cryptography

MDPI

Article

Certificate Management Scheme for VANETs Using Blockchain Structure

Maharage Nisansala Sevwandi Perera [1,*], Toru Nakamura [2], Masayuki Hashimoto [2], Hiroyuki Yokoyama [1], Chen-Mou Cheng [3] and Kouichi Sakurai [4]

[1] Adaptive Communications Research Laboratories, Advanced Telecommunications Research Institute International (ATR), Kyoto 619-0288, Japan; hr-yokoyama@atr.jp
[2] KDDI Research, Inc., Saitama 356-8502, Japan; tr-nakamura@kddi.com (T.N.); masayuki.hashimoto@atr.jp (M.H.)
[3] Graduate School of Natural Science and Technology, Kanazawa University, Kanazawa 920-1192, Japan; cheng@se.kanazawa-u.ac.jp
[4] Department of Information Science and Technology, Graduate School and Faculty of Information Science and Electrical Engineering, Kyushu University, Fukuoka 819-0395, Japan; sakurai@inf.kyushu-u.ac.jp
[*] Correspondence: perera.nisansala@atr.jp

Abstract: Vehicular Ad-hoc NETworks (VANETs), a special kind of Mobile Ad-hoc NETworks (MANETs), play an important role in Intelligent Transportation Systems (ITS). Via wireless technology, vehicles exchange information related to road conditions and their status, and, thereby, VANETs enhance transportation safety and efficiency. A critical aspect of VANETs is providing privacy for the vehicles. The employment of pseudonym certificates is a well-known solution to the privacy problems in VANETs. However, certificate management faces challenges in renewing certificates and revoking vehicles. The centralized certificate management, especially resulting in the delay of the revocation process, harms the nodes of VANETs. This paper proposes a blockchain structure-based certificate management for VANETs and voting-based revocation to halt misbehaving vehicles' actions. Moreover, this paper presents extended privacy for the participants of the voting process using ring signatures.

Keywords: VANET; pseudonym certificates; certificate revocation; blockchain; public key encryption; e-voting; ring signatures

check for updates

Citation: Perera, M.N.S.; Nakamura, T.; Hashimoto, M.; Yokoyama, H.; Cheng, C.-M.; Sakurai, K. Certificate Management Scheme for VANETs Using Blockchain Structure. *Cryptography* **2022**, *6*, 20. https://doi.org/10.3390/cryptography6020020

Academic Editors: Duc-Phong Le, Rongxing Lu, Jun Shao and Cong Zuo

Received: 15 March 2022
Accepted: 19 April 2022
Published: 25 April 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

With the increasing number of vehicles on the road, urban traffic congestion has become critical. On the other hand, each year, the world's economy loses as much as 500 billion dollars due to traffic accidents [1], and, according to the World Health Organization [2,3] every year, over 1.35 million people are killed on the roads. The Vehicle Ad-hoc NETworks (VANETs), one of the fundamental components of Intelligent Transportation Systems (ITSs), enable vehicles to exchange road conditions and their status via wireless communication systems to alleviate road accidents and improve safe driving. VANETs provide road safety by informing vehicle positions and warning of out-of-sight collisions and reducing traffic congestion by monitoring traffic. Moreover, VANETs assist drivers, quickly reacting to driver's errors and priority vehicles like ambulances, issuing notifications about their approach to other vehicles [4]. As a result, VANET ensures the safety and efficiency of transportation systems and provides comfort for drivers and passengers. Typically, each vehicle is tailored with wireless On-Board Units (OBUs) to communicate with other vehicles (V2V) and infrastructure (V2I). Road-Side Units (RSUs), which are set up along roads, act as Internet providing units and message propagators specifically distributing updated messages received from infrastructure services and supplying road-related extra information to vehicles. The VANET architecture consists of the OBUs (vehicles, sometimes we call nodes), RSUs, and a central authority (CA) who is responsible for registering OBUs and RSUs and maintaining the system. When OBUs are on the road, CA communicates with them through RSUs. Other than V2V and V2I communication, VANETs provide I2I and V2X communication (where X is any device with Internet) [5]. Figure 1 depicts the architecture of a basic VANET system.

