Available online at www.sciencedirect.com

ScienceDirect

Future Generation Computer Systems 00 (2019) 1–12

FGCS

A Blockchain Based Certificate Revocation Scheme For Vehicular Communication Systems

Ao Lei[a], Yue Cao[b,*], Shihan Bao[a], Dasen Li[c], Philip Asuquo[a], Haitham Cruickshank[a], Zhili Sun[a]

[a]*Institute for Communication Systems, University of Surrey, UK*
[b]*School of Computing and Communications, Lancaster University, UK*
[c]*School of Computer Science and Engineering, South China University of Technology, China*

Abstract

Both the academy and industry believe that Intelligent Transportation System (ITS) would be achievable in one decade since modern vehicle and communication technologies advanced apace. Vehicular Communication System (VCS) introduces information technology to the ITS and aims to improve road safety and traffic efficiency. In recent year, security and privacy schemes in VCS are becoming important. However, recovery mechanisms to eliminate the negative effect of security and privacy attacks are still an important topic for research. Therefore, the certificate revocation scheme is considered as a feasible technique to prevent the system from potential attacks. The major challenge of the certificate revocation scheme is to achieve low-cost operation since the communication resources must be capable of carrying various applications apart from the security and privacy purposes. In this paper, we propose an efficient certificate revocation scheme in VCS. The Blockchain concept is introduced to simplify the network structure and distributed maintenance of the Certificate Revocation List (CRL). The proposed scheme embeds part of the certificate revocation functions within the security and privacy applications, aiming to reduce the communication overhead and shorten the processing time cost. Extensive simulations and analysis show the effectiveness and efficiency of the proposed scheme, in which the Blockchain structure costs fewer network resources and gives a more economic solution to against further cybercrime attacks.

Keywords: , Certificate Revocation, Low-cost Framework, Blockchain, VCS, ITS

1. Introduction

In recent years, the combining of vehicle and network communication technologies keeps pushing the boundary of the next generation vehicles, also known as Intelligent Transportation Systems (ITS). Vehicles and ITS infrastructures play the role of physical units, while the Vehicular Communication Systems (VCS) is the network platform of ITS. Infrastructure access points in VCS are called Road Side Units (RSUs) [1]. Traditional VCS is comprised of multiple RSU cells and offers a platform among ITS for vehicles to exchange various kinds of messages such as safety beacon messages. With the help of VCS, the vehicle becomes a platform which could receive information from its peers. For this reason, the environment and ITS can offer safer and efficient traffic management. Moreover, commercial applications, such as electric vehicle charging [2] can be implemented on a dedicated platform. A recent report from U.S Department of Transport (DoT) shows that 82% of the accidents can be prevented by using ITS systems [3].

Applications in VCS are normally classified into Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) [4]. The VCS security highly relies on the exchange of safety beacon messages. These beacon messages are usually referred to as Cooperative Awareness Messages (CAMs) in Europe [5] or Basic Safety Messages (BSMs) for US [6], as they enable other vehicles to be aware of their surroundings. Vehicles located in the same RSU cell form a group and the current traffic situation is generated based on the summary of safety beacon broadcast from other group members [7]. The problem of providing ITS security can be mapped into the problem of how to maintain the trustfulness and legality of safety beacon messages among the communicating participants. However, the ITS security can be compromised if an authenticated node suddenly launches attacks. Admittedly, the VCS faces the risk of disclosing the sensitive information about vehicles as many applications and services make use of safety beacon messages. The safety beacon message contains vehicle status information, such as identity, location and other personal data. Even though significant developments about VCS security and privacy have taken place over the past few years, revocation issues are still an open topic for research. High mobility, large volume of vehicular nodes

*Corresponding Author
Email addresses: mcclion@gmail.com (Ao Lei), yue.cao@lancaster.ac.uk (Yue Cao)

and heterogeneity networks pose different challenges compared to the traditional mobile networks. For this reason, the security robustness of VCS is maintained by introducing certificate revocation to eliminate further attacks by insider attackers.

The earlier schemes introduce pseudonym and pseudonym certificate to protect VCS security and privacy [8]. Vehicles carry a set of pseudonyms which are used under different time periods in VCS communication. The safety beacon messages are sent using a pseudonym set, instead of the permanent identity of the vehicle. The pseudonym set contains pseudonym identity, pseudonym certificate and the corresponding key pairs. The vehicle signs the beacon message with pseudonym private key, attaches the pseudonym certificate and sends out the beacon message. A pseudonym certificate is revoked if the certificate owner involves in malicious behaviours and other nodes are informed about the revocation information. Most of the current pseudonym based privacy preserving schemes use Certificate Revocation Lists (CRLs) [9] [10] to distribute the revocation information. To guarantee security and privacy, vehicles are supposed to use each pseudonym set for a short duration and frequently switch to a new pseudonym. The US-based VCS standard SAE J2735 [6] defines the pseudonym changing in 120 seconds or 1 km distance travelled (whichever stays longer), while the EU standard ETSI TS 102.867 [11] recommends changing pseudonyms every 5 minutes. This however increases the revocation efficiency as the central manager must revoke a malicious user by adding all its pseudonym sets to the CRL, as the CRL becomes tedious along with the number of revoked vehicle grows. Moreover, the CRL distribution and updating procedures result in large message overheads.

In this paper, we propose a distributed framework for providing efficient certificate revocation service. The certificate revocation should cover all the VCS nodes, therefore the revocation in VCS relies on the coordination between infrastructure and vehicle levels. The infrastructure and vehicle levels of the framework are discussed separately.

(i) *infrastructure level:* As mentioned above, accountability can be realised by distributing CRLs. However, the privacy requirement is guaranteed by shuffling vehicles pseudonyms regularly. This brings additional difficulty for the central manager to track the ownership of pseudonyms. The central manager should be able to update the mapping relationships between the permanent identity of vehicles and pseudonyms in order to maintain both privacy and accountability requirements. Therefore, a novel Blockchain [12] concept is introduced into the proposed framework to maintain and distribute CRL under distributed consensus among all the infrastructure participants [13]. Blockchain technology was previously proposed to simplify the network structure and accelerate key handover between security domains. The pseudonym shuffling is realised by using the Blockchain distributed consensus, instead of managed by the central manager. The pseudonym shuffling results are recorded in blocks (distributed ledger). The central manager in our proposed scheme uses the recorded block to reveal the mapping between the permanent identity and pseudonym sets of malicious users. In this way, the Blockchain system speeds up the processes of accountability function among infrastructures.

(ii) *vehicle level:* Within the vehicle level, the revocation is achieved by deleting the malicious users from the communication group instead of broadcasting CRL. Thus the broadcast overhead is much less than the traditional revocation schemes. A lightweight CRL-based revocation scheme is proposed to revoke the vehicle's access authority. Different from central manager distributing the CRL to all the vehicles via RSUs in the traditional methods, the scheme only broadcasts CRL to RSU level. The revocation is delivered along with the group key management procedures by not distributing group key to the malicious vehicle. The vehicle level revocation relies on the key management updating scheme in [14]. Malicious vehicles are excluded from the communication group according to the revocation list using the key management scheme.

The remainder of this paper is organised as follows: Section 2 briefly introduces the existing certificate revocation techniques and the novel Blockchain applications. The model structure overview, a comparison between Blockchain and traditional structure and details of our scheme are discussed in Section 3. The proposed certificate revocation scheme is introduced in details afterwards. The scenario set up and performance evaluation are demonstrated in Section 5. Section 6 concludes the paper and presents some future plans.

2. Related Work

In this section, we present the overview of the characteristics of any related techniques which is used in this paper. Blockchain concept and the related applications are discussed in the first place. Then we introduce pseudonym changing schemes in order to clarify the reason why we need Blockchain to assist certificate revocation. Blockchain concept and the related applications are discussed. A brief literature review about the previous works on certificate revocation schemes is illustrated afterwards.

2.1. Blockchain and Blockchain-based Applications

Nowadays, Bitcoin attracts a lot of attention along with its blockchain concept, which was proposed in 2008 [12]. The popular feature of Blockchain is that all the nodes distributed maintain an authenticated, shared and well-recorded transaction ledger. By not using central manager, the Blockchain system manages to ask all network participants to denote computation power to proofread transactions correctness and integrity. The authenticated transactions are recorded in the public ledger that every node in the network has a copy and is able to easily verify it. Hence the accountability is approved in the Blockchain by looking up previous blocks [15]. In addition, security and privacy of the blocks are protected by using consensus algorithm, such as the Proof-of-Work (PoW) [16]. The distributed network structure makes the Blockchain system achieve better robustness to against network failure which is caused by nodes disconnection. However, 51% attack is still a potential problem for Blockchain applications as it might allow an attacker to control the operation of entire network [16].

