B-TSCA: Blockchain assisted Trustworthiness Scalable Computation for V2I Authentication in VANETs

Chen Wang, Jian Shen, Jin-Feng Lai, Jianwei Liu

Abstract—The rapid development of 5G networks has made smart driving possible. The vehicular ad-hoc networks (VANETs) are the main environment for smart driving, providing road information, instant communication between vehicle and vehicle (V2V) or vehicle and infrastructure (V2I). The information interaction security of VANETs is critical to the proper functioning of the traffic. Much research in recent years has focused on secure communication in VANETs, especially the secure V2V or V2I communications. However, current security schemes often require complex identity re-authentication when vehicles enter a new infrastructure coverage, which greatly reduces the efficiency of the entire network. In addition, the emergence of blockchain has created opportunities to overcome the challenges in VANETs mentioned above. In this paper, blockchain is utilized to enhance the scalability of the trustworthiness scalable computation. The proposed blockchain assisted trustworthiness scalable computation based V2I authentication (B-TSCA) scheme achieves rapid re-authentication of vehicles through secure ownership transfer between infrastructures. Note that, trustworthiness scalable computation assisted by blockchian technology ensures the decentralization and non tamperability of the scalable computation result. The security analysis indicates that B-TSCA scheme is a CDH-secure scheme. The time cost of the novel handover authentication phase is half of that of the initial one as is presented in the simulation.

Index Terms—Trustworthiness scalable computation, blockchain, V2I authentication, VANETs.

1 Introduction

The development of the next generation networks push the researches of intelligent transportation. Vehicular ad hoc networks (VANETs) are the most considered network model for an intelligent transportation system. The decentralization, heterogeneity and nontrustworthiness of VANETs pose the challenges in secure message-transmission and transaction-execution [1], [2]. Advanced technologies such as cloud computing, smart chips, blockchain, etc., promote the development of VANETs [3], [4], [5]. Integrating blockchains with VANETs can provide solutions to some existing challenges. The establishment of VANETs can greatly promote breakthroughs in applications such as driverless and intelligent road rescue. Traffic safety and efficiency are constantly being optimized due to the extensive research of VANETs. The complex VANETs require the data transmission schemes to be extremely scalable. Hence, scalable computation is an important part of advancing VANETs technology. Furthermore, the increasing data scale of Internet of Things (IoT) and new trends in data applications have spurred the growing demand for scalable computation in new networks [6], [7]. In traffic networks, vehicles collect and upload their own attribute data or surrounding road condition information monitored by on-board units (OBUs) [8], [9]. Meanwhile, roadside infrastructure and remote servers can collect and analyze uploaded information. As a result, according to the analysis results, the traffic control center formulates the optimal traffic flow management strategy and emergency response method [10], [11].

The appearance of blockchain provides a solution for VANETs to solve the problems of trustworthiness scalable computation [12], [13]. A specific VANET integrated with blockchain, as illustrated by Fig. 1, is generally composed of three main bodies: vehicle units, roadside infrastructure and the blockchain maintained by the infrastructure. In detail, vehicle units mainly refer to various types of vehicles, on which OBUs such as sensor nodes are deployed to collect vehicle attribute parameters and road condition information around the vehicle [14]. Roadside infrastructure generally refers to roadside units (RSUs) that are utilized as relay nodes for communications. The blockchain is utilized to record the attributes and trustworthiness of the vehicles in the network. Note here that, Trustworthiness is an important reference for the reliability of the network. Trustworthiness scalable computation can help the system evaluate the trustworthiness of a changing vehicle. Simultaneously, the secure release of the traffic control information from the remote server can also be guaranteed. Without the intervention of a trusted third party, blockchains enable the trustworthiness be computed and be validated in a mutually distrusted system with a decentralized consensus. Various types of communication relationship are involved in

- *C. Wang and J. Shen are with the School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, China and the Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen 518000, China. E-mail: {wangchennuist, s_shen}@126.com*
- *J-F. Lai is with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China. E-mail: lcf2018@uestc.edu.cn*
- *J. Liu is with the School of Cyber Science and Technology, Beihang University, Beijing 100191, China. E-mail: liujianwei@buaa.edu.cn*

Manuscript received XXX XX, 20XX; revised XXX XX, 20XX.

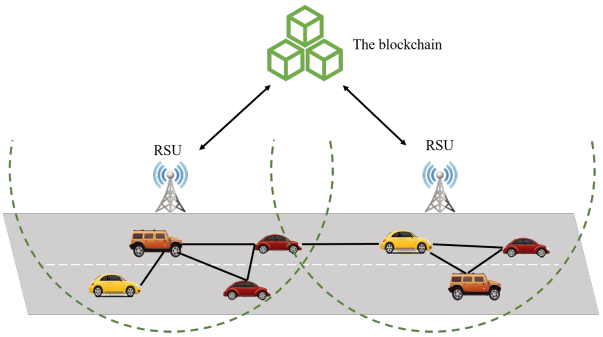

Fig. 1: The illustration of VANETs integrated with blockchain

VANETs [15], [16]. Vehicles in the network can communicate with each other, which is referred to as the vehicle-to-vehicle (V2V) communication. Additionally, roadside infrastructure also communicates with vehicles, known as the vehicle-to-infrastructure (V2I) communication. The security of these communications has been widely concerned and studied. Secure V2I communication can provide a channel for uploading vehicle attribute parameters and their surrounding road condition information. On account of the authentication of vehicles to be contacted with, the trustworthiness of a vehicle needs to be evaluated from time to time according to the uploaded attributes. The trustworthiness of a vehicle plays a crucial role in VANETs. The trustworthiness comes primarily from the evaluation of all aspects of the vehicle attributes collected by OBUs. What's more, the scalable computing ability is especially critical for trustworthiness computation.

1.1 Motivation:

As we all know, every terminal in VANETs may suffer from all kinds of malicious attacks, which brings great difficulties to the practical application of intelligent VANET protocols. V2I communication is an important part of VANETs, which can not be ignored. Most schemes nowadays designed for V2I communication require the vehicles to re-authenticate with every RSU when they join in the ranges of different RSUs. However, although these authentication methods can authenticate the identity of the vehicle every time, they also bring about problems such as large communication overhead and redundant operation. In most of the up-to-date research, every time a vehicle enters a new RSU coverage area, it needs to re-authenticate with the new RSU, which leads to a lot of unnecessary overhead and reduces the efficiency of the vehicle network. Due to the rapid change of the network topology, excessive delay cannot be tolerated. Thus, it is necessary to reduce the redundancy caused by repeated authentication, so as to reduce the computing burden of vehicles and the network time delay. Additionally, it is challenging to assure the trustworthiness in decentralized nontrusted VANETs and restrict the misbehaving vehicles [17]. Moreover, there is a lack of scalability in the computation of vehicle trustworthiness, which leads to the inability to adapt to the changing needs of vehicle networks.