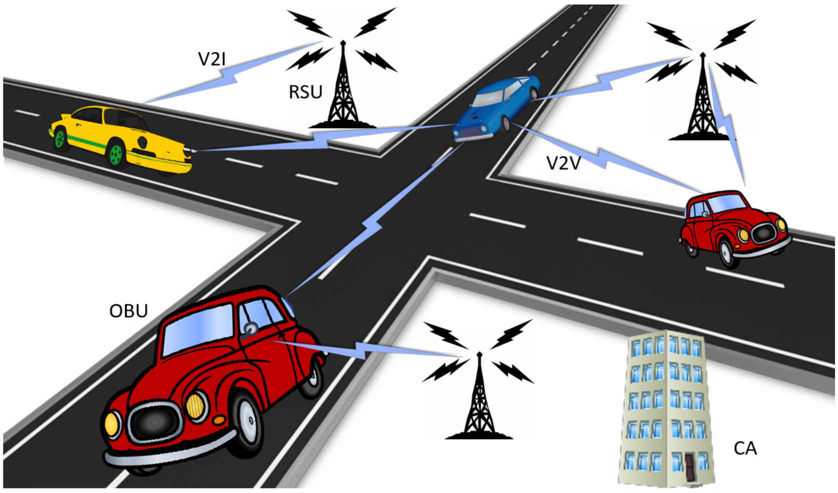

Figure 1. Architecture of the VANET system.

Vehicles should periodically transmit status messages, including position and speed, to achieve a high level of awareness. Basic safety messages (BSMs) consist of status information, and BSMs are broadcast as warning messages to prevent collisions. BSMs are broadcast at high speed and typically without encrypting them to allow fast processing. Thus, it makes the content of BSMs vulnerable to privacy attacks. It required authentication of vehicles to mitigate the security attacks that can happen in the wireless communication in VANETs. As a result, Public Key Infrastructure (PKI) based authentication systems became common in VANETs. PKI creates all the pseudonym-related cryptographic candidates like pseudonym certificates. The use of pseudonyms to secure the privacy of vehicles in V2X was first suggested by the SeVeCom project [6]. The survey presented by Petit et al. [7] discussed different approaches of the pseudonym-based VANETs. In VANETs, vehicles send messages with a certificate to support authentication of the vehicle. Pseudonyms (pseudonym certificates, sometimes call certificates) are temporary identifiers that hide the vehicle's real identity but show that the vehicle is part of the network. However, in order to prevent vehicle tracking, it is required to change the pseudonyms frequently [8].

As depicted in Figure 2, when a vehicle with a unique vehicle id *vid* requests pseudonyms, the pseudonym issuing authority (central authority CA) validates *vid* and issues pseudonym credentials to the vehicle. Since the maintenance of a single pseudonym is vulnerable to attacks, VANETs use a set of pseudonyms for each vehicle. Typically pseudonyms are assigned with an expiry date or validity period. Short validity periods and expiry dates ensure security against Sybil attacks. Sheikh et al. [9] pointed out that the Sybil attack is one of the most dangerous security attacks in VANETs. The message sending vehicle uses a valid pseudonym to authenticate himself as a valid user. However, the unlinkability property of pseudonyms prevents message receivers from understanding that these messages are originated from a single node without performing additional plausibility checks, such as position verification [10]. Thus, a mischievous vehicle may try to obtain advantages like clearing the path ahead of him by providing fake messages. VANETs require fresh pseudonyms to authenticate a vehicle to prevent such kinds of forgeries. Expired pseudonyms should not be used. Some approaches provide pre-loading of many pseudonyms sufficient for a few years, and some provide refilling of pseudonyms periodically from the pseudonym issuer. On the other hand, in traditional VANETs, if an RSU or a vehicle detects a misbehaving vehicle(s), it will report the incident to CA, the pseudonym issuing authority. After confirming the misbehavior, CA will add all pseudonym certificates of the misbehaving vehicle to the certificate revocation list CRL. The pseudonym issuing party—CA—may hold escrow information linking to pseudonym certificates that he provides. Thus, CA gains the ability to revoke the anonymity of vehicles by linking pseudonyms to the *vid* of each vehicle. Periodically, CA broadcasts CRL, and the message verifiers use updated CRL for authenticating a received message. The existing CRL updating methods suffer from drawbacks like CRL size growth, causing latency in the authentication of received messages.