Another consensus algorithm that worth to be mentioned is the Proof of Elapsed Time (PoET) which was developed by Intel. The PoET generates a random back-off time and attaches cryptographic receipt behind the message. The receipt is to prove that the back-off time was calculated under legal ways and a new block can only be broadcasted after the back-off time. PoET gives less computation burden but might cause longer time for blocks to join the network. Moreover, PoW is the most reliable consensus mechanism that has been tested in a sustained manner in an adversarial environment, and is the only known cryptographic puzzle that meets these testing requirements. Consensus mechanisms like PoET have not yet been tested in real and adversarial practice.

Researchers started to propose using blockchain not only for decentralized currencies, but also for applications in Internet-of-Things (IoT) scenarios [17] [18] [19]. Authors in [18] proposed a new digital currency based on Bitcoin, that provides better scalability and flexibility. Despite the fact that Blockchain gains a lot of attention from banking, people also find Blockchain could improve existing system in different ways such as trust management [20], insurance, electric vehicles charging and car sharing services [19]. Our previous contributions [13] [14] apply the Blockchain to VCS scenario. They focus on the key management within infrastructure and vehicle levels, respectively. Furthermore, the Blockchain in VCS has potential developments on privacy and revocation applications.

2.2. Pseudonym Changing Schemes

Pseudonyms and pseudonym certificates aim to protect information privacy of the safety beacon messages [8]. Vehicles are required to broadcast safety beacon messages using pseudonym sets instead of permanent identities. Each pseudonym set is expensive as it is supported by the corresponding pseudonym certificate and asymmetric key pairs to assure complete privacy. These materials require high processing power to generate and large storage space to store. It's a heavy burden for the central manager to generate multiple numbers of pseudonyms and distribute them to vehicles. For this reason, the pseudonym changing approaches are proposed to reuse the pseudonyms to reduce the production cost of pseudonym sets [21].

Authors in [22] analyse the effectiveness of the pseudonym changing inside mixed zone. A mixed zone is an area that all the nodes have similar movement conditions. The results show the pseudonym changing within mixed zone improves the privacy level if an attacker monitors less than half of the mix zones within the network. Changing pseudonym at social spots is discussed in [23] and [24]. The social spots are mixed zones with unpredicted position and further reduce the chance to be monitored by the malicious users. Vehicles decide the position of mix zone according to the real-time conditions and exchange their pseudonym sets. Paper [25] proposed a time-slotted pseudonym pools for pseudonym changing. A new pseudonym set is picked from the pseudonym pool to use whenever a new time-slot starts. Vehicle decides whether to exchange pseudonym with another vehicle depends on the speeds, headings and positions information. This approach proposes to change pseudonym candidates among pseudonym pool before they actually using them. A larger scale of pseudonym changing scheme is illustrated in [26], the changing is achieved using a distributed algorithm for shuffling pseudonyms among participated vehicles. Authors use RSUs to shuffle the pseudonyms sets instead of requiring vehicles to find similar movement partners. This pseudonym shuffling scheme proves its feasibility to manage a large number of pseudonym sets in the network.

The above pseudonym changing schemes cause frequent changing of pseudonym certificates' ownership. The original ownership mapping between pseudonym sets and permanent identities changes whenever a pseudonym changing scheme is executed. This however increases the difficulty of accountability service. We proposed to shuffle the used pseudonym sets among edge nodes. The shuffling results are distributed decided by verifying the consensus outcome of Blockchain algorithm. Blockchain helps to broadcast the mined blocks as CRLs and record the shuffling results. This aims to reduce the burden of the central manager and schedule pseudonym shuffling in a more efficient manner. More importantly, the central manager updates the fresh mapping between pseudonym sets and permanent identities by hearing the new blocks.

2.3. Certificate Revocation Schemes

The CRL-based schemes are the most widely used certificate revocation scheme which is proposed by lots of previous contributions such as [9][10]. However the other approaches are still worth to be discussed, including but not limited to the Short-Lived Certificates [27] and Tamper-Proof Device (TPD) schemes [28].

Short-Lived Certificates: The self revoked digital receipts which only valid before it reaches the expire time [27]. Each certificate is designed to have a field to show the valid time in order to control the lifecycle of the certificate. The certificate revocation is achieved by not issuing new certificates to the malicious user. This approach is clearly not suited to the mobile network, especially the VCS. Nodes are required to frequently contact the central manager to update their certificates which results in a huge amount of communication overheads. Moreover, the central manager will suffer from heavy computation burden to generate new certificates.

Tamper-Proof Device: TPD is a hardware device on the On-Board Unit (OBU) of vehicle which contains all the cryptographic materials and operates cryptography and authentication actions [3][28]. The revocation process in the TPD-based scheme is triggered by unicasting a revocation message to the TPD of malicious vehicle. Revocation is achieved by deleting the associated private keys so that the malicious can't generate valid signatures. Although no CRL distribution is needed, it still has two obvious disadvantages. First, TPD needs considerable storage space of a large amount of pseudonym sets. Second, a compromised TPD may refuse to revoke all the certificate. This causes other vehicles still trust the malicious vehicle as they have no knowledge about the revocation list.

Certificate Revocation Schemes: The framework of CRL was proposed in [29], also known as X.509 CRL. The CRL scheme had been further discussed in [9][10]. X.509 CRL-based schemes assume each node follows a copy of CRL which

is issued by the central manager (e.g. Certificate Authority). A certificate is considered as invalid if its digital identifier is contained in CRL. The central manager is responsible to periodically distribute the revoked certificates in order to timely update CRLs among the network. A format of CRL updating message is illustrated in [30]. Three fields are important to the CRL message readers, namely the list of revoked certificates, the name of CRL issuer and the signature of CRL issuer. The list of revoked certificates indicates the certificate identifier, revocation reason and the expiry date which are used for nodes to distinguish the validate of a certificate. Name and signature of the issuer maintain the authenticity and integrity of the CRL message, ensuring the trustworthiness of the CRL message. A node first checks the signature of CRL message when it received a CRL message. The updated list of revoked certificates is added to the local CRL of the node afterwards.

Unfortunately, The size of CRL becomes tedious with the increasing number of revoked vehicles. Additionally, expired certificates should be erased from local CRL. Authors in [31] introduce hash chains to reduce the CRL size. A similar scheme is proposed in [30], it broadcasts a lightweight CRL keychain so that the receivers can calculate the revoked pseudonym certificates using hash chain. However, this scheme is designed for smart meter scenarios since it has less mobility and a smaller amount of nodes. Moreover, it can only revoke self generated certificate but not the shuffled or exchanged pseudonym certificates from other vehicles. [32][33] both focus on the privacy preserving authentication for VCS scenario. Part of the schemes involves the procedures for vehicle revocation. However the procedures only consider the revocation between VCS infrastructures, excluding the revocation methods within vehicles.

2.4. Threat Model

Attackers threat the system security by tracking some specific information with the periodic safety messages. The network security aims to against both external and internal attacks. To prevent the external passive attacks, either local or global, messages are supposed to be encrypted using secret keys. Due to the limited message receiving capability, the local adversary analyses received safety messages from a small area in order to retrieve safety and privacy related information. A global adversary keeps listening and eavesdropping all the safety messages from a wide coverage range of a vehicle network.

The accountability function in this paper major focus on internal attacks. It brings higher threat level comparing to the external attacks as insider attackers are capable to touch and participant in a larger proportion of the network information. A compromised node could spoof safety messages and collaborate with other attackers to track and attack a specific vehicle. An internal adversary could reuse pseudonyms which have been allocated to others, allowing it to confuse the VCS and to attack other nodes. The best way to against insider attack is to revoke the malicious user when an attack happens because its hard to entirely prevent the insider attack from the beginning. Furthermore, adversaries in blockchain networks maybe attempt to insert a false block into the blockchain. Due to the nature of blockchain, its hard to achieve this attack as it requires at least 51% of the total blockchain network's processing power.

