constitute its complete private key $\mathrm{SK}_{\mathrm{SM}_i} = (\mathrm{SK}^1_{\mathrm{SM}_i}, \mathrm{SK}^2_{\mathrm{SM}_i})$. Then it extracts $\mathrm{PK}^2_{\mathrm{SM}_i}$ to constitute its complete public key $\mathrm{PK}_{\mathrm{SM}_i} = (\mathrm{PK}^1_{\mathrm{SM}_i}, \mathrm{PK}^2_{\mathrm{SM}_i})$. At the same time, SM_i can verify whether $\mathrm{PK}^2_{\mathrm{SM}_i} + H_0(\mathrm{ID}_{\mathrm{SM}_i}, \mathrm{PK}^2_{\mathrm{SM}_i}, \mathrm{PK}^1_{\mathrm{SM}_i}) \cdot \mathrm{PK_{AD}} = \mathrm{SK}^2_{\mathrm{SM}_i} \cdot P$ is true in order to judge the authenticity of the received private key$\mathrm{SK}^2_{\mathrm{SM}_i}$.

The registration process of an OBU executes the similar operations as follows.

1) An OBU_j randomly chooses an integer $\mathrm{SK}^1_{\mathrm{OBU}_j} \in Z_q^*$ as first part of its private key, calculates $\mathrm{PK}^1_{\mathrm{OBU}_j} = \mathrm{SK}^1_{\mathrm{OBU}_j} \cdot P$, and sends AD $\mathrm{Enc}_{\mathrm{PK_{AD}}}(\mathrm{PK}^1_{\mathrm{OBU}_j}||\mathrm{ID}_{\mathrm{OBU}_j})$, which is the encryption of the first part of public key and its identity.
2) AD decrypts the received $\mathrm{Enc}_{\mathrm{PK_{AD}}}(\mathrm{PK}^1_{\mathrm{OBU}_j}||\mathrm{ID}_{\mathrm{OBU}_j})$ and checks the identity. If successful, then it randomly selects an integer $d_j \in Z_q^*$, and calculates $\mathrm{PK}^2_{\mathrm{OBU}_j} = d_j \cdot P$ and $\mathrm{SK}^2_{\mathrm{OBU}_j} = d_j + \mathrm{SK_{AD}} \cdot H_0(\mathrm{ID}_{\mathrm{OBU}_j}, \mathrm{PK}^2_{\mathrm{OBU}_j}, \mathrm{PK}^1_{\mathrm{OBU}_j})$. After that, AD returns $\mathrm{SK}^2_{\mathrm{OBU}_j}||\mathrm{PK}^2_{\mathrm{OBU}_j}$ to OBU_j through a secure channel.
3) OBU_j extracts $\mathrm{SK}^2_{\mathrm{OBU}_j}$ and $\mathrm{PK}^2_{\mathrm{OBU}_j}$ from the received $\mathrm{SK}^2_{\mathrm{OBU}_j}||\mathrm{PK}^2_{\mathrm{OBU}_j}$ to constitute its complete private key $\mathrm{SK}_{\mathrm{OBU}_j} = (\mathrm{SK}^1_{\mathrm{OBU}_j}, \mathrm{SK}^2_{\mathrm{OBU}_j})$ and its complete public key $\mathrm{PK}_{\mathrm{OBU}_j} = (\mathrm{PK}^1_{\mathrm{OBU}_j}, \mathrm{PK}^2_{\mathrm{OBU}_j})$, respectively. Then, OBU_j can verify whether (1) is true in order to judge the authenticity of the received private key $\mathrm{SK}^2_{\mathrm{OBU}_j}$

$$\mathrm{PK}^2_{\mathrm{OBU}_j} + H_0\Big(\mathrm{ID}_{\mathrm{OBU}_j}, \mathrm{PK}^2_{\mathrm{OBU}_j}, \mathrm{PK}^1_{\mathrm{OBU}_j}\Big) \times \mathrm{PK_{AD}} = \mathrm{SK}^2_{\mathrm{OBU}_j} \cdot P. \tag{1}$$

3) Authentication Phase: This phase aims to authenticate OBUs through the corresponding SMs. After authentication, SMs broadcast the authentication results which are written to the public ledger with the consensus mechanism among WPs in the consensus phase. When a driving OBU_a first accesses VFS, it needs to execute the following operations.