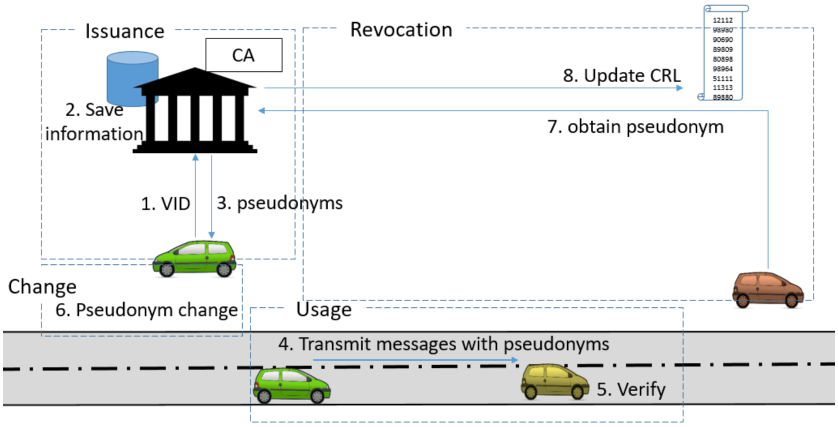

Figure 2. Life cycle of Pseudonym.

Addressing the size increase of CRL in VANETs, Verheul et al. [11] and Simplicio et al. [12] proposed a certificate management method from activation codes. As titled in Verheul et al. [11] work, it is an issue first activate later (IFAL) method. Vehicles obtain a set of inactive certificates first and periodically receive activation codes for the certificates. When a vehicle misbehaves, the authority will stop issuing future activation codes for that vehicle. Thus, that vehicle becomes revoked. However, still, the existing IFAL proposals are centralized. Centralized revocation involves considerable time delay due to reporting, investigation, updating CRL with numerous misbehaving vehicles' certificates, and broadcasting the CRL. Until the updated CRL is broadcast, mischievous vehicles have time continue their attacks. In the case of IFAL proposals, until the CA is acknowledged and stops issuing the next activation code, the system is in danger. Thus, centralized revocation affects the safety of other vehicles.

In 2019, Bao et al. [13] presented a pseudonym management scheme proposing a distributed framework from blockchain structure. There are privacy managers (PMs) who have a security domain such as one for one and who interact with CA to update CRL. Since revoked pseudonym details are collected with the support of PMs, centralized revocation cost is reduced. However, until the CA obtains information from PMs, misbehaving vehicles have a chance to continue their destructive actions. On the other hand, Asghar et al. [14] presented a voting-based decentralized revocation protocol, where a group of vehicles is capable of revoking a malicious vehicle by voting. Asghar's [14] proposal prevents malicious vehicles from jeopardizing further by restricting their communication ability immediately. Thus, compared to the traditional VANETs, it ensures the safety of other vehicles because vehicles do not need to wait for the CA's action of punishing the misbehaving vehicle. However, we observe that, in such systems, malicious vehicles may not continue voting or a group of vehicles that are acquaintances may revoke a targeted vehicle. This may support hiding crimes. For instance, if a law enforcement party is in the middle of identifying the path of a criminal's vehicle, that vehicle may hide with the support of his coalition vehicles.

Thus, we believe that revocation of suspicious vehicles should not be done permanently without a higher authority investigation. On the other hand, misbehaviors should be halted in minimum time for the sake of other vehicles' security. Moreover, the identification of voting parties puts them in danger. Allies of the revoked vehicle or targeted vehicle itself may harm the voting participants in the future. Answering these challenges, we present a distributed framework for certificate management from the blockchain structure with a ring signature-based voting process for providing secure and efficient certificate revocation.