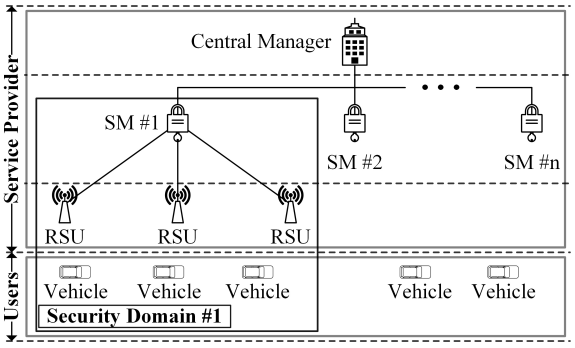

Figure 1. VCS Network Hierarchy [34]

2.5. Our Contributions

To the best of our knowledge, our previous schemes [13][14] are the first time the Blockchain technology has been introduced in VCS applications. Paper [14] illustrates a group key management scheme which helps to distribute group key with minimum message overhead. In [13], the edge node network is used to solve key handover between security domains, rather than forwarding keys to the central authorities. The key handover time between heterogeneous security domains is compressed by introducing the Blockchain structure.

A mature system requires both security and privacy and key management only secure the security purpose. For this reason, privacy is designed to be realised to use pseudonyms and shuffle the pseudonyms regularly. In this paper, we extend our previous idea to support accountability function. However, the difficulties in traditional networks are the central manager is not capable to handle shuffling planning regularly and follow the correct ownership mapping between the pseudonym sets and permanent identities of vehicles. Because the Blockchain concept can be generalised to further system to support accountability, we introduced Blockchain aiming to solve both the problems as the distributed property helps to against the problems. The Blockchain plays the role of shuffling planning, shuffling plan distributor and shuffling result recording. The mid layer infrastructures encapsulate used pseudonym sets into transactions, and the network participants make effort to generate blocks regarding these transactions. The shuffling planning is included in the processes of block preparation. In this way, pseudonym shuffling plans are executed, distributed and stored in Blockchain for the participant nodes to read, as well as for the central manager to update the mapping between permanent identities and pseudonym certificates. Additionally, the misbehaviours are reported to the network by sending transactions with related information.

3. System Framework

3.1. System Model

Nodes in VCS are hierarchically classified into four layers based on different responsibilities, namely central manager,

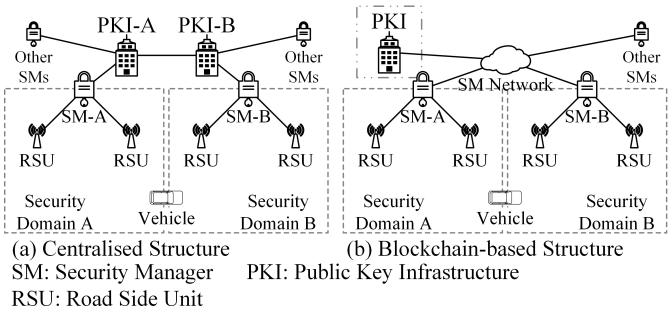

Figure 2. Nerwork structures. (a) Traditional structure (b) Blockchain-based structure

middle layer infrastructures, road side Access Points (APs) and vehicles. Three layers on the side of service providers, while the service user occupies a single layer [34]. As shown in **Fig.1**, the service provider comprises Public Key Infrastructures (PKIs), Security Managers (SMs) and RSUs. The PKI plays the central manager and contains Certificate Authority (CA), Law Enforcement Agency (LEA) and other management infrastructures to support applications. All the security-related cryptographic materials, such as secret key pairs, anonymous credential and pseudonym certificates are created by CA. The tasks of LEA are mapping the pseudonym sets to the permanent identity and identifying all the pseudonym sets of the malicious user. SMs are edge nodes logically below the PKI layer which help PKI to manage cryptography materials. Each SM has their own logical coverage area which is called the security domain. Thus SMs are properly deployed in a geographically sparse manner to handle individual security domain. RSUs act as APs which offer interfaces to bridge messages between the service provider and users. The RSUs have wireless communication devices which can communicate over the wireless medium utilises VCS communication standards (The DSRC in US [3] or/and the C-ITS in EU [35]).

Meanwhile, we assume that each vehicle is equipped with a built-in computerised device known as OBU to support the VCS standards. The vehicle will transmit and receive safety beacon messages with other vehicles and RSUs. These safety beacon messages are collected by RSUs that are built along the road at regular intervals in order to provide maximum network coverage (e.g. the radius of 300 meters in DSRC protocols). The safety beacon message includes a pseudonym, a timestamp and the current vehicle status (e.g. speed, orientation, position and vehicle dimensions). The pseudonym is used to hide the real identity of the vehicle so that the privacy purpose can be guaranteed.

3.1.1. Traditional Network Structure

The traditional structure strictly follows the aforementioned hierarchy. As shown in **Fig.2(a)**, security domains are areas under managing by different SMs and PKIs supervise the network at the top level. The PKI is a trusted authority which provides cryptographic keys, certificate and long-term identity to all legitimate nodes and infrastructures. Each PKI manages multiple numbers of SMs, the number depends on the geographical topology of the area. Moreover, PKIs bridge the connections between different security domains. Inspired by our previous work [13], we introduce SM to cover the security function of VCS. The RSU is a stationary device placed along the roads and at intersections, which is used to gather information about the road traffic and broadcasts it to the OBUs in communication range. Also, an RSU can communicate with other RSUs and the CA to exchange messages related to the road traffic through a secure channel.

3.1.2. Blockchain Based Structure

Different from traditional network structure, PKI is isolated and would be a part of existing authority such as Driver and Vehicle Licensing Agency, as shown in **Fig.2(b)**. The PKI is designed to dedicated generate cryptographic materials for all the nodes and link the pseudonyms of vehicles to their long-term identities. Cryptographic materials, such as vehicle identities, pseudonym certificates and the mapping relationship between pseudonyms and real identity, are supposed to be kept in a secured facility to cope with the privacy and security purposes [36]. Thus the central managers are accessed under the following two situations. **(i)** *Initial Registration*. New vehicles need to apply for the initial registration when they leave the manufacturer and first participate in a new security domain. **(ii)** *Certificate Revocation*. Vehicles are supposed to send messages using pseudonym. Therefore a compromised user could use its pseudonym to launch malicious behaviours. To eliminate the negative effect of the malicious behaviours, the VCS system needs to revoke all the pseudonym certificates which belong to the compromised user. However, the mapping relationships between the permanent identity and the pseudonym sets are stored in the PKI. Thus the certificates (pseudonym and permanent certificates) of the adversary is publicised once the malicious behaviours have been confirmed.

As a result, our proposed Blockchain based structure could enable SMs to distributed shuffling the pseudonym and PKI is capable of keeping the newest mapping between the pseudonym and the permanent identity. All SMs are connected with each other and the PKI on a domain. SMs communication mainly contains pseudonym shuffling and CRL updating. Similar to Bitcoin application, the ledger keeps all transactions from the beginning and is visible to all SMs. Apart from this, all SMs play the role of miners in exchange for accessing the VCS security and privacy services. With this Blockchain based structure, our system could obtain the latest CRL in the shortest possible time since the PKI provides the pseudonym certificates from the latest identity mapping. Finally, the newest CRL is distributed by RSUs to the vehicle nodes.

4. Blockchain Based Certificate Revocation Scheme

We first introduce the prerequisites of the Blockchain based scheme, namely the system initialisation and pseudonym shuffling. The certificate revocation scheme is shown in infrastructure and vehicle scenarios.

4.1. System Initialisation

PKI initialises the system by establishing all the cryptographic materials, include permanent identity, permanent key pairs, pseudonym sets. We assume these credentials are generated by PKIs and distributed to car manufacturers and equipment manufacturers which are responsible to produce vehicles and VCS infrastructures, respectively. All the nodes have their own permanent identities. Each permanent identity contains the identity number $\boldsymbol{ID}_{\mathbf{x}}$, certificate $\boldsymbol{CERT}_{\mathbf{x}}$ and key pairs (private key $\boldsymbol{SK}_{\mathbf{x}}$ and public key $\boldsymbol{PK}_{\mathbf{x}}$) which are used to prove the real node identity, where **x** is the node name. The distribution procedure between PKI and manufacturers is finalised via highly secured connections, such as optical fibre connections.

