A Privacy Preserving Blockchain-based Reward Solution for Vehicular Networks

Junho Lee, Jangwon Lee, and Hyungweon Park
Samsung Electronics, Hwasung-si, Gyeonggi-Do and Republic of Korea
{junho07.lee, jangwon.lee, froghwp}@samsung.com

Abstract—Vehicular networks use a vehicle to infrastructure (V2I) to improve traffic safety by gathering information from vehicles such as traffic conditions and accidents. This approach is based on the vehicle's location information and the reliability of the data collected from the vehicle. At the same time, the voluntary participation of drivers requires privacy protection and compensation for sharing trusted information. In this paper, we propose a blockchain-based decentralized reward solution considering drivers’ privacy. Using a unique identifier has a vulnerability of exposing the vehicle’s location to attackers and hence the attackers can easily trace any vehicles. By employing changing pseudonyms instead of using a unique identifier, the driver can protect their location privacy from other vehicles and Roadside Units (RSUs) that could be a potential attacker. The proposed solutions also enable service providers can verify the reliability and integrity of the messages transmitted by legitimate vehicles.

I. INTRODUCTION

With the rapid development of 5G mobile communication systems and vehicular electronic equipment, the vehicle is expected to produce a huge amount and various types of data through onboard devices. In this environment, it is possible to enhance the efficient operation and safety of the vehicle by analyzing driving and traffic-related messages such as position in the network, current speed, and road conditions. As the number of on-road vehicles exchanging data grows over the vehicular network, applications utilizing this data are appearing in various fields, e.g. safety, real-time traffic information, insurance, car sharing, and other applications [1]. To support these applications, data that is locally related to the vehicle has a spatial range and time-sensitive, such as current traffic information at the intersection, which requires low latency and location recognition for vehicle data sharing [2]. Recently, 5G networks are being designed to meet the very large growth in data and connectivity, with billions of connected devices. Mobile edge computing (MEC) is the key technology to meet low latency requirements of 5G networks, which can be equipped at the roadside units (RSUs) to support storage and computing close to the vehicles [3].

However, the growth of connectivity means that vehicles are more likely to spread false messages for malicious purposes such as traffic jamming. Location privacy is a security technology that must be provided to increase user participation in the vehicular network that relies on location data broadcasting. Thus, both security technologies that can adequately respond to attacks and that can protect the privacy of vehicles have become key requirements for the vehicles to reliably proliferate and be utilized. In particular, the blockchain could be very helpful in building architecture for automotive security and privacy [4]. It has attracted growing attention in vehicular networks because of its characteristics of decentralization, which makes it be facilitate established in MEC [5].

In section II, we describe the system model that forms the basis of the proposed protocol. In section III, we present the protocols that enable vehicles can send a valid message to the RSU while ensuring the privacy of the vehicles. We also describe the protocol for compensation on the blockchain system in this section. In section IV, we discuss the security and privacy of the proposed protocol. We conclude by discussing the contribution in section V.

II. SYSTEM MODEL

A. Network Model and Assumptions

The proposed system follows 5G ITS infrastructures each equipped with a device that is embedded with a wireless communication module based on 5G. Among the 5G features, ultra-low latency will change various industries, including the self-driving car industry because it determines the speed of the reaction to events such as car accidents. As illustrated in Fig. 1, RSUs are controlled by a core network and equipped with MEC to achieve low latency while being located close to a mobile device. MEC provides a platform for bringing services to the most suitable network locations such as mobile vehicles on roads [3].

B. Blockchain

Blockchain technology is used to maintain a consistent database among RSUs in an environment where vehicles travel across multiple RSUs. Since the blockchain require access by limited nodes and public readability may not preferable, a private blockchain is used for the proposed
system rather than a public blockchain like Bitcoin [6]. Above all, it doesn’t need for RSUs to build a blockchain through competition to receive awards. In the proposed system, it is assumed that the RSU with the smallest workload creates the blockchain at regularly scheduled times. Each RSU has a role to pack received data into a block and send blocks to the selected RSU which creates new blockchain at the scheduled time. Every RSUs have copies of the blockchain, which are constantly synchronized with other copies, so there are no centralized vulnerabilities available to computer hackers.