Our contributions: In this paper, a possible solution to the above problem is presented. The novel scheme is named as a blockchain assisted trustworthiness scalable computation based V2I authentication (B-TSCA) scheme. The contributions of this paper can be described as follows:

- **Blockchain based tamper-resistant and traceable vehicle attribute record is designed.** Tamper-resistance and traceability of the vehicle attributes are two essential properties of vehicle authentication in VANETs. In this paper, the proposal integrates blockchain for the record of the vehicle attributes and trustworthiness. The blockchain makes the provided services tamper-resistant and traceable. Changes in vehicle attributes are taken as data changes in Bitcoin transactions. The tamper-resistance ensures that the attributes of the vehicle cannot be arbitrarily falsified, thus ensuring the reliability of trustworthiness computation. Traceability ensures that the trustworthiness of the vehicle at any time can be queried, and a more reliable reference to the trustworthiness computation can be obtained by analyzing historical data.
- **A novel scalable computation system is presented for trustworthiness evaluation.** Trustworthiness computation ensures the reliability of the authenticated vehicle. In VANETs, the scalability of trustworthiness computation is very important, because the performance, number and relationship of vehicles in the network change at any time. These changes need to be recorded in real time for analysis of the vehicle reliability. In this paper, we present a blockchian assisted trustworthiness scalable computation system. As the miner in the system, RSUs implement the validation of the trustworthiness level through the consensus mechanism. The system utilize Merkle hash tree (MHT) to realize real-time recording of vehicle attributes. The record can be extended for new vehicles, different vehicle models and other new changes in the network, which greatly increases the practicability of the system.
- **A time-efficient V2I-handover authentication scheme is proposed.** For the new vehicles entering the network, this paper gives a detailed initial authentication phase. This phase first combines the blockchain-assisted trustworthiness scalable computation, and utilizes the queried trustworthiness value to check the reliability of the vehicle. The initial phase enables the authentication of a new vehicle with low client computing overhead. With this authentication, roadside infrastructure is able to fully confirm the legality of the vehicle. What's more, an additional handover phase is designed for the following authentication of a vehicle when it is already a legal member of the network by the initial authentication. Some handover message and a token are utilized to simplify this handover authentication phase and save time on calculations in subsequent vehicle authentication processes. The design of the handover phase makes it convenient and secure for the ownership of a vehicle to be transfered between different RSUs, which makes the network more scalable.

1.2 Related Work

VANET authentication has generated considerable recent research interest. In particular, some researchers have made efforts and produced some results in the trustworthiness scalable computation of VANETs. In addition, blockchains are also widely utilized in the integration of new technologies in VANETs.

Some researchers put forward solutions for the privacy protection of vehicles. Huang *et. al.* [18] presented a pseudonymous authentication scheme for conditional privacy in VANETs. The scheme can provide vehicle anonymity and revocation. However, an off-road unit was utilized to achieve motor vehicles division which might lead to an additional computing overhead. Horng *et. al.* [19] also proposed a secure and privacy enhancing communication schemes for vehicle-to-vehicle communications which can resist impersonation attack. Roadside infrastructure RSUs were utilized to collect messages from vehicles in their scheme, while V2I communications were not considered. Zhong *et. al.* [20] presented a privacy-preserving authentication scheme with full aggregation in VANETs using certificateless aggregate signature to achieve secure vehicle-to-infrastructure (V2I) communications.

Some researchers achieved authentication with signature. Biswas *et. al.* [21] verified messages of each vehicle according to medium access control (MAC) layer priorities and the application relevance of individual safety messages. A cross-layer privacy-preserving authentication scheme was proposed for OBUs and RSUs. However, the scheme was proven to be insecure against secret key recovery attacks [22]. Shim pointed out that in this scheme anyone can recover OBUs' or mobile nodes' private keys from transmitted signed messages just eavesdropping in the scheme. After that, Cui *et. al.* [23] proposed a self-healing key distribution method with a certificateless signature in VANETs.

Batch authentication is also an important research topic for group verification in VANETs. Shao *et. al.* [24] proposed a group authentication scheme for both V2V and V2I authentication in VANETs, which is actually a signature scheme providing no message encryption. Jiang *et. al.* [25] achieved batch authentication by calculating the hash message authentication code. Cuckoo filter and the binary search methods were utilized in [26] and was claimed to achieve high success rate in the batch verification phase.

Road condition monitoring is one of the main purposes of the development of VANETs. Wang *et. al.* [27] presented a source authentication scheme for road condition monitoring associated by cloud computing technology. Multi-keys were utilized in authentication scheme proposed in [28] to achieve location based services in VANETs.

In addition, researchers have proposed some schemes for the application of blockchain for trustworthiness computation in VANETs. For instance, Yang *et. al.* [29] developed a trust-management platform in VANETs on top of blockchains. The trustworthiness of messages can be validated via proof of work (PoW) and proof of stake (PoS) consensus executed by RSUs. Lu *et. al.* [30] presented a blockchain-based trust management scheme for VANETs. The scheme is utilized to break the linkability between the real ID and the public key.

However, the excising research has not paid much attention to the authentication when the vehicle travels from one RSU coverage to the next. Simultaneously, the attribute parameters of vehicles are not fully utilized to compute the trustworthiness of a vehicle, so as to improve the reliability and scalability of VANETs.

1.3 Organization

The remainder of this paper is organized as follows. Section 2 presents some preliminaries of this paper, including bilinear pairing and the computational Diffie-Hellman assumption. Section 3 presents the system model and the security model of this paper. Section 4 introduces the blockchain assisted trustworthiness scalable computation in detail. Section 5 puts forward the proposed B-TSCA scheme. Section 6 presents the security analysis. Section 7 shows the performance analysis according to some simulations. Finally, the conclusion is drawn in Section 8.

2 Preliminaries

In this section, some necessary preliminaries, such as bilinear pairing and computational Diffie-Hellman assumption are listed.

2.1 Bilinear Pairing

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two groups of the same prime order q. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two multiplicatively written group. Given a mapping e, a bilinear pairing on $(\mathbb{G}_1, \mathbb{G}_2)$: $\mathbb{G}_1^2 \to \mathbb{G}_2$ satisfying the following properties is called a cryptographic bilinear map.

Bilinearity. $e\left(h^a, g^b\right) = e\left(h, g\right)^{ab}$ for all $h, g \in \mathbb{G}_1$ and $a, b \in Z_q^*$.

Non-degeneracy. If P is a generator of $\mathbb{G}_1$, then $e(g, g)$ is a generator of $\mathbb{G}_2$. In other words, $e(g, g) \neq 1$.

Computability. e can be efficiently computed.

2.2 Computational Diffie-Hellman (CDH) Assumption

CDH problem, which is detailedly defined in Definition. 1, is considered in this paper.

Definition 1 (CDH Problem in $\mathbb{G}$). The computational Diffie-Hellman problem (CDH Problem) in a multiplicative group $\mathbb{G}$ and g is the generator of $\mathbb{G}$. The problem is that compute g^{ab} only with $g, g^a, g^b \in \mathbb{G}$, where $a, b \in \mathbb{Z}$.

Definition 2 (DDH Problem in $\mathbb{G}$). The decisional Diffie-Hellman problem (DDH Problem) in a multiplicative group $\mathbb{G}$ and g is the generator of $\mathbb{G}$. The problem is that decide if $g^{ab} = g^c$ only with $g, g^a, g^b, g^c \in \mathbb{G}$, where $a, b, c \in \mathbb{Z}$.

Definition 3 (CDH-Security in $\mathbb{G}$). A scheme is considered CDH-Secure in $\mathbb{G}$ when it satisfy the following definition: any probabilistic polynomial time adversary (PPTA) who cannot solve CDH problem with a non-negligible probability has negligible chance to obtain the secret value of the protocol in $\mathbb{G}$.