PKIs generate a certain number of pseudonyms off line and then distributes to vehicles through manufacturer as initial pseudonym sets. Each pseudonym set $\{\boldsymbol{PN_1} \cdots \boldsymbol{PN_n}\}$ contains the corresponding pseudonym certificates $\{\boldsymbol{cert_1} \cdots \boldsymbol{cert_n}\}$ and private/public key pairs $\{\boldsymbol{sk_1}/\boldsymbol{pk_1} \cdots \boldsymbol{sk_n}/\boldsymbol{pk_n}\}$.

4.2. Pseudonym Shuffling

In the proposed Blockchain structure, SMs are responsible to retrieve the 'used' pseudonym sets and reallocate these pseudonym sets. When vehicles running on the road, they will frequently exchange pseudonym followed by certain pseudonym shuffling algorithm. The pseudonym shuffling is supposed to execute within mixed zones which is a geographic region within the VCS environment. Generally speaking, the mixed zone must be selected carefully to maximise the privacy level. For example, traffic junction, roundabout and temporary car park will help a lot to mix the privacy related messages by containing a large number of similar status vehicles. In the mixed zone, each vehicle first cloaks its location information according to the specific cloaking algorithm of the mixed zone [8]. This aims to mix all the vehicle so that the tracking probability can be minimised. The pseudonym shuffling has three steps:

(i) A vehicle changes to a new pseudonym set and marks the previously enabled pseudonym set as '**used**' if the pseudonym set meets its expiry conditions. Upon joining the next mixed zone, the vehicle encapsulates all the used pseudonym sets into a package and sends to the current SM via an RSU.

(ii) SMs will collect used pseudonym sets for a fixed period of time and then aggregate all the pseudonyms in a single package. All the packages are signed by the private key $\boldsymbol{SK}_{\mathbf{SM}}$ of the sender and broadcast to the SM network, hence SMs could assure all pseudonyms are integrity and authenticated. These packages are shared within the SM network and each SM temporary stores a copy of the pseudonym sets in the packages. The stored pseudonym sets are deleted after the pseudonym shuffling finished.

(iii) Due to the fact that every communication between SMs contains timestamps, pseudonym shuffling will be triggered in every fixed interval. When pseudonym shuffling starts, each SM proposes a method about the pseudonym reallocation plan and the reallocated pseudonym sets with same destination SMs are encapsulated into a single transaction. The pseudonym sets are represented by indices in order to reduce the size of the messages. SMs starts the consensus mining algorithm afterwards, such as calculating the PoW. Whoever first finishes the mining process must add the mined block into the Blockchain. The SMs know the shuffling results from the transactions in the mined block. Pseudonym sets are picked according to the indices in the transactions. Finally, SMs delete the temporarily stored pseudonym sets in step (ii) to release the storage space. The shuffling algorithm is demonstrated in **Algorithm.1**.

Algorithm 1 The Pseudonym Shuffling Scheme

for $(x = 1; x \leqslant i; x{+}{+})$ **do**
  $\mathbf{SM_x}$ gathers all the used pseudonyms from mixed zones it manages;
  $\mathbf{PN}^{\mathbf{SM_x}} = \{PN_1^{SM_x} \cdots PN_{n_x}^{SM_x}\}$;
  Counts the number of used pseudonyms sets = n_x;
  Encapsulates $\mathbf{PN}^{\mathbf{SM_x}}$ into package and sends into SM network;
end for
for $(x = 1; x \leqslant i; x{+}{+})$ **do**
  $\mathbf{SM_x}$ picks up all the pseudonym package within SM network;
  Shuffles the sequence of pseudonym sets and **reallocates** to destination PMs;
  Reallocated pseudonym sets which have same destination are encapsulated into a single transaction.
  Encrypt the pseudonym sets use the private key of the destination SM;
end for
All the SMs start **Mining**;
The mining winner broadcasts the **Block** into PM network;
for $(x = 1; x \leqslant i; x{+}{+})$ **do**
  Retrieves new pseudonyms for $\mathbf{SM_x}$;
end for
End Algorithm

4.3. Certificate Revocation

We explain our certificate revocation scheme in two levels, namely the infrastructure level and vehicle level. The infrastructure level based on the pseudonym shuffling scheme in **Algorithm.1** which involves the accountability and CRL distribution, while the revocation on vehicle level is achieved by not issuing group secret key to the malicious vehicles.

4.3.1. Infrastructure Level

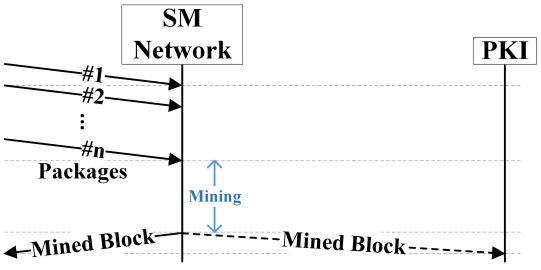

Figure 3. The Message Handshake Of Pseudonym Shuffling Mining

Based on the pseudonym shuffling scheme, the used pseudonym sets are sent to SM network so that SMs can propose new pseudonym allocation plan. According to the network structure, PKI is placed in a relatively isolated environment, but it is still connected with SM network and able to receive messages within SM network. The pseudonym shuffling results are

stored in new blocks and new blocks are broadcasted back to the network. Afterwards, new blocks are attached behind the end of the Blockchain and the Blockchain is updated at each participant SMs simultaneously. In this way, the mechanism of Blockchain helps to execute shuffling, share and store the results.

The PKI also captures the mined block after the mined block broadcasted into the SM network, as shown in **Fig.3**. Due to the fact that PKI has the knowledge of all the cryptographic materials of the network, it is capable of decrypting the transactions and view the reallocation results. We assume PKI maintains an identity mapping table between the nodes' permanent identities and the corresponding pseudonym sets. The identity mapping table is updated based on the pseudonym shuffling plans inside the new blocks so that the latest pseudonym set ownerships are recorded. The updated mapping table is then distributed to SMs which have a chance to contact the malicious vehicles. Similar to the pseudonym shuffling mining processes, the updated mapping table is then added to the blocks and distributed via Blockchain to SMs which have a chance to contact the malicious vehicles. By processing the above procedures, the accountability function can be realised along with the pseudonym shuffling and the CRL can be distributed using only one broadcast message.

As the most critical infrastructure, SMs are assumed to use secure cable connections. However, the worse things happen when SM is compromised by attackers. A compromised SM acts as insider attack to broadcast fake messages, transactions and blocks. Blockchain gives a good solution to against the problem: Due to the consensus mechanism of Blockchain, the computation power of the compromised node must beyond (at least 51% computation power of the entire network) rest of the nodes in order to consistently send out forged blocks and to have them accepted by the Blockchain network. In addition, all pseudonym sets that the compromised SM received from must be revoked in order to keep from further using.

Here we illustrate an example of how PKI updates the mapping between permanent identities and pseudonym sets by hearing the information inside the mined block. The example is based on the following three assumptions: **(i)** There are three vehicles are currently with the mixed zone which are managed by $\mathbf{SM}_1$. These vehicles have permanent identities $\mathbf{ID}_1$, $\mathbf{ID}_2$ and $\mathbf{ID}_3$, respectively. **(ii)** Each vehicle sends out three pseudonym sets which are marked as '**used**'. **(iii)** The volume of the pseudonym set pool in OBUs on the vehicles is set to store maximum five pseudonym sets. These assumptions are just used to assist the expression of the example but not stand the practice situations. The example is shown in **Table.1**, three vehicles are asked to exchange their used pseudonym sets. Each vehicle

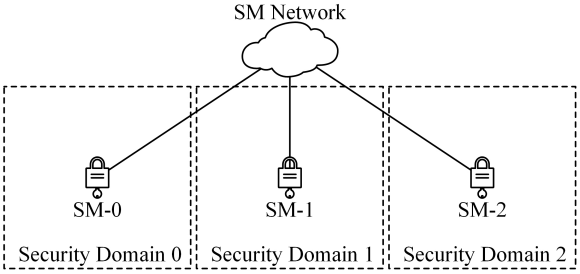

Figure 4. $\mathbf{SM}_1$ And Its Neighbour Security Domains

gives away three pseudonym sets, the original mapping table in PKI is shown in **Table.1 (a)**. The SM network executes the pseudonym shuffling and the final reallocation plan is shared in the form of a mined block. PKI decrypted the transaction to $\mathbf{SM}_1$ from the mined block, the transaction information is demonstrated in **Table.1 (b)**. The updated mapping table substitutes the used pseudonym sets with the reallocated pseudonym sets, as illustrates in **Table.1 (c)**.