C. Trust Assumption and Adversary Model

It is assumed that a service provider (SP) is a trust entity since it can trace the real identity of vehicles to reward for the data collected from them. A vehicle is equipped with an embedded tamper-resistant black box that has been used for designing a secure protocol in VANET [7], [8]. The vehicle’s black box (VBB) supports hardware secure storage for credentials like smart card and hence it never leak any information about the secrets, even when an attacker steal VBB. During a registration phase, there is a secure channel between VBB and SP’s server. The secure channel is established using protocols such as SSL and TLS. Each RSU and SP has a signature/verification key pair for use in a conventional digital signature (e.g., ECDSA[9]) and also a pre-shared secret value over the secure channel. To prevent linking between old and new pseudonym, whenever changing the link between old and new pseudonym, whenever changing the protocol, and network identifiers, such as IP or MAC addresses, are changed simultaneously [10]. The goal of the adversary is to inject wrong information in the network to affect the behavior of other vehicles. RSUs may perform attempts to trace the vehicles with their messages.

III. PROPOSED PROTOCOL WITH PSEUDONYM

This section presents the functioning of the proposed protocols. The main contribution is conditional anonymous user authentication and compensation based on blockchain.

A. System Parameter Initialization

The proposed protocol uses the initial parameter \((a, b, q, G, n)\) as follows. \(E\) is an elliptical curve defined in the finite domain \(\mathbb{F}_q\). \(G\) is a random base point with prime order of \(n\) for the elliptical curve \(E\). \(h\) is a cryptographic hash function. \(\text{sign}_i(m)\) is a signature of identity \(i\) to message \(m\). \(T\) is a timestamp at the time \(t\). The key notation used in this paper is described in Table I.

<table>
<thead>
<tr>
<th>Table I</th>
<th>KEY NOTATION USED FOR THE PROPOSED PROTOCOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notation</td>
<td>Definition</td>
</tr>
<tr>
<td>(q)</td>
<td>Large prime numbers</td>
</tr>
<tr>
<td>(ID_i)</td>
<td>Identity of a vehicle</td>
</tr>
<tr>
<td>(PID_i)</td>
<td>(ID_i)'s Pseudo-identity</td>
</tr>
<tr>
<td>(VBB_i)</td>
<td>(ID_i)'s black box</td>
</tr>
<tr>
<td>(RSU_i)</td>
<td>Identity of a RSU and a RSU building block</td>
</tr>
<tr>
<td>(\text{sign}_i(m))</td>
<td>Vehicle’s signature to message (m)</td>
</tr>
<tr>
<td>(s)</td>
<td>Shared value, (seZ^*_n), of SP and RSUs</td>
</tr>
<tr>
<td>(Pri, Pub)</td>
<td>ECDSA signature key and verification key</td>
</tr>
<tr>
<td>(h())</td>
<td>Cryptographic hash function</td>
</tr>
</tbody>
</table>

B. Registration Phase

\(VBB_i\) performs following process to register in the service.

Step 1. \(VBB_i\) internally creates key pairs, private key \(x_i \leftarrow \mathbb{Z}[1,n-1]\) and generates public key \(Q_i=vG\) and keep a private key \(x_i\) safe inside and never let it go outside, even a vehicle’s user request. It shares the vehicle’s identifier \(ID_i\) with public key \(Q_i\) to SP’s server which the vehicle’s user wants to share traffic information with and get rewards from.

Step 2. The SP’s server generates \(Q_{is}=sQ_i\) from the computation of secret value \(s \leftarrow \mathbb{Z}[1,n-1]\) which is pre-shared with RSU over a secure channel in Fig. 2. It selects a random value \(r_i \leftarrow \mathbb{Z}[1,n-1]\) and calculates \(y_i= r_i \cdot s^{-1} \mod n\) and then stores \(y_i\) and \(Q_i\) with the user’s \(ID_i\) in its storage as the form of \(ID_i\lceil r_i \rceil \lceil Q_i\). And then the server transmits two values, \(y_i\) and \(Q_{is}\) to \(VBB_i\) in Fig. 2.