To sum up, the proposed scheme is considered to achieve CDH-security in $\mathbb{G}$, as long as the calculation of the session key for a forged vehicle in our scheme is at least as hard as the CDH problem.

3 System Model and Security Model

The system model and security model of this paper are described in this section.

3.1 System Model

The system is composed of two main parts: the trustworthiness scalable computation part and the network authentication part. Vehicles and RSUs play different roles in the two parts. A vehicle will pass through the coverage of different RSUs while driving on the road. It needs to continuously authenticate with these RSUs to enter the network and participate in message interaction. An RSU needs to be responsible for the identity authentication of all vehicles entering its signal coverage range and the information interaction with legal vehicles.

In the trustworthiness scalable computation part, vehicles are considered as the uploader of attributes collected by the OBUs on the vehicle, while RSUs take the responsibility of evaluating the vehicles and recording the results into the blockchain.

In the network authentication part, vehicles need to apply to join the jurisdiction of an RSU, which is responsible for judging whether the vehicle is qualified to enter the network within its coverage. Certified vehicles will be utilized for aggregation and delivery of traffic condition, and will receive real-time information feedback from RSUs.

In detail, the components of this system are listed as follows:

- **Key generation system**: The key generation system (KGC) is a trusted component for key generation and distribution.
- **The blockchain**: The blockchain in this system is utilized to record the attributes and trustworthiness of vehicles. These information are very important references for the vehicle authentication.
- **Roadside units**: Roadside units (RSUs) are responsible for collecting vehicle attribute information and conducting trustworthiness scalable computation on vehicles, and maintaining the trustworthiness blockchain. In addition, a RSU is also responsible for authenticating the identity of a vehicle. If a vehicle have not been authenticated in the network, the RSU needs to initially authenticate it. If a vehicle drives into the area of this RSU after exiting from the previous RSU, the RSU shall carry out the handover authentication for it with the help of the information of the previous RSU.
- **Vehicles**: A vehicle is equipped with a large number of sensor nodes, which are called on-board units (OBUs). OBUs collect the real attribute information of the vehicle and send the information to the nearby RSUs. When the vehicle enters the coverage of an RSU, it needs to carry out initial authentication or handover authentication with the RSU, by using some original parameters distributed by KGC to itself and authentication parameters or tokens sent from the RSU.

3.2 Security Model

The security model of this paper is presented in this section. Note that, the RSU is considered as a trusted terminal in our scheme.

3.2.1 A Forged Vehicle

There are two types of forged vehicle in this paper: one is a forged newcomer and the other one is a forged handover vehicle.

An adversary $\mathcal{A}$, who has forged a vehicle which is going to join in the network, wants to be authenticated as a legal vehicle by the RSU. In our assumption, $\mathcal{A}$ can read the storage of the forged vehicle and obtain the session key SK_1 which has been generated by the vehicle with the public key of the RSU and his own secret key. $\mathcal{A}$ also can receive the parameters and timestamps sent by the RSU.

An adversary $\mathcal{A}$, who has forged a vehicle which is going to join in the region of the next RSU, wants to be authenticated by the next RSU. In our assumption, $\mathcal{A}$ has the ability to get the former session key generated by the vehicle with the parameters sent by the former RSu. $\mathcal{A}$ also can receive parameters and timestamps sent by the former RSU and the token sent by the next RSU.

3.2.2 Man-in-the-Middle Attack

Man-in-the-Middle (MITM) attack refers to the attack that the attacker intercepts and attempted to tamper with the message. This kind of attack will cause the original information to be changed. We assume that an MITM attacker have the ability to block the message and implement all necessary calculations.

3.2.3 Reply Attack

Replay attack means that the attacker collects authentication messages sent before from the vehicle and to the RSU, trying to pass the authentication by RSU. A message that has been authenticated is utilized in this kind of attack. An old authentication message might be abused by malicious users to achieve their goals.

4 Blockchain assisted Trustworthiness Scalable Computation

In this section, the blockchain assisted trustworthiness scalable computation is presented, which will be utilized in the proposed authentication scheme for region access control and vehicle authentication [31]. Based on the characteristics of blockchain, such as tamper-resistance and traceability, a blockchain assisted trustworthiness scalable computation system is designed. In this system, RSU is regarded as the hub of trustworthiness scalable computation, mining the attribute data of vehicles to realize the real-time scalable computation of vehicle trustworthiness. With the consensus mechanism, the reliability of vehicles is guaranteed to be unified in the whole network in real time. Each RSU can find the trustworthiness value of any vehicle in the blockchain to determine whether the vehicle meets the requirements of information access in the region. The trustworthiness is also utilized to assist the realization of identity authentication. With the aid of the blockchain, the vehicle trustworthiness computation will be more scalable.

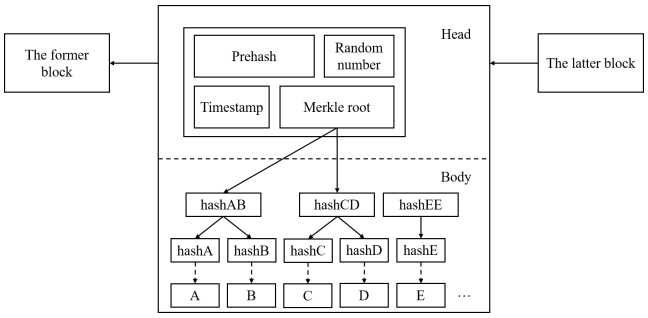

Fig. 2: The structure of blocks

4.1 The Concept of Blockchain

Blockchain is a decentralized distributed accounting system. The advantage of blockchain is that it can deal with issues such as personal trustworthiness record in network with very low cost. Peer-to-peer (P2P) interaction is utilized to avoid the traditional centralized structure. Blockchain applies cryptography technology, timestamp and consensus algorithm to ensure the consistency of information in each node database, so that records can be instantly verified, transparent and traceable, undeniable and difficult to tamper.

Hash functions are mainly utilized for data integrity preserving, data encryption, consensus calculation for workload proof, block linkage, etc. Hash functions such as SHA256 and RIPEMD160 are widely used in blockchain. SHA256 is mainly used to encrypt transactions and form blocks, while RIPEMD160 is used to generate bitcoin addresses. Fig. 2 indicates the application of hash function being hash pointers for block linkage. Merkle hash tree (MHT), which is similar to that mentioned in data structure, is widely utilized in blockchain. A binary tree is usually applied in blockchain. The hash values of information are stored in the nodes. Each transaction record is calculated as a hash value and be stored as a leaf node in MHT. Then, two leaf nodes are hashed in pairs and stored in the block until the last hash value is taken as the Merkle root. As is shown in Fig. 2, the node hashAB's value is the hash of two leaf nodes hashA and hashB. When there is only one leaf node like hashE, the system will consider it as two same leaf nodes, and use the above method to calculate hashEE.

4.2 Details of Blockchain Assisted Trustworthiness Scalable Computation

The trustworthiness scalable computation system utilized in this paper is assisted by blockchain.

Consider a typical VANET, there are vehicles and roadside infrastructure RSUs communicating with each other. Every moment, each vehicle node belongs to a unique RSU, and each RSU is responsible for the scalable computation of the trustworthiness value of multiple vehicle nodes. A single RSU is responsible for mining the attribute information of vehicles within its jurisdiction, evaluating it, and entering the evaluated vehicle trustworthiness value into the blockchain ledger.