Now the PKI get the latest identity mapping information. A CRL can be sent from PKI to $\mathbf{SM}_1$ and its neighbour SMs (e.g. $\mathbf{SM}_0$ and $\mathbf{SM}_2$ in **Fig.4**) if any vehicle in the area of $\mathbf{SM}_1$ involving in malicious behaviours. This aims to inform SMs which have the opportunity to receive the messages from malicious vehicles.

4.3.2. Vehicle Level

The trustfulness and legality of safety beacon information are secured by encrypting the beacon message with a pre-agreed Group Key (GK). As mentioned above, the GK is not given to the malicious vehicle in order to revoke them. This mechanism is only used to forbid the malicious involving in normal network messaging, but not actually deletes the cryptographic materials inside malicious vehicles. Furthermore, by reading the broadcasted CRLs, nodes on the infrastructure level learn these cryptographic materials come from malicious users. Therefore, the remaining cryptographic materials are not capable to further interface the network. The major task of key management at the vehicle level is distributing GK to the authorised vehicles. The membership list of each communication group changes dynamically, hence GK must be updated and redistributed whenever membership changes to provide forward and backward secrecy. Forward secrecy is a mechanism to prevent the departing user from understanding future group broadcast, while backward secrecy means that a fresh member can't obtain information from previous messages. The procedures to update and redistributed GK to the communication participants are called rekeying. In our previous contribution [14], we manage keys based on the

Table 1. An Example of Updating The Identity Mapping Table

Original Mapping Table	
Permanent ID No.	Pseudonym Sets
$\mathbf{ID}_1$	$PN_1, PN_2, PN_3, PN_4, PN_5$
$\mathbf{ID}_2$	$PN_6, PN_7, PN_8, PN_9, PN_{10}$
$\mathbf{ID}_3$	$PN_{11}, PN_{12}, PN_{13}, PN_{14}, PN_{15}$

(a)

→

Transaction for SM_1	
Dest Vehicle ID	Pseudonym Sets
$\mathbf{ID}_1$	PN_6, PN_7, PN_{11}
$\mathbf{ID}_2$	PN_1, PN_{12}, PN_{13}
$\mathbf{ID}_3$	PN_2, PN_3, PN_8

(b)

→

Updated Mapping Table	
Permanent ID No.	Pseudonym Sets
$\mathbf{ID}_1$	$PN_4, PN_5, PN_6*, PN_7*, PN_{11}*$
$\mathbf{ID}_2$	$PN_1*, PN_9, PN_{10}, PN_{12}*, PN_{13}*$
$\mathbf{ID}_3$	$PN_2*, PN_3*, PN_8*, PN_{14}, PN_{15}$

(c)

∗: The updated pseudonym sets

key tree approach. key tree approach structure [37] [38] is one of the most protruding group key management structures. The GK is placed at the root of the tree and user nodes are separated at the termination of branches. Logical key tree bifurcation points are introduced into the key tree approach with corresponding secret keys (Key Encryption Key, KEK) on them. An example of key tree approach is shown in **Figure.5**. The most significant advantage of LKH is the scalability: For a $d-$degree LKH tree with N nodes, the communication overhead for each group rekeying is $d \log_d N$.

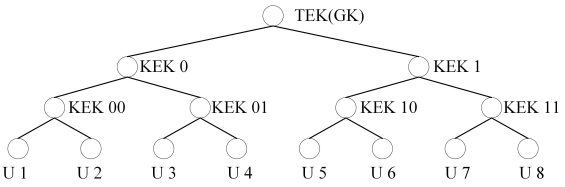

Figure 5. A Typical Structure Of The Key Tree Approach

The safety beacon message consists of a piece of safety information which is encrypted with GK, a digital signature and certificate. A receiver will not read the safety information before the correctness of all these three digital receipts are checked. The final object of certificate revocation is to prevent vehicles from reading the safety beacon messages with fake information inside. For this reason, SMs can finalise the certificate revocation by not issuing valid GK to the malicious user. For example in **Figure.5**, user $U1$ is found involving in malicious behaviours. The next rekeying messages should update users with new secret keys, excluding $U1$, as shown below:

$$Enc\{KEK_{00}^{new}, KEK_{0}^{new}, GK^{new}\}_{PK_{U2}} \rightarrow U2$$
$$Enc\{KEK_{0}^{new}, GK^{new}\}_{KEK_{01}} \rightarrow U3, U4$$
$$Enc\{GK^{new}\}_{KEK_{1}} \rightarrow U5, U6, U7, U8$$

4.4. Accountability Report

To realise the certificate revocation function, the revocation system should have a mechanism to report the malicious behaviour to the PKI. RSUs in [30] [32] [33] are designed to send a dedicated message to PKI in order to report the malicious actions. Alternatively, we propose to embed the accountability report function within either the key management scheme in [13] or the pseudonym shuffling scheme, aiming to reduce the communication overhead. Based on the above idea, SM encounter communications with the SM network under two situations: **(i)** The system needs to shuffle the pseudonym sets to protect privacy. **(ii)** The system has key handover requirements. Consider VCS covers multiple security domains and large number of vehicle nodes, these two situations happen frequently (no less than one times per second [13]). The proposed accountability report mechanism starts with the initial malicious behaviour detection. SM waits for the next communication opportunity with the SM network before sends out all the collected malicious report. Finally, the PKI receives the reports and starts the CRL distribution task. A complete certificate revocation procedures are displayed in **Algorithm.2**

Algorithm 2 The Certificate Revocation Procedures For PKI and SMs

Algorithm For PKI:
Hear messages in the SM network;
if (New Block Comes In the SM Network) **then**
    Update **mapping** between permanent identity and pseudonym sets;
else if (New Messages Contains Report Of Malicious Behaviours) **then**;
    Look up the **mapping** of the malicious user;
    Prepare the updated **CRL**;
    Find SMs around the malicious user **SM** = $\{SM_1 \cdot SM_n\}$;
    Sends **CRL** $\rightarrow$ **SM**;
end if
End Algorithm
Algorithm For SM:
SM hears messages from SM network and RSUs;
if (New Messages Contains Report Of Malicious Behaviours) **then**
    Packet the report into a **package** with other messages;
    if (New Time Slot Of Forwarding Messages Starts) **then**
        Forward the **Package** to SM network;
    end if
else if (New **CRL** From PKI **then**
    Inform RSUs not to update Group Key according to **CRL**;
end if
End Algorithm

4.5. Block format

Table 2. The Format of Transaction

Transaction Header
Hashed Transaction Header
Transaction No.
Transaction Type
Source SM
Destination SM
Digital Signature
Payload: (Encrypted Transaction Information) $Ciphertext = Enc\{Information\}_{PK_{SM-dest}}$

Table.2 shows the format of each transaction in the block which contains transaction header and payload. In the transaction header, the number of this transaction gives the position where the transaction locates in the Blockchain. Transaction type indicates the purpose of the transaction, either the privacy preserving or security reinforcement. the source and destination SM address are similar to bitcoin input and output [12]. The signature occupies the last position of the transaction to maintain the authentication, integrity, and non-repudiation of key transfer information.

Table 3. The Format of Block

Block Header	
Field	Description
Version	Block Version Number
Previous Block Hash	Hash of the previous block in the chain
Merkle Tree Root	Hash of the merkle tree root $Root_M$
Timestamp	Creation time of this block
Consensus Receipt	Information about the consensus algorithm
Block Payload (Transactions)	
Transaction No.1 $\cdots$ Transaction No.n	

The block is designed for containing all transactions and attaching it into blockchain. The format of a block is shown in **Table.3**. The first row shows the block number which is the sequence number of the whole Blockchain. The previous block hash links this block to its parent one. This hash structure makes blocks attached with each and generates a chain structure. The Merkle tree root is used for securing the transactions integrity [39]. All transactions in this block are joined into the Merkle tree root, so that any alteration on any transactions would cause a different value of Merkle root value. Similarly to bitcoin, we add a timestamp to prove that this block of transactions has existed and to prevent from time tempering. The consensus receipt field includes the digital materials to calculate and verify the consensus algorithm, the targeted difficulty and nonce are illustrated if the current Blockchain uses the proof of work algorithm [16]. The payload field contains the aforementioned transactions that the block creator randomly allocated.