Contribution

This paper provides a process of punishing a misbehaved vehicle in two processes: global revocation and local revocation. In global revocation, CA can revoke a vehicle with the support of collected information from the network as in Bao's proposal [13]. However, to prevent the further malicious actions of the misbehaving vehicle until the global revocation is done, we suggest a local revocation. In local revocation, a set of nodes in the visible range of a misbehaving vehicle can revoke that vehicle (halt further actions) by voting as discussed by existing works [14,15]. However, since the vehicles on the roads are not trusted parties, we allow vehicles only to halt identified misbehaving vehicles' actions by voting in local revocation. We present this voting process from ring signatures to protect the voters' privacy. Thus, each vehicle has a public key and a secret key, and they can vote against a vehicle anonymously using ring signatures. The local revocation process maintains a list called the local certificate revocation list LCRL. Since we cannot trust vehicles, revocation information in LCRL should be investigated and confirmed by an authority. Thus, we present a global revocation process that decides whether the vehicle should be revoked permanently or released to active. Global revocation maintains the revocation list CRL, a public ledger. On the other hand, instead of a set of vehicle certificates, CRL consists of public keys of dishonest vehicles. In contrast, LCRL is updated with the certificate that the malicious vehicle holds at present. As a result, both CRL and LCRL are short and make the authentication process efficient. While the global revocation process is executed periodically, the local revocation process is executed only if necessary. Moreover, using blockchain structure, we provide a distributed framework for VANETs. Our proposal also consists of PMs who own a security domain and an LCRL. In our proposal, PMs are responsible for updating CA with LCRL consisting of the latest identified misbehaved vehicles' certificates. Moreover, PMs are responsible in case of initializing voting against a suspected vehicle. Once the privacy manager detects a complaint against a vehicle, he initializes a voting process, and when the voting count reaches the threshold value, he updates the LCRL.

Since PMs can be compromised, they are not allowed to access vehicle ids. However, we assume they honestly execute ring signature-based voting to limit malicious vehicle actions via local revocation. On the other hand, as discussed by Bao et al. [13], the ledger keeps all the transactions that can be seen by all PMs and all the PMs play the role of miners.

2. Background and Related Works

VANETs are networks of vehicles connected with each other and other infrastructures to share information to prevent collisions and traffic congestion to provide a secure and comfortable drive. With the rapid development of VANETs, numerous research works were published. Moreover, several organizations like Preserve in Europe, IntelliDrive in the USA, and ITS in Japan have been established. However, still, VANETs suffer from challengers [16], and, among them, security and privacy concerns [16–19] are crucial. Vehicles should authenticate themselves before accessing any service and sharing information, to prevent malicious users from abusing the system. One approach is ensuring the trustworthiness of nodes and messages by employing the blockchain technology [20,21]. Shrestha et al. [20] showed that blockchain can be used to store the trustworthiness of nodes and messages in VANETs. On the other hand, the anonymity of vehicles should be satisfied to ensure their privacy. The privacy preserving and authenticating security requirements can be accomplished by employing digital signatures and signing the broadcasting messages. At the same time, misbehaved vehicles should be punished by revoking them to secure the system. The message receiving vehicles trust only authenticated messages signed by non-revoked vehicles. However, vehicles should not have a long lifespan single certificate to prevent privacy issues. A potential solution is Security Credential Management System (SCMS) [22,23]. In the SCMS process, each vehicle carries a set of pseudonym certificates, which probably lasts longer for a few years. Thus, even though each pseudonym is short-lived, since the batch of certificates carried by each vehicle is sufficient for a few years, vehicles do not require to refill certificates for a long time. On the other hand, since a message signed by an exact vehicle cannot be linked unless the same certificate is reused too often, the privacy of the vehicle is ensured. However, SCMS provides certificate revocation and linkage when misbehavior occurs. When a malicious behavior is observed, CA adds all the pseudonyms of that vehicle to CRL.

One of the problems with the revocation process of traditional VANETs is the increase of CRL. Since one vehicle carries a batch of pseudonyms, CRL size increases when those certificates are added. As a result, it slows down the authentication process. Answering this CRL expansion problem, many works, including the revocation using activation codes [11,12], were published. In the activation code-related proposals, vehicles obtain a batch of short-lived and inactive pseudonym certificates from CA. While the vehicles are in the network, they obtain activation codes periodically. Thus, the vehicles can use fresh certificates for the authentication process. These systems are called 'issue first activate later' (IFAL). Authority will not issue activation codes for malicious vehicles, and thereby those vehicles become revoked and they are unable to communicate in the network in the future. IFAL removes the need for CRL. However, a small CRL can be maintained to protect vehicles from misbehaving entities. Even though IFAL removes the requirement of CRL, the revocation process is still centralized.