1) Randomly choose an integer $r_1 \in Z_q^*$ and a pseudonym pid_u, calculate $s = [(r_1 + \mathrm{SK}^1_{\mathrm{OBU}_a})/(\mathrm{SK}^1_{\mathrm{OBU}_a} + h \cdot \mathrm{SK}^2_{\mathrm{OBU}_a})]$ where $T = r_1 \cdot P$ and $h = H_1(T + \mathrm{PK}^1_{\mathrm{OBU}_a}, \mathrm{ID}_{\mathrm{OBU}_a}, \mathrm{pid}_u, \mathrm{PK}^2_{\mathrm{OBU}_a})$.
2) Calculate $h_i = H_0(\mathrm{ID}_{\mathrm{SM}_i}, \mathrm{PK}^2_{\mathrm{SM}_i}, \mathrm{PK}^1_{\mathrm{SM}_i})$, $1 \le i \le k$. Then randomly choose an integer $r_2 \in Z_q^*$, and calculate $R = r_2 \cdot P$ and $C = H_2(R) \oplus (\mathrm{pid}_u||\mathrm{ID}_{\mathrm{OBU}_a}||s)$.
3) Calculate $x_i = H_3(\mathrm{ID}_{\mathrm{SM}_i})$, $1 \le i \le k$. After that, generate k coefficients $c_{i1}, c_{i2}, \ldots, c_{ik} \in Z_q^*$ by constructing the following Lagrange difference polynomial:

$$f_i(x) = \prod_{1 \le j \ne i \le k} \frac{x - x_j}{x_i - x_j} = c_{i1} + c_{i2}x + \cdots + c_{ik}x^{k-1}.$$

4) Calculate $Y_i = r_2 \cdot (\mathrm{PK}^1_{\mathrm{SM}_i} + \mathrm{PK}^2_{\mathrm{SM}_i} + h_i \cdot \mathrm{PK_{AD}})$ and use $c_{i1}, c_{i2}, \ldots, c_{ik} \in Z_q^*$ from the previous step to calculate $V_i = \sum_{l=1}^{k} c_{li} Y_l$, $1 \le i \le k$.
5) OBU_a sends ciphertext $\delta = (V_1, V_2, \ldots, V_k, T, C)$ to the RSU which is closest to it, assumed as RSU_m.
6) RSU_m receives ciphertext δ. Then it will forward δ to its region manager which is assumed to be SM_n.

After receiving ciphertext δ, SM_n executes the following operations.

1) Use its own identity to calculate $x_n = H_3(\mathrm{ID}_{\mathrm{SM}_n})$ and $Y'_n = V_1 + x_n V_2 + \cdots + x_n^{k-1}(\mathrm{mod} q)V_k$.
2) Calculate $R' = (\mathrm{SK}^1_{\mathrm{SM}_n} + \mathrm{SK}^1_{\mathrm{SM}_n})^{-1} Y'_n$, and resume original message and signature $(\mathrm{pid}_u||\mathrm{ID}_{\mathrm{OBU}_a}||s) = H_2(R') \oplus C$.
3) Get OBU_a's identity from the recovered message. If its public key is not in the revocation list, then calculate

$$\begin{cases} h'_a = H_0\Big(\mathrm{ID}_{\mathrm{OBU}_a}, \mathrm{PK}^2_{\mathrm{OBU}_a}, \mathrm{PK}^1_{\mathrm{OBU}_a}\Big) \\ h' = H_1\Big(T + \mathrm{PK}^1_{\mathrm{OBU}_a}, \mathrm{ID}_{\mathrm{OBU}_a}, \mathrm{pid}_u, \mathrm{PK}^2_{\mathrm{OBU}_a}\Big). \end{cases}$$

4) Verify whether (2) is true

$$h' = H_1\Big(s \cdot \Big(\mathrm{PK}^1_{\mathrm{OBU}_a} + h' \cdot \Big(\mathrm{PK}^2_{\mathrm{OBU}_a} + h'_a \cdot \mathrm{PK_{AD}}\Big)\Big) \mathrm{ID}_{\mathrm{OBU}_a}, \mathrm{pid}_u, \mathrm{PK}^2_{\mathrm{OBU}_a}\Big). \tag{2}$$

5) If the result is true, SM_n will search its local database. If the authentication information exists, it will update the authentication result in its database. At the same time, it will broadcast the authentication result to all WPs and inform RSU_m to provide VFS for OBU_a.

4) Consensus Phase: After receiving the authentication results, WPs write them into the corresponding public ledger through the PBFT consensus algorithm. We assume that there are k WPs, which are $\{\mathrm{WP}_1, \mathrm{WP}_2, \ldots, \mathrm{WP}_k\}$, respectively. For each round of consensus making, a WP will play as a speaker of the house while the left WPs play as congressmen. The detailed procedure is as follows.

1) Determine the speaker WP_x by $x = (\text{heightmod}k) + 1$, where height is the current block height. Because the selected speaker cannot affect the consensus results, he is allowed to host the consensus process n times in order to save the time of selecting speakers.
2) Any SM can broadcast its signed authentication results to all WPs.
3) All WPs monitor authentication result data sent out in the previous step and store the data in their own memory, respectively.
4) Define t to denote the time interval of generating a block. After the time t, the broadcasted authentication results during the period t constitute a block. Then the speaker sends $<$ *p_request*, height, WP_x, block, $\mathrm{Sig}_{\mathrm{WP}_x}(\text{block})$ $>$ to all congressmen. Here, *p_request* denotes the speaker asking the congressmen to vote.
5) After receiving the proposal, a congressman WP_i sends out $<$ *p_response*, height, WP_i, block, $\mathrm{Sig}_{\mathrm{WP}_i}(\text{block})$ $>$. Here, *p_response* denotes the congressmen response to the request of the speaker.
6) Any WP, upon receiving $\mathrm{Sig}_{\mathrm{WP}_i}(\text{block})$ from at least $(k - f)$ peers, reaches a consensus and publishes a full block. If the number of $\mathrm{Sig}_{\mathrm{WP}_i}(\text{block})$ does not reach $(k-f)$, the next round consensus will be executed. Here, $f = \lfloor (k-1)/3 \rfloor$, stands for the maximum number of erroneous WPs allowed in the system, for example, a WP has network fault.
7) Any WP, after receiving the full block, deletes the authentication results, which are contained in the block from its memory and begins the next round consensus.