4.6. Consensus algorithm

The nature of consensus in Blockchain is a distributed way to establish an agreement between a group of nodes, instead of relying on the central manager's decision. The most well known consensus method is Proof of Work (PoW) which is calculated by trying multiple hushes. The PoW system originally was proposed for being able to deter spam email. All proof-of-work applications (e.g bitcoin) require participated nodes contribute a significant amount of computation power to obtain a digital proof that can be verified easily. The procedure that nodes contribute their computation power to solve the mathematical question and obtain the proof of work is called mining. Whoever that solved the question first is able to attach its block into the chain. In this paper, consensus algorithm mainly used to distribute decide pseudonym shuffling plan among SMs and record the most updated mapping between pseudonym sets and permanent identities in new blocks. The PoW with low difficulty is proposed in this approach as all the SMs have identical processing modules inside and they are assumed to link with highly secured wire connections. The low difficulty allows a short PoW computation time, resulting in efficient consensus.

5. Performance Evaluation

The performance evaluation of the proposed certificate revocation scheme was carried out using simulations. The simulations enforce the revocation processes to produce the final results. The performances are quantified by measuring the system efficiency of the proposed scheme comparing to the benchmark. Performance evaluation analyses the system efficiency in two parts:

Proecssing Time: This part includes the handshake processing time to process accountability and revocation.

Overhead: The comparison of message overhead and processing time between the Blockchain structure and the traditional structure is demonstrated as another metric. The CRL distribution benchmarks are based on the X.509 [29] and optimised X.509 CRL in [40].

Finally, a brief analysis of the capability to support security services within the Blockchain network is illustrated.

5.1. Simulation Assumptions

Our result is generated using OMNeT++ 4.5 [41][42] with the dedicated network simulation (Veins) packet [42]. Elliptic Curve Integrated Encryption Scheme (ECIES)[43] with elliptic curve secp160r1 in Crypto++ [44] is selected not only for cryptographic scheme ECIES, but Elliptic Curve Digital Signature Algorithm (ECDSA) as well. Cipher block has a length of 75 bytes which is because ECIES provides much better security level. 20 bytes are used to store the security and privacy information in transactions. Due to the fact that SMs are trusted entities, the PoW mining difficulty of each block is set to 3 which allows a short PoW computation time, resulting in efficient consensus. We simulated that blocks are mined by our laptop with Intel Core i5 and 8GB RAM and display card GeForce 920M. This device can complete 250K hash calculations per second. Other parameters come from VCS standards [3] and [5], including using frequency of 5.9 GHz and safety beacon message frequency 10 times per second.

5.2. Certificate Revocation List Size

The CRL size in the X.509 CRL [29] defines that each entry in the 'Revoked Certificates' field consists of 39 bytes, including a long serial number of revoked certificate, revocation date and revocation reason for 6 bytes, 13 bytes and 12 bytes, respectively. The mandatory fixed fields in X.509 CRL occupies 400 bytes [40]. This CRL is initially broadcasted to the infrastructures (SM or RSU) and next distributed to vehicles via RSU access points. An optimised X.509 CRL scheme in [40] proposes to compress the size of mandatory fixed fields in X.509 CRL so that only 39 bytes are needed for each revocation element. Based on the pseudonym shuffling and certificate revocation algorithms in Section 4.2 and Section 4.3, SMs use the indices to reduce the message size. Moreover, the mandatory fixed fields are removed since our CRLs only circulate among the VCS infrastructure network which consists of trust nodes. We refer to the information size in [29], each certificate index requires 6 bytes (the long serial number). The CRL in the Blockchain based scheme is only distributed among VCS infrastructures. Therefore, the total size of X.509 based CRL schemes and our proposed CRL can be calculated as follows, we assume $n_{revoked}$ is the number of revoked certificates:

Among VCS Infrastructures:

X.509 CRL size = $(400 + n_{revoked} \times 39)$ bytes
Optimiesed X.509 CRL size = $n_{revoked} \times 38$ bytes
Blockchain Based scheme CRL size = $n_{revoked} \times 6$ bytes

Among Vehicles:

X.509 CRL size = $(400 + n_{revoked} \times 39)$ bytes
Optimiesed X.509 CRL size = $n_{revoked} \times 38$ bytes
Blockchain Based scheme CRL size = 0

The sizes of the X.509 CRL, optimised X.509 CRL in [40] and the CRL in Blockchain based scheme are shown in **Fig.6**

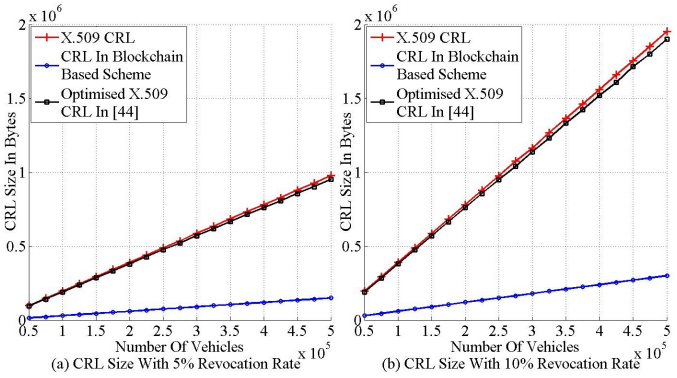

Figure 6. CRL Size Among Infrastructures In Terms Of Vehicle Number

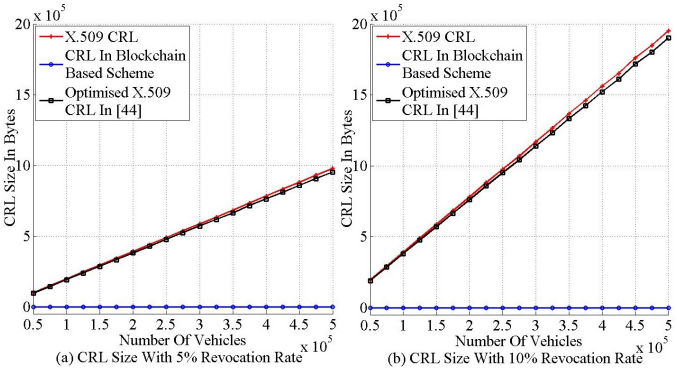

Figure 7. CRL Size Among Vehicles In Terms Of Vehicle Number

and **Fig.7** regarding to different number of vehicles and certificate revocation rates. The upper and the lower amounts of the vehicle are considered between 50,000 to half million, which is considered to cover most traffic conditions. Two revocation rate, 10% and 5% are assumed to provide a various number of revocation requests. **Fig.6** shows CRL sizes among infrastructure network, optimised scheme in [40] achieves minor improvement comparing to the X.509 CRL as it deletes some redundancy fields in the CRL header. The proposed scheme decreases the CRL size significantly comparing to the X.509 CRL scheme. The results of X.509 CRL sizes are approximately eight times of the results in Blockchain based scheme which is because the X.509 CRL introduces too many profile fields, such as mandatory fields, reason code and revocation proof [40]. Due to the fact that the vehicle level revocation in the Blockchain based scheme is realised by removing the malicious user out of the communication group, thus the CRL is only distributed to the infrastructure level, resulting zero CRL size on the vehicle level. The CRL sizes in vehicle level are illustrated in **Fig.7**.

5.3. Revocation Overhead And Processing Time

A comparison of the communication handshake procedures between the X.509 CRL, optimised X.509 CRL and the Blockchain based certificate revocation scheme is shown in **Fig.8**. In the traditional X.509 certificate revocation scheme and the optimised X.509 CRL scheme in [40], a report about the malicious behaviour is sent to the PKI to check and prepare the

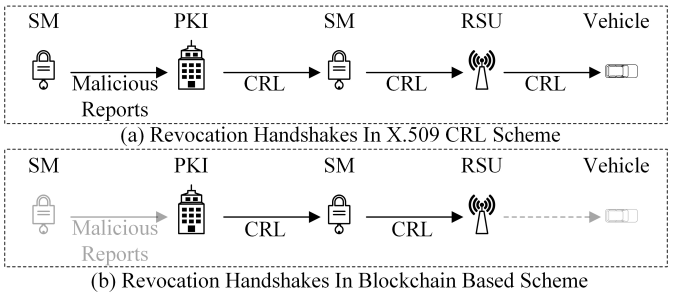

Figure 8. Handshake Procedures Of The Certificate Revocation Schemes

CRL. PKI sends back the updated CRL to RSUs through SM. Finally RSUs are responsible for distributing the CRL to vehicles, as shown in **Fig.8(a)**. In **Fig.8(b)**, different from the X.509 scheme, the Blockchain based scheme embeds the malicious report within the other service messages which are sent to SM network by SMs. Furthermore, RSU does not need to distribute CRL to vehicles as the malicious user is excluded from the group key management. Due to the fact that the message overhead increases linearly in terms of the growing number of revocation broadcast, the Blockchain based certificate revocation scheme reduces one-third of the message overheads comparing to the X.509 based schemes among the infrastructure level. Furthermore, our proposed scheme achieves zero message overhead which is caused by CRL distribution.