Step 3. \(VBB_i\) saves two initial values \(y_i\) and \(Q_{is}\) used to generate pseudo identities directly on its internal storage.

C. Anonymous signature with pseudonyms

To enhance the privacy and anonymity of transactions, the vehicle uses pseudo identities as the result of the computation of the public key and random numbers. The pseudo identities can be changed automatically according to settings (e.g. per time \(t\)) to prevent traceability.

Step 1. \(VBB_i\) generates pseudonym \(\text{PID}_i=r_jr_iQ_i\) by using a random number \(r_j \leftarrow \mathbb{Z}[1,n-1]\) and the initial values of \(y_i\) and \(Q_{is}\) at time \(t\) in (1).

\[
\text{PID}_i=r_j \cdot y_i \cdot Q_{is} = r_j \cdot r_i \cdot s^{-1} \cdot s \cdot Q_i = r_j \cdot r_i \cdot Q_i
\]

Step 2. \(VBB_i\) selects \(k \leftarrow \mathbb{Z}[1,n-1]\) to get \(E\) coordinates \((a, b)=kG\) and sets the x-coordinate \(a\) to the variable \(v\) in (2). It creates a signature on the hash of message \(m\) at time \(t\) in (3).

\[
v=a
\]

\[
\text{sign}_i(m)\]

\[
T
\]

Fig. 2. Registration over the secure channel.
Step 3. VBBᵢ sends the message $PIDᵢ||m||sign(m)||v||t$ to a nearby RSU over wireless mobile networks and saves $m||rᵢ||t$ in its storage in Fig. 3.

D. Verifying signature

As illustrated in Fig. 3, RSU validates the received message through the signature verification phase.

Step 1. For the signature verification, it computes $w=sign(m)⁻¹ \mod n$. And it calculates $u₁=w⋅h(m)\mod n$ and $u₂=w⋅v⋅s⁻¹ \mod n$ with the received value $v$ and the inverse of the value $s$ which is pre-shared with SP.

Step 2. The signature is verified by comparing the value $x'$ of x-coordinate in (4) and the value $v$. If two values are the same, the signature is valid and proven to be delivered from a legitimate vehicle which is registered in SP.

\begin{equation}
(x', y') = u₁G + u₂PIDᵢ
\end{equation}

In (11), $kG$ is derived from the calculation of $u₁G+u₂PIDᵢ = w⋅h(m)⋅xᵢ + xᵢ⋅yᵢ \mod n \mod n$.

Step 3. RSU stores valid record sets in the storage of MEC as the form of $rcd=PIDᵢ||m||sign(m)||t$ and delivers $rcd$ to SP.

E. Creation of blockchain

Each RSUᵢ generates $recordᵢ=rcdᵢ||rcdᵢ-1||...||rcd₁$ from the set of valid n-rcd stored in the MEC repository and create block with the signature based on the ECDSA [9]. The detailed steps are as follows.

Step 1. RSUᵢ signs the record and creates transaction $transᵢ = RSUᵢ||ECDSA_Sign(Priᵢ, recordᵢ)|||recordᵢ||t$. RSUᵢ delivers $transᵢ$ to RSUᵢ₋₁. It is assumed that RSUᵢ₋₁ is selected by turn or has the smallest workload among RSUs at time $t$.

Step 2. RSUᵢ₋₁ build a block $BL = Header||Body$. It constructs the body for n-numbers of transactions, $body = transᵢ||transᵢ₋₁||...||trans₁$. RSUᵢ₋₁ calculates a hash root of $transᵢ$ based on a Merkle hash tree[11]. And it compose the header with the hash of previous BC’s header, a timestamp and the hash root header $= h(Previous\ BC\ Header)||t||Hashroot$.

F. Compensation Phase

The user can get rewards from SP for the information provided to RSUs through the following procedure.