5) Service-Delivery Phase: During this phase, when an OBU moves to another VFD of a new RSU, it could choose no reauthentication. The description is the following procedure.

1) When OBU_a drives to the service range of another RSU, assumed as RSU_x, it submits its access request $ac_{\mathrm{OBU}_a} = \{\mathrm{Sig}_{\mathrm{SK}_{\mathrm{OBU}_a}}(\mathrm{pid}_z, tst), \mathrm{pid}_z, tst\}$ to RSU_x.
2) Similarly, RSU_x forward ac_{OBU_a} to its region manager SM_q.
3) SM_q first looks up its local database to find $\mathrm{PK}_{\mathrm{OBU}_a}$. If there is no information, SM_q looks up the public ledger to get its information. If $\mathrm{PK}_{\mathrm{OBU}_a}$ is not in the revocation list, SM_q verifies $\mathrm{Sig}_{\mathrm{SK}_{\mathrm{OBU}_a}}(\mathrm{pid}_z, tst)$. If the result of authentication is successful and the timestamp tst is valid, SM_q directly informs RSU_x to respond to the service request of OBU_a. Otherwise, SM_q refuses to provide services.

During the whole process, if an illegal vehicle is reported to AD, AD will randomly access a public ledger, find out its identity and inform all SMs that the public key of the illegal vehicle is invalid and add it to revocation list.

V. Security Analysis

We analyze the security features of BLA with respect to the design goals given in Section IV-B.

A. Correctness

For the correctness proof of the proposed mechanism, we need to verify $Y'_v = Y_v (1 \le v \le k)$, $R' = R$ and (2) is true, respectively. The details are as follows:

$$
\begin{aligned}
Y'_v &= V_1 + x_v V_2 + \cdots + x_v^{k-1} (\mathrm{mod} q) V_k (1 \le v \le k)\\
&= \sum_{l=1}^{k} c_{l1} Y_l + x_v \left(\sum_{l=1}^{k} c_{l2} Y_l \right) + \cdots + x_v^{k-1} \left(\sum_{l=1}^{k} c_{lk} Y_l \right)\\
&= \left(\sum_{l=1}^{k} c_{1l} x_v^{l-1} \right) Y_1 + \left(\sum_{l=1}^{k} c_{2l} x_v^{l-1} \right) Y_2 + \cdots\\
&\quad + \left(\sum_{l=1}^{k} c_{vl} x_v^{l-1} \right) Y_v + \cdots + \left(\sum_{l=1}^{k} c_{kl} x_v^{l-1} \right) Y_k\\
&= f_1(x_v) Y_1 + f_2(x_v) Y_2 + \cdots + f_v(x_v) Y_v\\
&= Y_v\\
R' &= \left(\mathrm{SK}^1_{\mathrm{SM}_v} + \mathrm{SK}^2_{\mathrm{SM}_v} \right)^{-1} Y'_v\\
&= \left(\mathrm{SK}^1_{\mathrm{SM}_v} + \mathrm{SK}^2_{\mathrm{SM}_v} \right)^{-1} r_2 \left(\mathrm{PK}^1_{\mathrm{SM}_v} + \mathrm{PK}^2_{\mathrm{SM}_v} + h_v \mathrm{PK}_{\mathrm{AD}} \right)\\
&= \left(\mathrm{SK}^1_{\mathrm{SM}_v} + \mathrm{SK}^2_{\mathrm{SM}_v} \right)^{-1} r_2 \left(\mathrm{SK}^1_{\mathrm{SM}_v} + d_v + h_v \mathrm{SK}_{\mathrm{AD}} \right) P\\
&= \left(\mathrm{SK}^1_{\mathrm{SM}_v} + \mathrm{SK}^2_{\mathrm{SM}_v} \right)^{-1} r_2 \left(\mathrm{SK}^1_{\mathrm{SM}_v} + \mathrm{SK}^2_{\mathrm{SM}_v} \right) P\\
&= r_2 P\\
&= R
\end{aligned}
$$