The trustworthiness scalable computation method for vehicles is first mentioned in [32]. Two definitions are defined well: trustworthiness attribute information (TAI) and trustworthiness level (TL).

Definition 4 provides the meaning of TAI.

Definition 4 (Trustworthiness attribute information, TAI). TAI is a collection of various attribute parameters reflecting the attributes of a vehicle. Set $\mathfrak{A} = \{\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, ...\mathfrak{a}_m\}$, where $\mathfrak{A}$ represents the set of TAI, and $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, ...\mathfrak{a}_m$ denote different parameters collected by m On Board Units (OBUs).

These messages are collected by OBUs and sent to the RSU. TAI increases the scalability of the trustworthiness computation data source. The RSU will calculate the vehicle trustworthiness level (TL) according to TAI. The definition of TL is presented in Definition 5.

Definition 5 (Trustworthiness level, TL). The TL of a vehicle is an scalable computation standard shared among RSUs, calculated according to the TAI collected from that vehicle.

The TL value is denoted as $\mathfrak{C}$. Eq. (1) provides the instantaneous TL value $\mathfrak{C}^{inst}(t)$ of a vehicle at time t.

$$\mathfrak{C}^{inst}(t) = \frac{\sum_{i=1}^{m} \mathfrak{w}_i \mathfrak{a}_i}{m} \tag{1}$$

where $\mathfrak{w}_i$ is the weight of the i-th TAI, which should be carefully selected so that each parameter change can be reflected in the TL value. Additionally, $\mathfrak{C}^{inst}(t)$ is the weighted mean of the m attributes contained in $\mathfrak{A}$.

Trustworthiness scalable computation is adjusted dynamically over time based on the up-to-date status of the vehicle. The integrated TL value $\mathfrak{C}(t)$ at the end of a time period t is formulated in Eq. (2). $\mathfrak{C}(t)$ is the weighted sum of the instantaneous TL value $\mathfrak{C}^{inst}(t)$ and the last integrated TL value $\mathfrak{C}(t^-)$ recorded in the blockchain at time t^-.

$$\mathfrak{C}(t) = \left(1 - \frac{\delta}{\theta \cdot (1 + \Delta t)}\right) \cdot \mathfrak{C}^{inst}(t) + \frac{\delta}{\theta \cdot (1 + \Delta t)} \cdot \mathfrak{C}(t^-) \tag{2}$$

where δ indicates that the previous TL value $\mathfrak{C}(t^-)$ should be accounted for. Δt is the time interval between time t and time t^-. θ is utilized to control the annealing speed of the previous TL value. The final scalable computation results will be recorded in the blockchain by RSUs. Any legitimate user in the network can search for the data at any time.

Here gives an instance of the proposed blockchian assisted trustworthiness scalable computation as is shown in Fig. 3. The RSUs in the scheme help the blockchain to update and record the trustworthiness of a vehicle. The newly added TL_n means the trustworthiness level at timestamp n. The RSU help the system to calculate the trustworthiness of the vehicle at this time and added it in to the blockchain. Then, the blockchain calculate the block informationaccording to the historical trustworthiness and the newly added one. Finally, these values are recored in the blockchain for inquiry of all the RSUs in the network. The entire computation is mainly divided into the following five steps:

- **TAI generation**: The OBUs on the vehicle generate TAI (which is defined in Definition. 4). Changes in

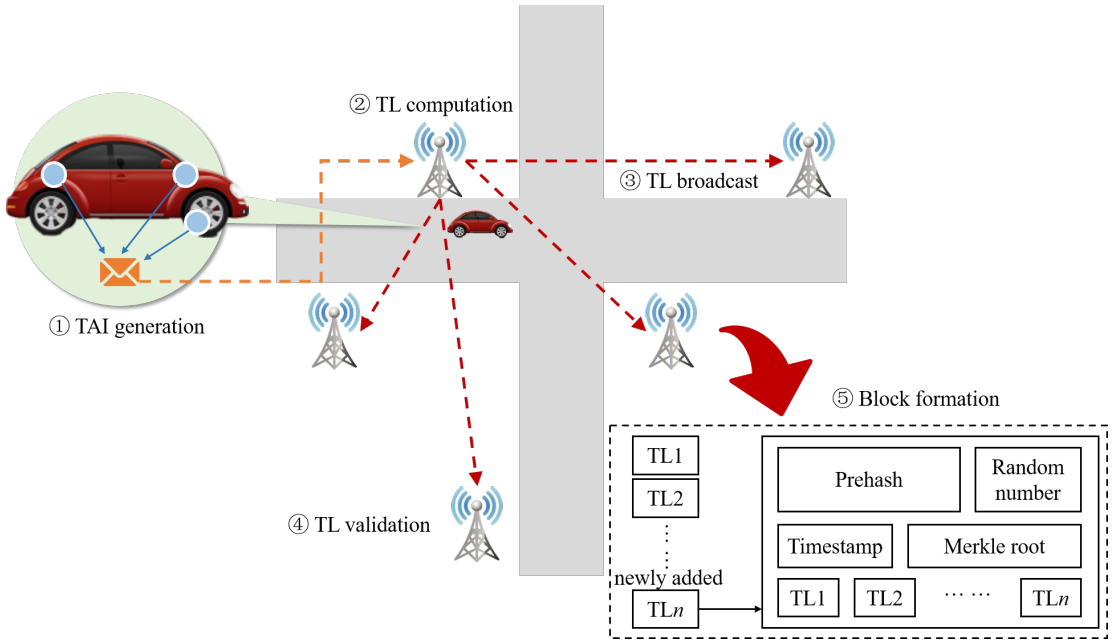

Fig. 3: An instance of the proposed blockchian assisted trustworthiness scalable computation

these attributes are reflected by the Bitcoin wallet to the roadside equipment.

- **TL computation**: When the TAI is transmitted to the nearest RSU, the RSU knows the identity of the vehicle, the number of the node, and the specific changes in the vehicle properties. The RSU then computes the TL value of the vehicle based on the TAI (which is defined in Definition. 5).
- **TL broadcast**: Not only the TL but also the TAI are broadcast to other RSUs in the network.
- **TL validation**: All RSUs are committed to solving this puzzle after receiving the broadcast. A validated TL is then appended to the end of the chain consequently forming a new block in the blockchain once a miner successfully solves the puzzle.
- **Block formation**: Finally, every node saves a replica of the updated blockchain when the validated TL is appended to the blockchain.

5 Our Proposed Scheme

In this section, the proposed time-efficient V2I authentication scheme is detailedly described. Table. 1 lists the frequently used notations in our scheme.

5.1 Overview of Our Scheme

In view of the problem of secure handover of vehicles between two adjacent RSUs, we propose a trustworthiness-based time-efficient V2I authentication scheme. Fig. 4 depicts the application scenario of the proposed scheme. The general process of the scheme is as follows. First, based on the current trustworthiness level of the vehicle, the RSU and the vehicle complete the authentication and generate a initial session key. Then, when the RSU communication range to which the vehicle belongs changes, the previous RSU sends a handover certificate (OC) to the next RSU and the vehicle, and the latter RSU sends a token to the vehicle. Finally, the vehicle resumes communication with the roadside infrastructure after the vehicle and the latter RSU simultaneously calculate the corresponding session key. Note here that, when the vehicle enter the cover range of the next RSU. The RSU only needs to check whether the trustworthiness of the vehicle is changed or not.