Step 1. VBBᵢ sends an reward requesting message $RMM₁=IDᵢ||mᵢ||rᵢ||tᵢ$ ($1≤i≤n$) for n-numbers transmitting messages to SP’s server in the secure channel. For example, if VBBᵢ transmitted two messages $m₁$ and $m₂$ at time $t₁$ and $t₂$ respectively, the message is $IDᵢ||mᵢ||rᵢ||tᵢ||mᵢ||rᵢ||tᵢ$.

Step 2. SP’s server searches $IDᵢ||rᵢ||tᵢ||Qᵢ$ corresponding to $IDᵢ$ of the received messages $RMMᵢ$. It then retrieves all records $rcdᵢ=PIDᵢ||mᵢ||sign(mᵢ)||tᵢ$ from the repository that satisfies both conditions, $t₁ = tᵢ$ and $mᵢ = mᵢ$, at the same time. The SP rewards the user for records that satisfies $Qᵢ'=rᵢ⁻¹⋅rᵢ'PIDᵢ$ as shown in Fig. 5.

IV. SECURITY AND PRIVACY ANALYSIS

A. Anonymity and unlinkability

In the proposed protocol, whenever VBBᵢ sends a message to a RSU, it hides the identity by using and ensure a pseudonymous identity that cannot be linked with a real identity. $PIDᵢ$ is the result of an operation with a random number $r_j$ ($PIDᵢ = r_j \cdot r_iQ_i$). For the RSU, there is no information about the relationship between $PIDᵢ$ and $IDᵢ$. Thus if the RSU is compromised by an adversary, the proposed protocol enables the vehicle to preserve its privacy against the RSU. The adversary can also attempt to trace a target vehicle by analyzing broadcasted messages it collects. For example, when the adversary is given two pseudonyms, $PID₁ = r₁ \cdot r_iQ_i$ and $PID₂ = r₂ \cdot r_iQ_i$, it will try to find a link

```
<table>
<thead>
<tr>
<th>VBBᵢ</th>
<th>RSU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create pseudonym</td>
<td>rᵢ, kG = Eₙᵢ</td>
</tr>
<tr>
<td>$PIDᵢ = r_j \cdot r_iQ_i$</td>
<td>$rᵢQᵢ, rⱼQⱼ, rᵢ⁻¹Qᵢ, rⱼ⁻¹Qⱼ$</td>
</tr>
<tr>
<td>Signature at time t</td>
<td>$sign(m) = \frac{h(m)\mod n+rᵢQᵢ}{v\mod n}$</td>
</tr>
<tr>
<td>Verify Signature</td>
<td>$PIDᵢ</td>
</tr>
<tr>
<td>$PIDᵢ</td>
<td></td>
</tr>
</tbody>
</table>

| Valid or invalid | $v \cdot x' = m'$ |

Fig. 3. Signature with pseudonym and verification.
```

```
<table>
<thead>
<tr>
<th>VBBᵢ</th>
<th>Secure Channel</th>
<th>SP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request a reward for n numbers messages</td>
<td>$mᵢ, rᵢ, tᵢ...mᵢ, rᵢ, tᵢ$</td>
<td>$mᵢ, rᵢ, tᵢ...mᵢ, rᵢ, tᵢ$</td>
</tr>
<tr>
<td>$IDᵢ</td>
<td></td>
<td>mᵢ</td>
</tr>
<tr>
<td>Search $IDᵢ</td>
<td></td>
<td>rᵢ</td>
</tr>
</tbody>
</table>

Computes on $mᵢ||rᵢ||tᵢ$($1≤i≤n$)
1. Reward = 0
2. Find $j$ such that $rᵢ = rⱼ$ 
3. Search for corresponding to $xᵢ, xⱼ$
4. If $h(xᵢ) = PIDᵢ||mᵢ||sign(mᵢ)||tᵢ$ 
5. Valid = $vᵢ = vⱼ$ 
6. Then $rᵢ = rⱼ$
7. Then $R = reward$ 
8. Reward $R$ |

Fig. 5. Reward request and compensation
```