$$
\begin{aligned}
&H_1\Big(s\Big(\mathrm{PK}^1_{\mathrm{OBU}_a} + h'\Big(\mathrm{PK}^2_{\mathrm{OBU}_a} + h'_a \cdot \mathrm{PK}_{\mathrm{AD}}\Big)\Big), \mathrm{ID}_{\mathrm{OBU}_a}, \mathrm{pid}_u, \mathrm{PK}^2_{\mathrm{OBU}_a}\Big)\\
&= H_1\Bigg(\Bigg(\frac{r_1 + \mathrm{SK}^1_{\mathrm{OBU}_a}}{\mathrm{SK}^1_{\mathrm{OBU}_a} + hSK^2_{\mathrm{OBU}_a}}\Bigg)\\
&\qquad \times \Big(\mathrm{PK}^1_{\mathrm{OBU}_a} + h\Big(\mathrm{PK}^2_{\mathrm{OBU}_a} + H_0\\
&\qquad\qquad\qquad \times \Big(\mathrm{ID}_{\mathrm{OBU}_a}, \mathrm{PK}^2_{\mathrm{OBU}_a}, \mathrm{PK}^1_{\mathrm{OBU}_a}\Big) \cdot \mathrm{PK}_{\mathrm{AD}}\Big)\Big)\\
&\qquad \mathrm{ID}_{\mathrm{OBU}_a}, \mathrm{pid}_u, \mathrm{PK}^2_{\mathrm{OBU}_a}\Bigg)\\
&= H_1\Bigg(\Bigg(\frac{r_1 + \mathrm{SK}^1_{\mathrm{OBU}_a}}{\mathrm{SK}^1_{\mathrm{OBU}_a} + hSK^2_{\mathrm{OBU}_a}}\Bigg)\Big(\mathrm{SK}^1_{\mathrm{OBU}_a} \cdot P + h\Big(\mathrm{SK}^2_{\mathrm{OBU}_a} \cdot P\Big)\Big)\\
&\qquad \mathrm{ID}_{\mathrm{OBU}_a}, \mathrm{pid}_u, \mathrm{PK}^2_{\mathrm{OBU}_a}\Bigg)\\
&= H_1\Bigg(\Bigg(\frac{r_1 + \mathrm{SK}^1_{\mathrm{OBU}_a}}{\mathrm{SK}^1_{\mathrm{OBU}_a} + h\mathrm{SK}^2_{\mathrm{OBU}_a}}\Bigg)\Big(\mathrm{SK}^1_{\mathrm{OBU}_a} + h\mathrm{SK}^2_{\mathrm{OBU}_a}\Big)P\\
&\qquad \mathrm{ID}_{\mathrm{OBU}_a}, \mathrm{pid}_u, \mathrm{PK}^2_{\mathrm{OBU}_a}\Bigg)\\
&= H_1\Big(\Big(r_1 + \mathrm{SK}^1_{\mathrm{OBU}_a}\Big)P, \mathrm{ID}_{\mathrm{OBU}_a}, \mathrm{pid}_u, \mathrm{PK}^2_{\mathrm{OBU}_a}\Big)\\
&= H_1\Big(T + \mathrm{PK}^1_{\mathrm{OBU}_a}, \mathrm{ID}_{\mathrm{OBU}_a}, \mathrm{pid}_u, \mathrm{PK}^2_{\mathrm{OBU}_a}\Big)\\
&= h'.
\end{aligned}
$$

Thus, the proposed mechanism satisfies correctness.

B. Confidentiality

First, in *Initialization phase*, according to ECDLP in Section III, given AD's public key $\mathrm{PK}_{\mathrm{AD}} = \mathrm{SK}_{\mathrm{AD}} \cdot P$, it is difficult for attackers to calculate AD's private key. In the same way, $\mathrm{SK}^1_{\mathrm{SM}_i}$ and $\mathrm{SK}^1_{\mathrm{OBU}_j}$ are also hard to calculate. This is the basis of the following. Second, during the whole process of executing BLA, the transmitted private information is always encrypted. In *Registration phase*, the real identities of SMs and OBUs are encrypted by AD's public key. Anyone, except AD, who possesses the corresponding private key, cannot decrypt the messages. About the message $\mathrm{SK}_X^2||\mathrm{PK}_X^2$ returned by AD, the registrants can obtain offline. Because they only need to be registered one time unless their private keys are compromised. In *Authentication phase*, the ciphertext $\delta = (V_1, V_2, \ldots, V_k, T, C)$ can be calculated to get the information only by SMs. Moreover, only the legal authorized ones can access the public ledger, such as SMs, WPs, and AD. In *Service-Delivery phase*, when the transmitted message $ac_X = \{\mathrm{Sig}_{\mathrm{SK}_X}(\mathrm{pid}_X, tst), \mathrm{pid}_X, tst\}$ is intercepted by an adversary, the adversary can only get the worthless pseudonym pid_X and timestamp tst. Therefore, the proposed mechanism BLA ensures the confidentiality of key information during its entire workflow.