TABLE 1: Notations in our scheme

Symbol	Description
$\mathbb{G}, \mathbb{G}_T$	Cyclic groups with bilinear paring $\hat{e}: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
g, h	Generators of $\mathbb{G}$
$\mathfrak{C}$	The trustworthiness level (TL) value
$\mathfrak{C}(t)$	The instantaneous TL value of a vehicle at time t
H_1, H_2, H_3	Cryptographic hash functions
$PKI_(i,1)$	Public key part 1 of the i-th infrastructure
$PKI_(i,2)$	Public key part 2 of the i-th infrastructure
$PK_(v,1)$	Public key part 1 of the v-th vehicle
$PK_(v,2)$	Public key part 2 of the v-th vehicle
a_i	Private key of the i-th infrastructure
u	Private key of the vehicle
r_i	Random value chosen from Z_p^*
SK_x, SK_x^*	Partial secret keys
SK, SK^*	Session keys

5.2 Setup Phase

The setup phase aims to generate public and private key pairs for vehicles and roadside infrastructures. The key generation center (KGC) generates a bilinear paring $\hat{e}: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, where $\mathbb{G}$ and $\mathbb{G}_T$ are two cyclic groups with order p satisfying the mapping relation. Hash functions H_1, H_2, H_3 are chosen as: $H_1: \mathbb{G} \rightarrow \{0,1\}^*$, $H_2, H_3: \{0,1\}^* \rightarrow Z_p^*$ Besides, g and h are two different generators in the group $\mathbb{G}$. $a_i, a_{i+1}, \cdots$ are randomly chosen from non-zero integer group Z_p^* with prime order p for roadside infrastructure $\text{RSU}_i, \text{RSU}_{i+1}, \cdots$.

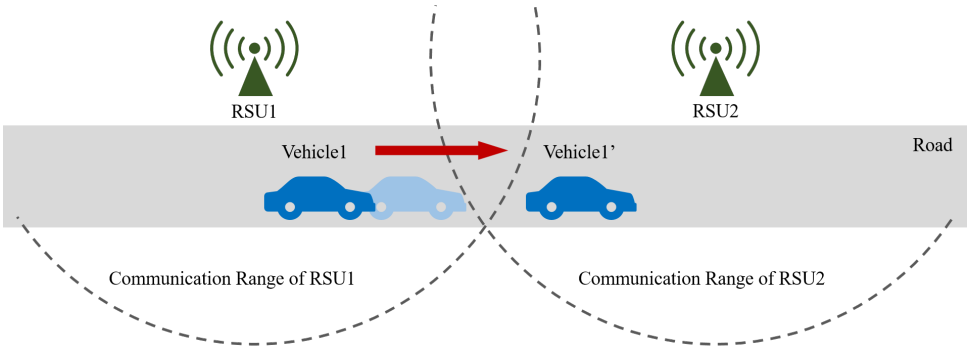

Fig. 4: Description of the proposed scheme

5.3 V2I-Initial Authentication Phase

The second phase of the proposed scheme is named as V2I-initial authentication phase. The TL value generated by the trustworthiness scalable computation system is utilized in this phase. This phase aims to help an RSU authenticate a vehicle's identity when the vehicle participate in the network under the signal coverage of the RSU and generate a session key for the RSU and this vehicle. This phase is composed of three phases: **PreKeyGen**, **VehiSKGen** and **RSUSKGen**.

PreKeyGen: The RSU and the vehicle generate a Diffie-Hellman secret key with each other's public key, respectively. RSU_i calculates $SK_1 = (PK_{v,1})^{a_i}$ and the vehicle calculates $SK_1 = (PKI_{i,1})^{u}$, where a_i and u are the private key of RSU_i and the vehicle. Then, RSU_i chooses $r_i \in Z_p^*$. $R_{i,1} = g^{r_i}$ is calculated and kept secret by RSU_i. $R_{i,2} = h^{r_i}$is then calculated and sent to the vehicle together with a timestamp T_1 recored before sending the message.

VehiSKGen: In this algorithm, the vehicle check the timestamp T_i from RSU_i. Then, the vehicle calculates SK_2:

$$SK_2 = R_{i,2} \cdot PKI_{i,2}^{uH_2(ID||T_1||(T_1)\mathfrak{C}(T_1)||H_1(SK_1))}, \quad (3)$$

where $R_{i,2}$ is the message sent by RSU_i, ID denotes the unique identity number of the vehicle, $\mathfrak{C}(T_1)$ represents the trustworthiness level of the vehicle at time T_1.

Finally, the vehicle computes the session key SK:

$$SK = \hat{e}(SK_2, g). \quad (4)$$

RSUSKGen: RSU_i calculates SK_3:

$$SK_3 = R_{i,1} \cdot SK_1^{H_2(ID||T_1||\mathfrak{C}(T_1)||H_1(SK_1))}, \quad (5)$$

where $R_{i,1}$ is the secret message computed by himself, ID denotes the unique identity number of the vehicle, $\mathfrak{C}(T_1)$ represents the trustworthiness level of the vehicle at time T_1.The TL value is generated by the trustworthiness scalable computation system. If the instant trustworthiness of the vehicle is recorded as 0, the RSU will consider the vehicle as a revoke one and refuse to provide services. Due to the tamer-resistance of blockchain, a revoked vehicle cannot be disguised as a normal vehicle and exchange data with the RSU.

Finally, RSU_i computes the session key SK:

$$SK = \hat{e}(h, SK_3). \quad (6)$$

5.4 V2I-Handover Authentication Phase

The third phase of the proposed scheme is named as the V2I-handover authentication phase. When a vehicle exits the signal coverage of the previous RSU and enters the coverage of the next RSU, the system performs this phase to hand over the communication between the vehicle and the infrastructure to the next RSU. The RSU first inquires the blockchain for the trustworthiness of the vehicle. If the trustworthiness of the vehicle has not changed during the period from the beginning of its acceptance of the last RSU authentication to the current time, the current RSU has no need to authenticate the trustworthiness again. Then, the following steps will be implemented.

OCGen: This algorithm is performed by RSU_i to generate handover certificate (OC) to RSU_{i+1} and the vehicle. RSU_i chooses a random number $r \in Z_p^*$. OC_1 is computed as:

$$OC_1 = SK_1^{rH_3(SK)}, \quad (7)$$

where SK_1 is calculated in the algorithm PreKeyGen and SK is the session key generated in the algorithm RSUSKGen. OC_1 is sent to next infrastructure RSU_{i+1}. Then, OC_2 is computed as:

$$OC_2 = PKI_{i+1,2}^{a_i r}, \quad (8)$$

where $PKI_{i+1,2}$ is the part of the public key of RSU_{i+1} generated in the setup phase. OC_2 is sent to the vehicle.

TokenGen: When received OC_1 from RSU_i, a random value r_{i+1} is chosen from Z_p^*. $R_{i+1,1} = g^{r_i+1}$ is calculated and kept secret by RSU_{i+1}. $R_{i+1,2} = h^{r_i+1}$ is treated as a token and sent to the vehicle.

VehiSKGen2: When the vehicle receives the token from RSU_{i+1} and OC_2 from RSU_i, he computes SK_1^* and SK_2^* as follows:

$$SK_1^* = OC_2^{uH_3(SK)}, \quad (9)$$

$$SK_2^* = R_{i+1,2} \cdot SK_1^*, \quad (10)$$

where $R_{i+1,2}$ is the token.