<table>
<thead>
<tr>
<th>Block BL₁₂</th>
<th>Block BL₂₂</th>
<th>Block BL₃₂</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header</td>
<td>Header</td>
<td>Header</td>
</tr>
<tr>
<td>Hash of Header of BC</td>
<td>Hash of Previous Block Header</td>
<td>Hash of Previous Block Header</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Timestamp</td>
<td>Timestamp</td>
</tr>
<tr>
<td>Merkle Root</td>
<td>Merkle Root</td>
<td>Merkle Root</td>
</tr>
<tr>
<td>Body</td>
<td>Body</td>
<td>Body</td>
</tr>
</tbody>
</table>

Fig. 4. The blockchain and Merkle hash tree
between \( PID_1 \) and \( PID_2 \) for tracing the target but cannot get any linkable information between the two pseudonyms because of random values, \( r_1 \) and \( r_2 \).

B. Anonymous Authentication

While RSU cannot guess which vehicle transmit the message \( m||PID||v||\text{sign}(m) \), it can authenticate message with the value \( s \leftarrow [1, n-1] \) which is pre-shared with SP. In (4), the RSU prepares \( u_2 = w \cdot v \cdot s^{-1} \) for the verification of signature using the inverse of \( s \). And a vehicle obtains the initial value which computed by public key \( Q \) and \( s, Q \cdot s = sQ \), from SP in the registration phase. Thus, malicious vehicles not registered in the SP’s server fail to generate a signature that can pass a RSU’s signature verification.

C. Non-reputation

If a legitimate vehicle requests compensation for data transmitted through RSU, SP cannot simply deny the validity of the vehicle’s transaction. All data delivered to the RSU is stored in one of the blocks on BC as the form of a transaction after being signed by RSU. And BC is periodically updated and synchronized with all RSUs and vehicles. Conversely, if SP or RSU determines that a vehicle provided incorrect information, the vehicle can be traced by SP which knows the real identity of the vehicle for the same reason.

V. PERFORMANCE ANALYSIS

In order to analyze the performance of the proposed protocol, we simulate the protocol by using OpenSSL library for SHA256 and ECC equations. The experiment environment used by the test program is Ubuntu 16.04LTS with 4GB memory and core i5-4590@ 3.30GHz *4 CPU. In this experiment, 239-bit elliptic curve domain parameters are used and SHA256 is used to hash the message. The performance was measured for each of the three phases: registration, anonymous signature, and signature verification. The computational overhead of ECC and big integer was described and the performance time was measured for each phase in Table II.

<table>
<thead>
<tr>
<th>TABLE II PERFORMANCE ANALYSIS OF THE PROPOSED PROTOCOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computational Overhead</td>
</tr>
<tr>
<td><strong>Registration</strong></td>
</tr>
<tr>
<td><strong>Signature</strong></td>
</tr>
<tr>
<td><strong>Verification</strong></td>
</tr>
<tr>
<td>Performance Time</td>
</tr>
<tr>
<td>Run</td>
</tr>
<tr>
<td><strong>Registration</strong></td>
</tr>
<tr>
<td><strong>Signature</strong></td>
</tr>
<tr>
<td><strong>Verification</strong></td>
</tr>
</tbody>
</table>

\*EPM = Elliptic Curve Point Multiplication, EPA = Elliptic Curve Point Addition, BMM = Biginteger Modular Multiplication, BMI = Biginteger Modular Inverse, BMA = Biginteger Modular Addition, CMP = Biginteger Comparison

VI. CONCLUSION

In this paper, we proposed the anonymous protocol using a pseudonym for drivers’ privacy. If vehicle use one credential, their whole transactions via the network on the road can be linked to each other. Except for service providers registered by users to receive compensation, RSUs and other vehicles cannot track specific vehicles through the data transmitted in the network. Therefore, the RSUs don’t know which vehicle sent the data because of the vehicle’s pseudo-identity, but the signature verification of the proposed protocol indicates that the data was transmitted from a legitimate vehicle. Besides, the proposed protocol was designed to prevent service providers from rejecting users’ demand for compensation using distributed blockchain-based distributed systems. We also measured performance for the procedures, which is reasonable in that it provides authentication services that provide anonymity.

REFERENCES