C. Integrity

To achieve the *integrity*, it must be ensured that no adversary can tamper with the transmitted messages or the tampered messages can be discovered in BLA. First, according to CDHP, if given $R, \mathrm{PK}_{\mathrm{SM}_i}^1, \mathrm{PK}_{\mathrm{SM}_i}^2, \mathrm{PK}_{\mathrm{AD}}$, it is difficult for attackers to calculate Y_i. Second, in *Registration phase*, the real identities of SMs and OBUs are encrypted by AD's public key. An adversary does not possess the corresponding private key, and thus the messages cannot be tampered. When the message $\mathrm{SK}_X^2||\mathrm{PK}_X^2$ is returned by AD, the registrants obtain the message offline. An adversary has no opportunity to tamper with it. In *Authentication phase*, if the ciphertext $\delta = (V_1, V_2, \ldots, V_k, T, C)$ is tampered with, each SM cannot calculate the correct information, and the authentication is failed. That is, the tampered message can be discovered. In *Service-Delivery phase*, when the transmitted message $ac_X = \{\mathrm{Sig}_{\mathrm{SK}_X}(\mathrm{pid}_X, tst), \mathrm{pid}_X, tst\}$ is tampered with by an adversary, each SM will not allow an user to access VFS. The vehicle just needs to resend a new access request. However, not only an adversary does not know whose messages are tempered with, but also all the above tampering behaviors will come at a cost and have no benefit for an adversary. Hence, BLA can also ensure the integrity of messages from the viewpoint of game theory.

D. Anonymity

To achieve the anonymity, it must ensure that no adversary can extract real identities when BLA is deployed. First, as mentioned above, BLA can guarantee the confidentiality of the transmitted messages. No real identities can be obtained by an adversary because they are hidden in the encrypted messages. Second, in *Authentication phase*, a vehicle can randomly choose a pseudonym and decide when the pseudonym expires. It grants the responsibility of preserving privacy to users themselves, which is an advantage of BLA. If an driving vehicle wants to change its pseudonym, it just needs to be reauthenticated. What is more, the real identities are written into the public ledger, but only legal authorized entities can access the public ledger. It is difficult for an adversary to get the real identities of vehicles, and the pseudonym of a vehicle can be changed regularly. Thus, the anonymity of the mechanism is guaranteed.

E. Noninteractivity

The description in Section IV-B indicates that each time a vehicle accesses VFS, it only sends one message (authentication request or service access request) to an SM, and has no need to transmit additional messages for accessing services in *Authentication phase* and *Service-Delivery phase*. Thus, BLA is noninteractive.

F. Traceability and Nonrepudiation

AD aims to achieve the traceability goal. When misbehaviors of a vehicle are found and reported, AD will check one public ledger to find out the corresponding real identity of the illegal anonymous vehicle and revoke its public key. Thus, the traceability can be guaranteed. Meanwhile, the real identity of the illegal anonymous vehicle is revealed and then it cannot deny its misbehaviors. Accordingly, the nonrepudiation goal is achieved in BLA.

VI. Performance Evaluation of BLA

This section analyzes the BLA performance by first analyzing the overhead caused by BLA and then simulating the BLA workflow to illustrate that the proposed BLA mechanism is feasible in terms of VFS response time.

A. Overhead of the Proposed Mechanism

This section evaluates the overheads of *Authentication*, *Consensus*, and *Service-Delivery* phases by realistic experiments. Due to the preset of *Initialization phase* and *Registration phase*, their overhead is not in our consideration.

In *Authentication phase*, the operations executed by an OBU can be precomputed before it is authenticated. It is because most of the SM information, including the number of SMs, ID, public key, location, and so on, remains unchanged for a long time. A driving OBU can only be in charge of sending the ciphertext to RSU and accept the VFS. After receiving the message, RSU needs to forward it to SM, which consumes the transmission time. To measure the transmission delay, we use three PC as sender (OBU), transfer (RSU), and receiver (SM), respectively. Their configurations are given in Table III. The protocol we used is IEEE 802.11p and the size of a message is set to 24 bytes. Under the settings, the average transmission time of one message is 2.137 ms. When an SM receives the message, it will authenticate the message. The main two operations in the process are hash functions and point multiplications. The corresponding average time measured through Java Runtime Environment is 0.596 ms and 1.473 ms, respectively. According to the SM workflow in *Authentication phase*, the number of point multiplication operations is $(k+3)$ which is related to the k SMs, and the number of hash functions is five. The time overhead in *Authentication phase* is shown in Table IV, where time overhead $= 1.473(k+3) + 2.98$.

TABLE III
CONFIGURATIONS OF RSU AND SM

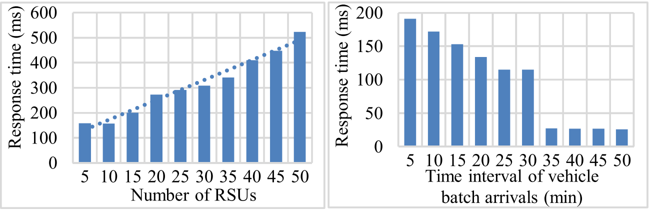
Item	OBU (sender)/RSU (transfer)	SM (receiver)
CPU	Intel(R) Core(TM) i5-2400 CPU at 3.10 GHz	Intel(R) Core(TM) i7-4790 CPU at 3.60 GHz
RAM	4.00 GB	8.00 GB
Operation System	Windows 10 Professional 64-bit version	Windows 7 Ultimate 64-bit version