Table 4. The Overhead Comparison Between CRL Schemes

Scenario	Scheme	Overhead/CRL Distribution
Infrastructure Level	X.509 CRL (**Fig.8(a)**)	3 Broadcasts
	CRL in [40] (**Fig.8(a)**)	3 Broadcasts
	Blockchain-CRL (**Fig.8(b)**)	2 Broadcasts
Vehicle Level	X.509 CRL (**Fig.8(a)**)	1 Broadcast
	CRL in [40] (**Fig.8(a)**)	1 Broadcasts
	Blockchain-CRL (**Fig.8(b)**)	0 Broadcast

The message overhead for the infrastructure and vehicle levels are shown in **Table.4**, we can see the X.509 based scheme cost an extra handshake step on the infrastructure level in order to report the malicious behaviour to PKI, while the Blockchain based scheme removes this step by meriting the report with other messages. Similar to the infrastructure level, the Blockchain base scheme revokes malicious user by not containing it to the communication group, thus there has no CRL broadcast step in vehicle level.

Table 5. Average Cryptography Processing Time [13]

Cryptography Scheme	Processing Time (Milliseconds)
ECIES Encryption	0.51027
ECIES Decryption	0.73996
ECDSA Signing	0.51011
ECDSA Verifing	1.10171

Based on the message handshake procedures in **Fig.8**, in order to assure message integrity and authenticity, each message exchange involves signature verification, signature generation, ciphertext decryption and encryption. **Table.5** records the time cost to process ECC-based cryptographic schemes on our computer. Generally speaking, messages should be encrypted and

attached a digital signature before it is sent to the next node. The receiver checks the correctness of the signature, decrypts the ciphertext to process the message if receives a new message. Therefore, the traditional network needs 4 encryptions, signings, verifications and decryptions to finish one CRL distribution process, overall costs 11.4482 milliseconds, while the Blockchain based scheme only requires half of the efforts (5.7241 ms).

5.4. Time Cost To Update CRL

Two reasons that the proposed scheme gives fewer message overheads are the efficient CRL updating mechanism and the malicious reports which are embedded with other service messages. Although the mechanisms help to optimise the certificate revocation performance, the impacts on the VCS network still need to be discussed.

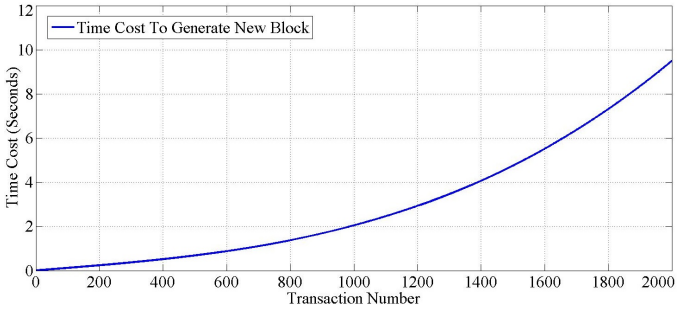

Figure 9. Time Cost From Transaction Broadcast To Block Broadcast

As mentioned in Section 4, the PKI updates the CRL by listening to the mined block from the SM network, thus the processing time to generate a block is considered. The processing time consists of message propagation, block preparation, mining and cryptographic materials preparation. We acquire each time component from our previous contribution [13] and calculate the result of total time cost to update CRLs in PKI. As can be seen in **Fig.9** the total time increases exponentially when the transaction number grows. The results are count from the transactions first joining the network to the mined block broadcasting back to SM network. The Blockchain base system can support 600 and 1000 transactions within one and two seconds, respectively.

Table 6. The Number Of Roads Can Blockchain System Support

Vehicles /hour/road	Vehicles Handover/Sec	Malicious Report/Sec	Vehicles /Mixed Zone	Roads Can Support	
				1 Sec	2 Sec
3,000	0.83	0.08	4	122.2	171.82
6,000	1.67	0.17	8	60.97	85.62
9,000	2.50	0.25	12	40.68	57.14
12,000	3.33	0.33	16	30.52	42.88
15,000	4.16	0.42	20	24.41	34.29

The number of roads which can be supported by Blockchain system are considered as metric to measure the performance, as shown in **Table.6**. The last two columns are the results under Blockchain mining frequency of one and two seconds. Considering the rush hours have 15,000 vehicles passing a highway each hour in Beijing, the busiest city in the world [13], which means there have an average four key handover transactions. Meanwhile the off peak hours have only 3000 vehicles passing a highway in one hour. We evaluate the maximum certificate revocation rate of 10%. Here assume during rush hours there has mixed zone on each road (e.g. traffic light, roundabout, etc.) and 20 vehicles within the mixed zone who require to change their pseudonym sets. For lower traffic levels the number of vehicles within mixed zone decrease proportionally. To this account, around 25 transactions are forwarded to the SM network per second per road during rush hours. That means the Blockchain based system is capable to support the security, privacy and revocation services for approximately 25 highways in one second and 34 highways in two seconds. From another perspective, the network burden caused by reporting the malicious behaviour occupies no more than 4% of the Blockchain resources which is considered as an acceptable range.

6. Conclusion

In this paper, a novel certificate revocation scheme for preventing insider attacks in VCS networks is proposed. Our scheme introduces Blockchain concept and reduces the CRL size and the broadcast message overheads. The proposed Blockchain structure allows the PKI to keep tracing the ownership of pseudonym sets and distribute the CRL in an efficient manner. We developed an effective malicious behaviour report mechanism. Part of the CRL distribution is combined with the group key management scheme to minimise the message overhead of certificate revocation. Two CRL scenarios are discussed separately, namely the infrastructure level and the vehicle level. We first studied the CRL sizes of different schemes which prove the Blockchain base scheme is capable to significantly compress the size of CRL. Secondly, by analysing the message handshake procedures between infrastructures and vehicles in VCS, our Blockchain structure achieves more efficiency and robustness compared to the traditional structure since the Blockchain provides a distributed network structure. The results of message overheads between certificate revocation scheme demonstrate the Blockchain based scheme releases the communication burden by reducing the overall number of broadcast messages.

Our future work focuses to further take optimise the entire Blockchain network, including the investigation of more efficient consensus algorithm and further analysis of the combination of security, privacy and accountability. In the future, the extension of our work aims to analysis with additional performance measurements, including but not limited at message latency, delivery ratio, identity tracking probability and computation overhead. Moreover, our future work should involve a complete performance evaluation so that users are able to decide the trade-off between security and privacy.

References

[1] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, J.-P. Hubaux, Secure vehicular communication systems: design and architecture, Communications Magazine, IEEE 46 (11) (2008) 100–109. doi:10.1109/MCOM.2008.4689252.

[2] Y. Cao, N. Wang, G. Kamel, Y. J. Kim, An electric vehicle charging management scheme based on publish/subscribe communication framework, IEEE Systems Journal PP (99) (2015) 1–14. doi:10.1109/JSYST.2015.2449893.

[3] J. B. Kenney, Dedicated short-range communications (dsrc) standards in the united states, Proceedings of the IEEE 99 (7) (2011) 1162–1182.

[4] H. Hartenstein, K. Laberteaux, A tutorial survey on vehicular ad hoc networks, Communications Magazine, IEEE 46 (6) (2008) 164–171. doi:10.1109/MCOM.2008.4539481.

[5] T. ETSI, 102 637-2, intelligent transport systems (its); vehicular communications; basic set of applications; part 2: Specification of co-operative awareness basic service, ETSI, Sophia Antipolis Cedex, France.

[6] D. SAE, J2735 dedicated short range communications (dsrc) message set dictionary, Society of Automotive Engineers, DSRC Committee.

[7] B. Zhou, Q. Chen, P. Xiao, L. Zhao, On the spatial error propagation characteristics of cooperative localization in wireless networks, IEEE Transactions on Vehicular Technology 66 (2) (2017) 1647–1658. doi:10.1109/TVT.2016.2555329.