Finally, SK^* of the vehicle is calculated as:

$$SK^* = \hat{e}(SK_2^*, g). \quad (11)$$

RSUSKGen2: RSU_{i+1} also computes SK_1^* and SK_3^* as follows:

$$SK_1^* = OC_1^{a_{i+1}}, \quad (12)$$

$$SK_3^* = R_{i+1,1} \cdot SK_1^*. \quad (13)$$

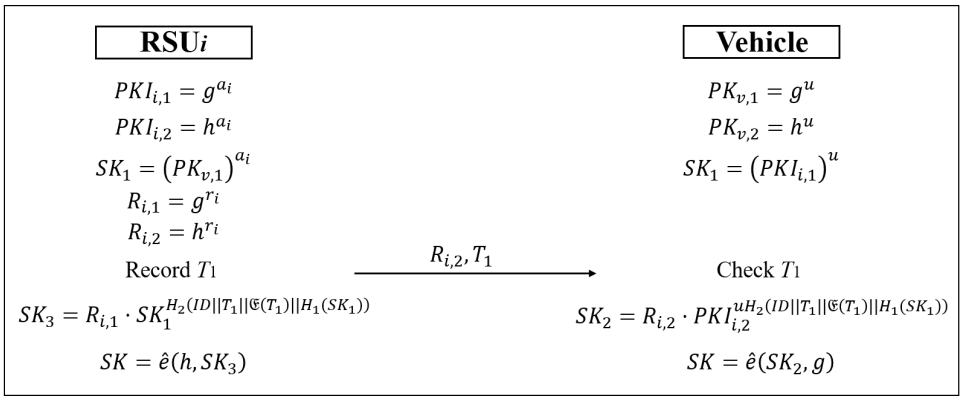

Fig. 5: V2I-initial authentication phase

Finally, SK^* of RSU$_{i+1}$ is calculated as:

$$SK^* = \hat{e}\left(h, SK_3^*\right). \tag{14}$$

6 Security Analysis

This section analysis the correctness and other security performance of the novel scheme.

6.1 Correctness

1. **Correctness of V2I-initial authentication phase**. In this phase, the session keys separately computed by the RSU and the vehicle need to be the same. The session key generated by the vehicle is $SK = \hat{e}\left(SK_2, g\right)$ and the one generated by the RSU is $SK = \hat{e}\left(h, SK_3\right)$. The proof is provided as follows:

$$\begin{aligned} SK &= \hat{e}\left(SK_2, g\right) \\ &= \hat{e}\left(R_{i,2} \cdot PKI_{i,2}^{uH_2(ID||T_1||(T_1)\mathfrak{C}(T_1)||H_1(SK_1))}, g\right) \\ &= \hat{e}\left(h^{r_i} \cdot h^{a_i u H_2(ID||T_1||(T_1)\mathfrak{C}(T_1)||H_1(SK_1))}, g\right) \\ &= \hat{e}\left(h, g^{r_i} \cdot g^{a_i u H_2(ID||T_1||(T_1)\mathfrak{C}(T_1)||H_1(SK_1))}\right) \\ &= \hat{e}\left(h, R_{i,1} \cdot {SK_1}^{H_2(ID||T_1||(T_1)\mathfrak{C}(T_1)||H_1(SK_1))}\right) \\ &= \hat{e}\left(h, SK_3\right) \end{aligned}$$

The correctness of this phase is proved.

2. **Correctness of V2I-handover authentication phase**. In this phase, the session keys separately computed by the next RSU and the vehicle need to be the same. The session key generated by the vehicle is $SK^* = \hat{e}\left(SK_2^*, g\right)$ and the one generated by the RSU is $SK^* = \hat{e}\left(h, SK_3^*\right)$. The proof is presented as follows:

$$\begin{aligned} SK^* &= \hat{e}\left(SK_2^*, g\right) \\ &= \hat{e}\left(R_{i+1,2} \cdot SK_1^*, g\right) \\ &= \hat{e}\left(h^{r_{i+1}} \cdot OC_2^{uH_3(SK)}, g\right) \\ &= \hat{e}\left(h^{r_{i+1}} \cdot PKI_{i+1,2}^{a_i r u H_3(SK)}, g\right) \\ &= \hat{e}\left(h^{r_{i+1}} \cdot h^{a_{i+1} a_i r u H_3(SK)}, g\right) \\ &= \hat{e}\left(h, g^{r_{i+1}} \cdot g^{a_{i+1} a_i r u H_3(SK)}\right) \\ &= \hat{e}\left(h, R_{i+1,1} \cdot SK_1^*\right) \\ &= \hat{e}\left(h, SK_3^*\right) \end{aligned}$$

The correctness of this phase is also proved. To sum up, the scheme we are involved in is correct.

6.2 Security of V2I-Initial Authentication Phase

Here, the security of V2I-initial authentication phase is proved in this subsection.

Theorem 1. The proposed V2I-initial authentication is CDH-secure in $\mathbb{G}$.

Proof. In our security model, the $\mathcal{A}$ has the ability to read the storage of the vehicle and get the SK_1 which is generated in **PreKeyGen**. With the value of SK_1, $\mathcal{A}$ can calculate $H_2\left(ID||T_1||\left(T_1\right)\mathfrak{C}\left(T_1\right)||H_1(SK_1)\right)$ with the ID of the vehicle, the timestamp T_1 sent by the RSU$_i$ and the vehicular trustworthiness $\mathfrak{C}\left(T_1\right)$ calculated by the trustworthiness scalable computation, which can be checked in the blockchain. $\mathcal{A}$ also can obtain the public parameter $PKI_{i,2}$ of RSU$_i$ and the value $R_{i,2}$ sent by RSU$_i$.

If the adversary can calculate the session key of this phase, he is able to first calculate the value of SK_2. As we can see in the algorithm **VehiSKGen**:

$$SK_2 = R_{i,2} \cdot PKI_{i,2}^{uH_2(ID||T_1||(T_1)\mathfrak{C}(T_1)||H_1(SK_1))},$$

where u is a secret value of the vehicle which is not known by $\mathcal{A}$.

That is to say, $\mathcal{A}$ can solve the CDH problem and DDH problem in $\mathbb{G}$. However, in our security model, the CDH problem and DDH problem in $\mathbb{G}$ is hard to be solved. So, $\mathcal{A}$ has a negligible advantage to calculate $g_1^{(l_{i+1}-l_{i-1})l_i}$ in $\mathbb{G}_1$.

Secondly, if the $\mathcal{A}$ wants to calculate SK with algorithm **RSUSKGen**, he needs to know the value of $R_{i,1}$, which is also kept secret by RSU$_i$.

To sum up, the V2I-initial authentication phase of B-TSCA scheme is CDH-secure in $\mathbb{G}_1$.

□

6.3 Security of V2I-Handover Authentication Phase

The security of V2I-handover authentication phase is proved in this subsection.

Theorem 2. The proposed V2I-handover authentication is CDH-secure in $\mathbb{G}$.