TABLE IV
TIME OVERHEAD IN *Authentication Phase*

Number of SM	Time Overhead (ms)
$k = 4$	13.291
$k = 7$	17.71
$k = 10$	22.129

TABLE V
TIME OVERHEAD IN *Consensus Phase*

Number of WP	Time Overhead (ms)
4	1.8
7	2.4
10	4.6



(a) (b)

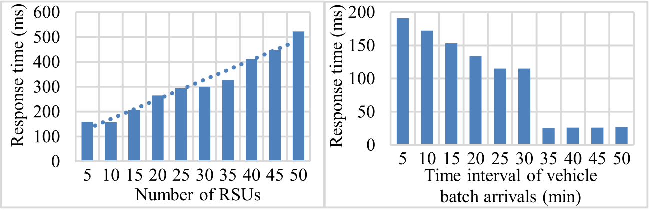
Fig. 3. (a) Average time for authenticating a request with the increasing RSU number under 4 SMs. (b) Average time for authenticating a request with the increasing time interval of vehicle batch arrivals under 4 SMs.

Consensus phase is independent of the authentication and service-delivery workflow. Thus, we evaluate it individually. We set $t = 1$ s for generating a block. The consensus time is measured with 4 WPs, 7 WPs, and 10 WPs, as shown in Table V.

In *Service-Delivery phase*, the time overhead is mainly generated by transmission and data searching. The transmission time refers to the forward time of one message, which is 2.137 ms. The data searching methods we can adopt is a fast searching algorithm, for example, hash search algorithm. Since this paper mainly focuses on the authentication, we do not simulate *Service-Delivery phase* in the following.

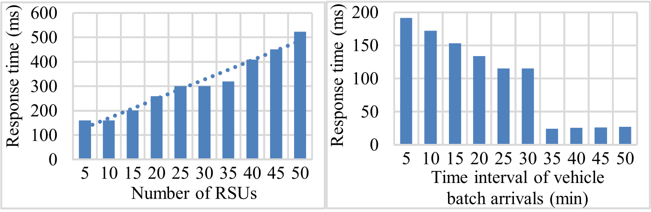
B. Simulations of the Proposed Mechanism

We simulate the BLA workflow with k SMs and m RSUs in the governed range of each SM. The settings are assumed as follows: 1) there are m RSUs in an SM and vehicle batches arrive at the ith RSU ($1 \leq i \leq m$) as Poisson stream with rate λ_i; 2) vehicle batch sizes conform to uniform distribution; 3) the forward time of a batch is the product of 2.137 ms and the number of vehicles in the batch; and 4) the authentication time of a batch is the product of $1.473(k + 3) + 2.98$ ms and the number of vehicles in the batch. With these settings, we conduct the following four groups of simulations and each group includes two sets of simulations.



(a) (b)

Fig. 4. (a) Average time for authenticating a request with the increasing RSU number under 7 SMs. (b) Average time for authenticating a request with the increasing time interval of vehicle batch arrivals under 7 SMs.



(a) (b)

Fig. 5. (a) Average time for authenticating a request with the increasing RSU number under 10 SMs. (b) Average time for authenticating a request with the increasing time interval of vehicle batch arrivals under 10 SMs.

In the first group of simulations with 4 SMs (i.e., $k = 4$), we first set parameters as follows: 1) $m \in [5, 50]$; 2) $1/\lambda_i = 5$ min; 3) batch sizes are uniformly distributed with [1, 100]; and 4) the authentication time of a batch is the product of 13.291 ms (due to $k = 4$) and the number of vehicles in the batch. The results are shown in Fig. 3(a). In the second set of the first group, we set: 1) $m = 5$ and 2) $1/\lambda_i \in [5, 50]$ min; the other parameters are set same as in the first set. The results are shown as Fig. 3(b).

In the second and third groups of simulations, we set the number of SMs is 7 and 10, respectively. The other parameters are same as in the first group of simulations. The results of the second group are shown in Fig. 4(a) and (b). The results of the third group are shown in Fig. 5(a) and (b). In the fourth group of simulations, we compare the average response time in the first three groups under the different numbers of SMs. The results are shown in Fig. 6(a) and (b).

From Figs. 3(a), 4(a), and 5(a), we observe that with the increasing number of RSUs, the average response time for authenticating a request increases. The reason is that the waiting time increases with the increasing number of RSUs. However, Fig. 6(a) depicts that with the increasing number of SMs, the average response time for authenticating a request almost has no change. The reason is that when the number of SMs is 4, 7, and 10, the authentication time is 13.291 ms, 17.71 ms, and 22.129 ms, respectively, among which the disparity is not obvious.