[8] P. Asuquo, H. Cruickshank, J. Morley, C. P. A. Ogah, A. Lei, W. Hathal, S. Bao, Z. Sun, Security and privacy in location-based services for vehicular and mobile communications: An overview, challenges and countermeasures, IEEE Internet of Things Journal (2018) 1–1doi:10.1109/JIOT.2018.2820039.

[9] P. P. Papadimitratos, G. Mezzour, J.-P. Hubaux, Certificate revocation list distribution in vehicular communication systems, in: Proceedings of the Fifth ACM International Workshop on VehiculAr Inter-NETworking, VANET '08, ACM, New York, NY, USA, 2008, pp. 86–87. doi:10.1145/1410043.1410062.
URL http://doi.acm.org/10.1145/1410043.1410062

[10] K. P. Laberteaux, J. J. Haas, Y.-C. Hu, Security certificate revocation list distribution for vanet, in: Proceedings of the Fifth ACM International Workshop on VehiculAr Inter-NETworking, VANET '08, ACM, New York, NY, USA, 2008, pp. 88–89. doi:10.1145/1410043.1410063.
URL http://doi.acm.org/10.1145/1410043.1410063

[11] T. ETSI, Etsi ts 102 867 v1.1.1, intelligent transport systems (its); security; stage 3 mapping for ieee 1609.2, ETSI, Sophia Antipolis Cedex, France.

[12] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system (2008).

[13] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, Z. Sun, Blockchain-based dynamic key management for heterogeneous intelligent transportation systems, IEEE Internet of Things Journal PP (99) (2017) 1–1. doi:10.1109/JIOT.2017.2740569.

[14] A. Lei, C. Ogah, P. Asuquo, H. Cruickshank, Z. Sun, A secure key management scheme for heterogeneous secure vehicular communication systems, ZTE Communications 21 (2016) 1.

[15] C. Decker, R. Wattenhofer, Information propagation in the bitcoin network, in: IEEE P2P 2013 Proceedings, 2013, pp. 1–10. doi:10.1109/P2P.2013.6688704.

[16] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, 1st Edition, O'Reilly Media, Inc., 2014.

[17] G. Danezis, S. Meiklejohn, Centrally banked cryptocurrencies, arXiv preprint arXiv:1505.06895.

[18] G. Zyskind, O. Nathan, A. . Pentland, Decentralizing privacy: Using blockchain to protect personal data, in: Security and Privacy Workshops (SPW), 2015 IEEE, 2015, pp. 180–184. doi:10.1109/SPW.2015.27.

[19] A. Dorri, M. Steger, S. S. Kanhere, R. Jurdak, Blockchain: A distributed solution to automotive security and privacy, IEEE Communications Magazine 55 (12) (2017) 119–125. doi:10.1109/MCOM.2017.1700879.

[20] Z. Yang, K. Yang, L. Lei, K. Zheng, V. C. M. Leung, Blockchain-based decentralized trust management in vehicular networks, IEEE Internet of Things Journal (2018) 1–1doi:10.1109/JIOT.2018.2836144.

[21] D. Eckhoff, C. Sommer, T. Gansen, R. German, F. Dressler, Strong and affordable location privacy in vanets: Identity diffusion using time-slots and swapping, in: 2010 IEEE Vehicular Networking Conference, 2010, pp. 174–181. doi:10.1109/VNC.2010.5698239.

[22] L. Buttyán, T. Holczer, I. Vajda, On the effectiveness of changing pseudonyms to provide location privacy in vanets, in: ESAS, Vol. 4572, Springer, 2007, pp. 129–141.

[23] R. Lu, X. Lin, T. H. Luan, X. Liang, X. Shen, Anonymity analysis on social spot based pseudonym changing for location privacy in vanets, in: 2011 IEEE International Conference on Communications (ICC), 2011, pp. 1–5. doi:10.1109/icc.2011.5962919.

[24] R. Lu, X. Lin, T. H. Luan, X. Liang, X. Shen, Pseudonym changing at social spots: An effective strategy for location privacy in vanets, IEEE Transactions on Vehicular Technology 61 (1) (2012) 86–96. doi:10.1109/TVT.2011.2162864.

[25] D. Eckhoff, R. German, C. Sommer, F. Dressler, T. Gansen, Slotswap: strong and affordable location privacy in intelligent transportation systems, IEEE Communications Magazine 49 (11) (2011) 126–133. doi:10.1109/MCOM.2011.6069719.

[26] H. Artail, N. Abbani, A pseudonym management system to achieve anonymity in vehicular ad hoc networks, IEEE Transactions on Dependable and Secure Computing 13 (1) (2016) 106–119. doi:10.1109/TDSC.2015.2480699.

[27] M. Jakobsson, S. Wetzel, Efficient attribute authentication with applications to ad hoc networks, in: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, VANET '04, ACM, New York, NY, USA, 2004, pp. 38–46. doi:10.1145/1023875.1023882.
URL http://doi.acm.org/10.1145/1023875.1023882

[28] M. Raya, D. Jungels, P. Papadimitratos, I. Aad, J.-P. Hubaux, Certificate revocation in vehicular networks, Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences, EPFL, Switzerland.

[29] R. Housley, W. Polk, W. Ford, D. Solo, Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile, http://www.rfc-editor.org/rfc/rfc3280.txt, online; accessed 04 July 2017 (2002).

[30] M. M. E. A. Mahmoud, J. Misic, K. Akkaya, X. Shen, Investigating public-key certificate revocation in smart grid, IEEE Internet of Things Journal 2 (6) (2015) 490–503. doi:10.1109/JIOT.2015.2408597.

[31] Y. Sun, R. Lu, X. Lin, X. Shen, J. Su, An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications, IEEE Transactions on Vehicular Technology 59 (7) (2010) 3589–3603. doi:10.1109/TVT.2010.2051468.

[32] U. Rajput, F. Abbas, H. Oh, A hierarchical privacy preserving pseudonymous authentication protocol for vanet, IEEE Access 4 (2016) 7770–7784. doi:10.1109/ACCESS.2016.2620999.

[33] U. Rajput, F. Abbas, H. Eun, H. Oh, A hybrid approach for efficient privacy-preserving authentication in vanet, IEEE Access 5 (2017) 12014–12030. doi:10.1109/ACCESS.2017.2717999.

[34] M. Raya, P. Papadimitratos, J. p. Hubaux, Securing vehicular communications, IEEE Wireless Communications 13 (5) (2006) 8–15. doi:10.1109/WC-M.2006.250352.

[35] A. Festag, Cooperative intelligent transport systems standards in europe, IEEE Communications Magazine 52 (12) (2014) 166–172. doi:10.1109/MCOM.2014.6979970.

[36] R. Schlegel, C. Y. Chow, Q. Huang, D. S. Wong, User-defined privacy grid system for continuous location-based services, IEEE Transactions on Mobile Computing 14 (10) (2015) 2158–2172. doi:10.1109/TMC.2015.2388488.

[37] C. K. Wong, M. Gouda, S. Lam, Secure group communications using key graphs, Networking, IEEE/ACM Transactions on 8 (1) (2000) 16–30. doi:10.1109/90.836475.

[38] H. Harney, E. Harder, Logical key hierarchy protocol, Tech. rep., Internet draft (1999).

[39] R. C. Merkle, A digital signature based on a conventional encryption function, in: Advances in Cryptology, CRYPTO87, Springer, 1987, pp. 369–378.

[40] M. N. M. Bhutta, H. Cruickshank, Z. Sun, Public-key infrastructure validation and revocation mechanism suitable for delay/disruption tolerant networks, IET Information Security 11 (1) (2017) 16–22. doi:10.1049/iet-ifs.2015.0438.

[41] A. Varga, et al., The omnet++ discrete event simulation system, in: Proceedings of the European simulation multiconference (ESM2001), Vol. 9, sn, 2001, p. 65.

[42] C. Sommer, R. German, F. Dressler, Bidirectionally coupled network and road traffic simulation for improved ivc analysis, Mobile Computing, IEEE Transactions on 10 (1) (2011) 3–15.

[43] D. Hankerson, A. J. Menezes, S. Vanstone, Guide to elliptic curve cryptography, Springer Science & Business Media, 2006.

[44] W. Dai, Crypto++ library 5.6. 0, http:/www. cryptopp. com.