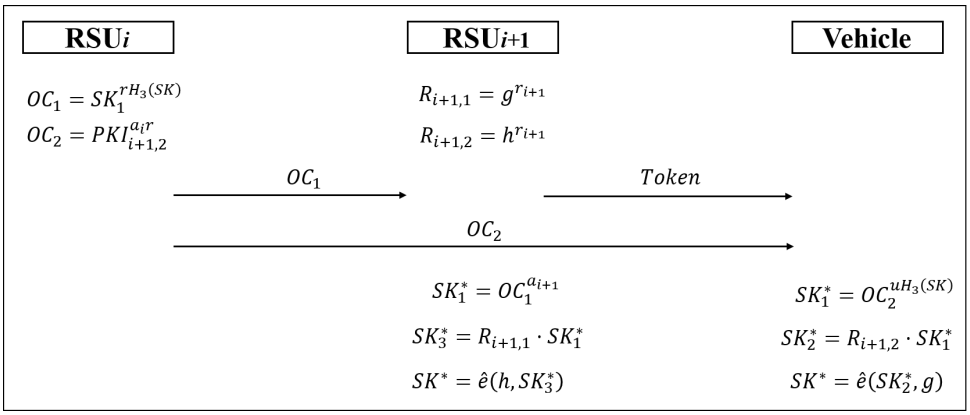

Fig. 6: V2I-handover authentication phase

Proof. In our security model, in the handover phase, the $\mathcal{A}$ has the ability to read the storage of the vehicle and get the SK which is generated in initial phase. With the value of SK, $\mathcal{A}$ can calculate $H_2(SK)$. $\mathcal{A}$ also can obtain the value $R_{i+1,2}$ sent by RSU$_{i+1}$.

If the adversary can calculate the session key of this phase, he needs to have the ability to calculate the value of SK_2^*. As we can see in the algorithm **VehiSKGen2**:

$$SK_2^* = R_{i+1,2} \cdot SK_1^*, \tag{15}$$

where $SK_1^* = OC_2^{uH_3(SK)}$. As described in the scheme, u is a secret value of the vehicle which is not known by $\mathcal{A}$.

That is to say, $\mathcal{A}$ can solve the CDH problem and DDH problem in $\mathbb{G}$. However, in our security model, the CDH problem and DDH problem in $\mathbb{G}$ is hard to be solved. So, $\mathcal{A}$ has a negligible advantage to calculate $g_1^{(l_{i+1}-l_{i-1})l_i}$ in $\mathbb{G}_1$.

Secondly, if the $\mathcal{A}$ wants to calculate SK^* with algorithm **RSUSKGen2**, he needs to know the value of $R_{i+1,1}$, which is also kept secret by RSU$_i$.

To sum up, the V2I-handover authentication phase of B-TSCA scheme is CDH-secure in $\mathbb{G}$. □

We can draw out theorem 3.

Theorem 3. The proposed B-TSCA scheme is CDH-secure in $\mathbb{G}$.

Proof. Theorem 3 can be easily proved if theorems 1 and 2 hold. □

6.4 Security against MITM Attack

An MITM attacker may block the message sent by the RSU$_i$ or RSU$_{i+1}$. He may change the message and send a new one to the vehicle. If a tampered $R_{i,2}$ and T_1 is sent to the vehicle, the vehicle will generated a session key according to the tampered message.

However, the session key generated with the tampered parameter will not be authenticated by RSU.

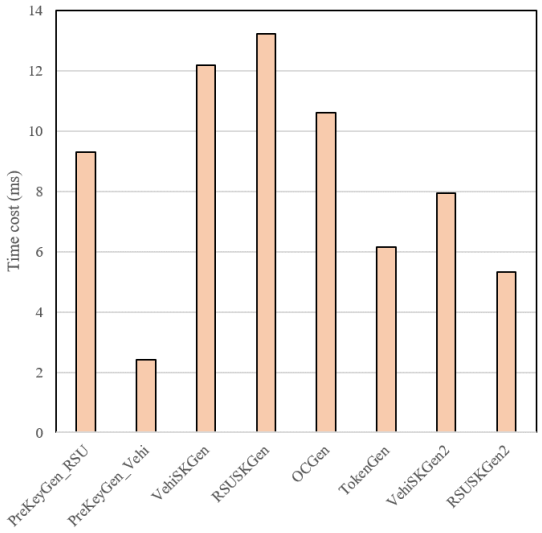

Fig. 7: The overhead comparison among different algorithms of B-TSCA

6.5 Security against Reply Attack

A reply attacker may block a message encrypted with SK by the vehicle. If the attacker delays sending the encrypted data to the RSU, the encrypted timestamp will be invalid and the data could not be authenticated. In addition, if the attacker sends the data authenticated by the previous RSU to the next RSU, the data will also fail to pass the authentication. Because this data is not encrypted by the session key generated by the vehicle and the next RSU.

7 Performance Analysis

The proposed scheme is simulated on GNU Multiple Precision Arithmetic (GMP) library and Pairing-Based Cryptography (PBC) library [1] to show its efficiency. C language is utilized on a Linux system with Ubuntu 16.04 TLS, a 2.60 GHz Intel(R) Xeon(R) CPU E5-2650 v2, and 8 GB of RAM.

We first simulate the time cost of different algorithms running on different system components. As is shown in Fig. 7, eight algorithms, **PreKeyGen** of RSU, **PreKeyGen**

1. https://crypto.stanford.edu/pbc/

of vehicle, **VehiSKGen**, **RSUSKGen**, **OCGen**, **TokenGen**, **VehiSKGen2**, and **RSUSKGen2**, are simulated and compared. Among them, **PreKeyGen** of RSU, **PreKeyGen** of vehicle, **VehiSKGen**, and **RSUSKGen** are algorithms of the V2I-initial authentication phase, while the others are algorithms of the handover phase. RSU_i runs **PreKeyGen** of RSU, **RSUSKGen**, and **OCGen**. RSU_{i+1} runs **TokenGen** and **RSUSKGen2**. The vehicle runs part of **PreKeyGen**, **VehiSKGen**, and **VehiSKGen2**. It is not difficult to see that the cost of a vehicle in the handover phase is significantly less than that in the initial phase. In addition, the operations run by vehicles are less time consuming than that of the RSUs.

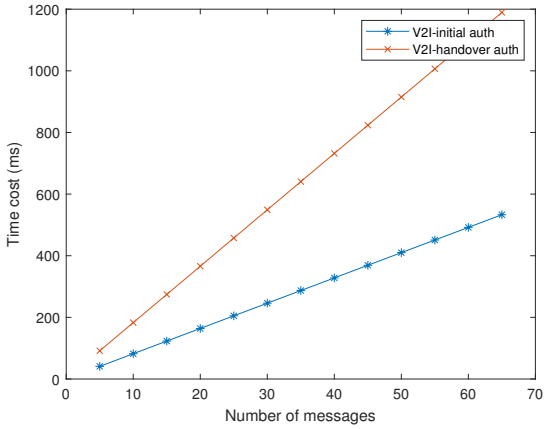

Fig. 8: Time cost comparison of a vehicle between different phases of B-TSCA

In our simulation, the time cost of the V2I-initial authentication phase and the V2I-handover authentication phase are separately simulated. The results are shown in Fig. 8. The time cost on the designed overhand authentication phase is reduced by half compared to the time required for the initial authentication phase. This is because, in the handover phase of the novel scheme, the vehicle only needs to implement a few operations according to the former session key generated with the help of the former RSU. Some of the computing operations are transferred to the handover between the previous RSU and the current RSU.