From Figs. 3(b), 4(b), and 5(b), we can get that with the increasing time intervals of vehicle batch arrivals, the average response time for authenticating a request first decreases

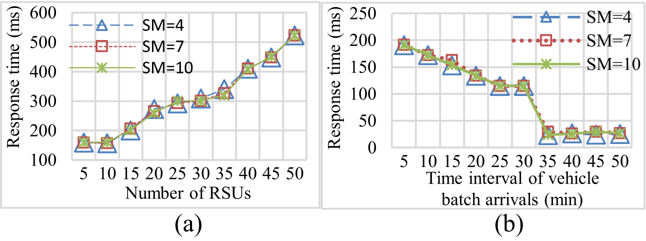


Fig. 6. (a) Comparison of average time for authenticating a request with the increasing number of RSUs under 4, 7, and 10 SMs. (b) Comparison of average time for authenticating a request with the increasing time interval of vehicle batch arrivals under 4, 7, and 10 SMs.

and sudden drops at the 30th min point, then remains almost unchanged. The reason is that with the increasing time intervals of vehicle batch arrivals, the waiting time for authenticating a request becomes shorter and shorter, causing the average response time to decrease gradually. When the time interval of vehicle batch arrivals is 30 min, there is a sudden dropping in the response time. It is because there is no waiting time. When the time interval is longer than 30 min, the average response time is almost unchanged. Fig. 6(b) also depicts that with the increasing number of SMs, the average response time for authenticating a request almost has no change. The reason is same as above.

Fig. 6(a) indicates that, when the number of RSUs is 50, the SM receives 10–1000 authentication requests per minute and the average response time is not more than 450 ms. According to the common knowledge of the biggest speed 120 km/h on a highway, a vehicle can run 30 meters. If the vehicle is on the urban road, it almost can only run the distance of a crossroad. These simulation results indicate that the proposed BLA mechanism is feasible.

VII. Conclusion

In this paper, we propose a BLA mechanism for distributed VFSs with the following advantages: 1) a vehicle itself can decide whether or not to be reauthenticated when entering a new datacenter; 2) vehicles can access VFS anonymously and change their pseudonyms at any time; 3) BLA is noninteractive, significantly reducing communication delay; and 4) blockchain technology is adopted in order to not only effectively defend against the attack of compromising the database governed by a central authority but also reduce user authentication time by eliminating the communication between SMs in the authentication process. BLA's security features are demonstrated through security analysis and its performance is evaluated through extensive simulations. The results show that BLA is practical for VFS in terms of its overhead and security.

This paper only makes an informal security proof of security features of BLA. One future research direction is to explore the combination of the formal and informal security proof to make the security analysis of the mechanism. In addition, we plan to further reduce overhead in *Authentication phase* and *Consensus phase*. Designing a more secure and efficient vehicular service provision mechanism is also being a future research direction.

References

[1] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "On the integration of cloud computing and Internet of Things," in *Proc. IEEE Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2014, pp. 23–30.

[2] M. Shojafar, N. Cordeschi, and E. Baccarelli, "Energy-efficient adaptive resource management for real-time vehicular cloud services," *IEEE Trans. Cloud Comput.*, to be published, doi: 10.1109/TCC.2016.2551747.

[3] X. Hou *et al.*, "Vehicular fog computing: A viewpoint of vehicles as the infrastructures," *IEEE Trans. Veh. Technol.*, vol. 65, no. 6, pp. 3860–3873, Jun. 2016.

[4] V. G. Menon and P. M. J. Prathap, "Moving from vehicular cloud computing to vehicular fog computing: Issues and challenges," *Int. J. Comput. Sci. Eng.*, vol. 9, no. 2, pp. 14–18, 2017.

[5] J. Lin *et al.*, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[6] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sep. 2017.

[7] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, to be published, doi: 10.1109/TITS.2018.2818888.

[8] D. Tapscott and A. Tapscott, "How blockchain will change organizations," *MIT Sloan Manag. Rev.*, vol. 58, no. 2, pp. 10–13, 2017.

[9] Y. Yao, X. Chang, J. Mišić, and V. B. Mišić, "Reliable and secure vehicular fog service provision," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2855718.

[10] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 1015–1028, Apr. 2016.

[11] A. Karati *et al.*, "Provably secure identity-based signcryption scheme for crowdsourced industrial Internet of Things environments," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2904–2914, Aug. 2018.

[12] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 3, pp. 516–526, Mar. 2017.

[13] S. H. Islam *et al.*, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Gener. Comput. Syst.*, vol. 84, pp. 216–227, Jul. 2018.

[14] J. Xu, D. Zhang, L. Liu, and X. Li, "Dynamic authentication for cross-realm SOA-based business processes," *IEEE Trans. Services Comput.*, vol. 5, no. 1, pp. 20–32, Jan./Mar. 2012.

[15] W. Zhang, X. Wang, and M. K. Khan, "A virtual bridge certificate authority-based cross-domain authentication mechanism for distributed collaborative manufacturing systems," *Security Commun. Netw.*, vol. 8, no. 6, pp. 937–951, 2015.

[16] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2590–2601, Dec. 2017.

[17] D. He *et al.*, "A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network," *IEEE Trans. Depend. Secure Comput.*, vol. 15, no. 4, pp. 633–645, Jul./Aug. 2018.