8 Conclusion

In this paper, a novel V2I authentication scheme for VANETs named B-TSCA scheme is presented with a blockchian assisted trustworthiness scalable computation system. Integrating blockchain technology into trustworthiness computation ensures tamper-resistance and traceability of vehicle trustworthiness. The new B-TSCA scheme is composed of a V2I-initial authentication phase and a V2I-handover authentication phase. When the vehicles are authenticated by roadside infrastructures, the trustworthiness of the vehicle recorded in the blockchain is utilized as a part of the authentication parameters. This scheme aims at reducing the computational cost of continuous identity authentication when the vehicle passes through multiple RSUs. The handover strategy is designed to reduce the redundant cost in the subsequent authentication process, which enhances the scalability of VANETs. The security analysis shows that B-TSCA is a CDH-secure scheme. The time cost of the handover authentication phase turns out to be reduced by half compared to the initial authentication in our simulation.

Acknowledgment

This work is supported by the National Natural Science Foundation of China under Grant No. 61922045, No. 61672295, No. U1836115, the Peng Cheng Laboratory Project of Guangdong Province under Grant No. PCL2018KP004, the State Key Laboratory of Cryptology under Grant No. MMKFKT201830, the 2015 Project of Six Personnel in Jiangsu Province under Grant No. R2015L06, the CICAEET fund, and the PAPD fund.

References

[1] S. Xie, Z. Zheng, W. Chen, J. Wu, H. Dai, and M. Imran, "Blockchain for cloud exchange: A survey," *Computers and Electrical Engineering*, vol. 81, 2020, DOI: 10.1016/j.compeleceng.2019.106526.

[2] H. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: A survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019.

[3] J. Liu, Q. Hu, C. Li, R. Sun, X. Du, and M. Guizani, "A traceable concurrent data anonymous transmission scheme for heterogeneous vanets," in *GLOBECOM*. IEEE, 2018, pp. 1–6.

[4] S. Tang, X. Li, X. Huang, Y. Xiang, and L. Xu, "Achieving simple, secure and efficient hierarchical access control in cloud computing," *IEEE Trans. Computers*, vol. 65, no. 7, pp. 2325–2331, 2016.

[5] Z. Zheng, S. Xie, H. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *CoRR*, vol. abs/1912.10370, 2019. [Online]. Available: http://arxiv.org/abs/1912.10370

[6] X. Yuan, X. Yuan, B. Li, and C. Wang, "Toward secure and scalable computation in internet of things data applications," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3753–3763, 2019.

[7] T. Zhou, L. Chen, and J. Shen, "Movie recommendation system employing the user-based CF in cloud computing," in *2017 IEEE International Conference on Computational Science and Engineering, CSE 2017, and IEEE International Conference on Embedded and Ubiquitous Computing, EUC 2017, Guangzhou, China, July 21-24, 2017, Volume 2*, 2017, pp. 46–50. [Online]. Available: https://doi.org/10.1109/CSE-EUC.2017.194

[8] T. Li, C. Gao, L. Jiang, W. Pedrycz, and J. Shen, "Publicly verifiable privacy-preserving aggregation and its application in iot," *J. Network and Computer Applications*, vol. 126, pp. 39–44, 2019.

[9] W. Wang, P. Xu, L. T. Yang, and J. Chen, "Cloud-assisted key distribution in batch for secure real-time mobile services," *IEEE Trans. Services Computing*, vol. 11, no. 5, pp. 850–863, 2018. [Online]. Available: https://doi.org/10.1109/TSC.2016.2594071

[10] D. Liu, J. Shen, A. Wang, and C. Wang, "Lightweight and practical node clustering authentication protocol for hierarchical wireless sensor networks," *IJSNet*, vol. 27, no. 2, pp. 95–102, 2018. [Online]. Available: https://doi.org/10.1504/IJSNET.2018.092638

[11] C. Wang, W. Zheng, S. Ji, Q. Liu, and A. Wang, "Identity-based fast authentication scheme for smart mobile devices in body area networks," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 4 028 196:1–4 028 196:7, 2018. [Online]. Available: https://doi.org/10.1155/2018/4028196

[12] I. Ali, M. Gervais, E. Ahene, and F. Li, "A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs," *Journal of Systems Architecture - Embedded Systems Design*, vol. 99, 2019.

[13] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45 655–45 664, 2018.

[14] P. Xu, S. He, W. Wang, W. Susilo, and H. Jin, "Lightweight searchable public-key encryption for cloud-assisted wireless sensor networks," *IEEE Trans. Industrial Informatics*, vol. 14, no. 8, pp. 3712–3723, 2018. [Online]. Available: https://doi.org/10.1109/TII.2017.2784395

[15] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-preserving and lightweight key agreement protocol for V2G in the social internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2526–2536, 2018.
[16] Y. Hao, T. Han, and Y. Cheng, "A cooperative message authentication protocol in vanets," in *GLOBECOM*. IEEE, 2012, pp. 5562–5566.
[17] B. Li, Z. Fei, and Y. Zhang, "UAV communications for 5g and beyond: Recent advances and future trends," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2241–2263, 2019.
[18] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 3, pp. 736–746, 2011.
[19] S. J. Horng, S. F. Tzeng, Y. Pan, P. Fan, and M. K. Khan, "B-SPECS+: Batch verification for secure pseudonymous authentication in VANET," *IEEE Transactions on Information Forensics & Security*, vol. 8, no. 11, pp. 1860–1875, 2013.
[20] H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu, "Privacy-preserving authentication scheme with full aggregation in VANET," *Inf. Sci.*, vol. 476, pp. 211–221, 2019.
[21] S. Biswas and J. Misic, "A cross-layer approach to privacy-preserving authentication in WAVE-enabled VANETs," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2182–2192, 2013.
[22] K.-A. Shim, "Comments on "a cross-layer approach to privacy-preserving authentication in WAVE-enabled VANETs" by biswas and misic," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10 588–10 589, 2017.
[23] J. Cui, D. Wu, J. Zhang, Y. Xu, and H. Zhong, "An efficient authentication scheme based on semi-trusted authority in vanets," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2972–2986, 2019.
[24] J. Shao, X. Lin, R. Lu, and Z. Cong, "A threshold anonymous authentication protocol for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1711–1720, 2016.
[25] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 8, pp. 2193–2204, 2016.
[26] C. Jie, Z. Jing, Z. Hong, and X. Yan, "Spacf: A secure privacy-preserving authentication scheme for vanet with cuckoo filter," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10 283–10 295, 2017.
[27] Y. Wang, Y. Ding, Q. Wu, Y. Wei, B. Qin, and H. Wang, "Privacy-preserving cloud-based road condition monitoring with source authentication in VANETs," *IEEE Transactions on Information Forensics & Security*, vol. 14, no. 7, pp. 1779–1790, 2019.
[28] J. Zhou, Z. Cao, Z. Qin, X. Dong, and K. Ren, "LPPA: lightweight privacy-preserving authentication from efficient multi-key secure outsourced computation for location-based services in VANETs," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 420–434, 2020.
[29] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2019.
[30] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "BARS: A blockchain-based anonymous reputation system for trust management in VANETs," in *TrustCom/BigDataSE*. IEEE, 2018, pp. 98–103.
[31] H. Wang, Q. Wang, D. He, Q. Li, and Z. Liu, "BBARS: blockchain-based anonymous rewarding scheme for V2G networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3676–3687, 2019.
[32] C. Wang, L. Xiao, J. Shen, and R. Huang, "Neighborhood trustworthiness-based vehicle-to-vehicle authentication scheme for vehicular ad hoc networks," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 21, pp. 1–11, 2019.