[18] Y. Yang, X. Zheng, X. Liu, S. Zhong, and V. Chang, "Cross-domain dynamic anonymous authenticated group key management with symptom-matching for e-health social system," *Future Gener. Comput. Syst.*, vol. 84, pp. 160–176, Jul. 2018.

[19] Q. Chen, S. Shi, X. Li, C. Qian, and S. Zhong, "SDN-based privacy preserving cross domain routing," *IEEE Trans. Depend. Secure Comput.*, to be published, doi: 10.1109/TDSC.2018.2811807.

[20] Z. Qikun, G. Yong, Z. Quanxin, W. Ruifang, and T. Yu-An, "A dynamic and cross-domain authentication asymmetric group key agreement in telemedicine application," *IEEE Access*, vol. 6, pp. 24064–24074, 2018.

[21] C. Fromknecht, D. Velicanu, and S. Yakoubov, "Certcoin: A namecoin based decentralized authentication system," Massachusetts Inst. Technol., Cambridge, MA, USA, Rep. 6, 2014.

[22] A. Lei *et al.*, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.

[23] W. Wang, N. Hu, and X. Liu, "BlockCAM: A blockchain-based cross-domain authentication model," in *Proc. IEEE 3rd Int. Conf. Data Sci. Cyberspace (DSC)*, Jun. 2018, pp. 896–901.

[24] C. Fu, T. Kezmane, X. Du, Y. Fu, and C. Morrisseau, “An location-aware authentication scheme for cross-domain Internet of Thing systems,” in *Proc. IEEE Int. Conf. Comput. Netw. Commun. (ICNC)*, Mar. 2018, pp. 452–456.

[25] Y. Zhang, X. Lin, and C. Xu, “Blockchain-based secure data provenance for cloud storage,” in *Proc. Int. Conf. Inf. Commun. Security*, Oct. 2018, pp. 3–19.

[26] V. Buterin, *On Public and Private Blockchains*, Ethereum Blog, Aug. 2015. Accessed: Jan. 21, 2019. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[27] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[28] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper 151, pp. 1–32, 2014. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf

[29] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.

[30] Y. Zhang and J. Wen, “An IoT electric business model based on the protocol of bitcoin,” in *Proc. IEEE 18th Int. Conf. Intell. Next Gener. Netw. (ICIN)*, Feb. 2015, pp. 184–191.

[31] T. Hardjono and N. Smith, “Cloud-based commissioning of constrained devices using permissioned blockchains,” in *Proc. 2nd ACM Int. Workshop IoT Privacy Trust Security*, May 2016, pp. 29–36.

[32] Z. Chen, S. Chen, H. Xu, and B. Hu, “A security authentication scheme of 5G ultra-dense network based on block chain,” *IEEE Access*, vol. 6, pp. 55372–55379, 2018.

[33] A. Kiayias, A. Russell, B. David, and R. Oliynykov, “Ouroboros: A provably secure proof-of-stake blockchain protocol,” in *Proc. Annu. Int. Cryptol. Conf.*, Aug. 2017, pp. 357–388.

[34] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain technology: Beyond bitcoin,” *Appl. Innov.*, no. 2, pp. 6–10, Jun. 2016.

Yingying Yao received the B.S. degree in computer science and technology from the Ocean University of China, Qingdao, China, in 2012. She is currently pursuing the Ph.D. degree in cyberspace security at Beijing Jiaotong University, Beijing, China.

Xiaolin Chang (M’12) is a Professor with the School of Computer and Information Technology, Beijing Jiaotong University, Beijing, China. Her current research interests include edge/cloud computing, network security, and security and privacy in machine learning.

Jelena Mišić (M’92–SM’08–F’18) is a Professor of computer science with Ryerson University, Toronto, ON, Canada. She has authored or co-authored over 120 papers in archival journals and close to 200 papers at international conferences in the areas of wireless networks, in particular wireless personal area network and wireless sensor network protocols, performance evaluation, and security.

Ms. Mišić serves on the Editorial Boards of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, *Computer Networks*, *Ad Hoc Networks*, *Security and Communication Networks*, *Ad Hoc & Sensor Wireless Networks*, the *International Journal of Sensor Networks*, and the *International Journal of Telemedicine and Applications*. She is a member of the ACM.

Vojislav B. Mišić (M’92–SM’08) received the Ph.D. degree in computer science from the University of Belgrade, Belgrade, Serbia, in 1993.

He is a Professor of computer science with Ryerson University, Toronto, ON, Canada. He has authored or co-authored six books, 20 book chapters, and over 280 papers in archival journals and at prestigious international conferences. His current research interests include performance evaluation of wireless networks and systems and software engineering.

Dr. Mišić serves on the Editorial Boards of the IEEE TRANSACTIONS ON CLOUD COMPUTING, *Ad Hoc Networks*, *Peer-to-Peer Networks and Applications*, and the *International Journal of Parallel, Emergent and Distributed Systems*. He is a member of the ACM.

Lin Li is currently an Associate Professor with the School of Computer and Information Technology, Beijing Jiaotong University, Beijing, China. Her current research interests include cryptography and privacy preserving.