In SCMS, the centralized pseudonym certificate issuing authority CA retrains escrow information of each vehicle and pseudonyms to revoke later. Since CA is solely responsible for revoking pseudonyms and punishing misbehaved vehicles, the centralized revocation process is inefficient. Aiming to reduce the communication overhead and support CA to gather information on misbehaving vehicles, Bao et al. [13] suggested a blockchain structure-based pseudonym certificate management scheme. In their proposal, the network is structured based on blockchain, and consists of PKI and privacy managers PMs. Each PM has a logical coverage—a security domain that covers a certain amount of RSUs based on their geographical placement. Thus, malicious behaviors of vehicles are collected through the blockchain look-up. Mapping relationships between vehicles and pseudonyms are stored in PKI and PKI updates the public ledger CRL with all the pseudonyms of a vehicle when that vehicle's misbehavior is confirmed. However, even though Bao et al.'s proposal provides efficient information gathering via blockchain structure, until the PKI updates CRL, the misbehaving vehicle can harm the system.

As a solution to prevent jeopardizing of identified vehicles, Asghar et al. [14] presented a voting-based scheme, where a group of users can revoke a vehicle by voting in their vicinity. They employed the secret-sharing idea of Shamir [24]. Before Asghar's work, some related works were proposed. Papadimitratos et al. [25] distributed CRL as small pieces in the network. Laber et al. [26] also employed V2V communication to distribute CRL in the network. The voting-based revocation proposals allow the users, i.e., vehicles, to eliminate a vehicle by voting. At the registration of vehicles, each vehicles' secret (a key) is shared among n vehicles. Thus, those vehicles can execute a voting process and eliminate a targeted vehicle. The last t-th vehicle participating in the voting process generates the targeted vehicle's key and updates the CRL. As a result, this process effectively prevents further harm from the dishonest vehicle. However, their proposal puts trust in the vehicles, which does not seem practical.

There are numerous research works addressing the computation and communication cost of revocation of pseudonyms [13,14,25,27], and the survey paper submitted by Petit et al. [7] presented the existing pseudonym schemes for VANET, including most of the revocation approaches. However, only a few approaches discussed the security and efficiency issues in centralized revocation [14,28,29]. Among them, even though

Asghar et al. [14] suggested a voting-based system to prevent a user from compromising the system, they were not concerned about the risk of trusting vehicles. We discuss the risk of providing the revocation ability to users other than security and challenges in centralized revocation. We decentralize the revocation process via blockchain structure and ensure the security of the system and users.

Comparison of Our Proposal with Related Works

As the proposal of Bao et al. [13], our proposal also presents a distributed framework for VANETs from a blockchain structure. Thus, the central authority collects malicious vehicles' information through blockchain look-up. As a result, revocation information gathering is efficient. Our proposal prevents further malicious actions of a targeted vehicle allowing local level revocation via the voting process. Thus, compared to the proposal of Bao et al. [13], our proposal provides stronger security for the system. Asghar et al. [14] also presented a local-wise revocation process, which allows vehicles to permanently revoke the targeted vehicle by voting. In our proposal, local level revocation only limits further malicious actions of a targeted vehicle until the CA decides the permanent revocation because vehicles are not trusted parties. Moreover, we secure the privacy of voters using ring signatures. As a result, our proposal efficiently prevents further malicious actions of a targeted vehicle and provides strong security for the system and privacy for the vehicles.

3. Preliminaries

3.1. Notation

We denote by λ the security parameter of the scheme. Let $\mathbb{N} = \{1, 2, 3, \ldots\}$ be the set of *positive integers*. For any $k \geq 1 \in \mathbb{N}$, $[k]$ denotes the set of integers $\{1, \ldots, k\}$ and, if $k \in \mathbb{N}$, then 1^k denotes the string of k ones. An empty string is denoted by ε. If s is a string, then $|s|$ denotes the length of the string and, if $\mathcal{S}$ is a set, then $|\mathcal{S}|$ denotes the size of the set. If $\mathcal{S}$ is a finite set, $b \overset{\$}{\leftarrow} \mathcal{S}$ denotes that b is chosen uniformly at random from $\mathcal{S}$.

3.2. Blockchain Technology

Blockchain technology first appeared in public in 2008 with the implementation of the first cryptocurrency Bitcoin [30]. Blockchain is a distributed ledger system. All the network peers have an identical copy of the ledger. Thus, single copy cannot be modified solely. Blockchain provides user anonymity protecting user privacy. Moreover, blockchain provides decentralized, transparent, immutable, and secure data storage [31]. The basic data unit of a blockchain is a block, which stores information confirmed by the network and the header of the block consists of the hash of the previous block header. Thereby, it connects each other and maintains the immutability of data. The basic structure of the blockchain is as in Figure 3.

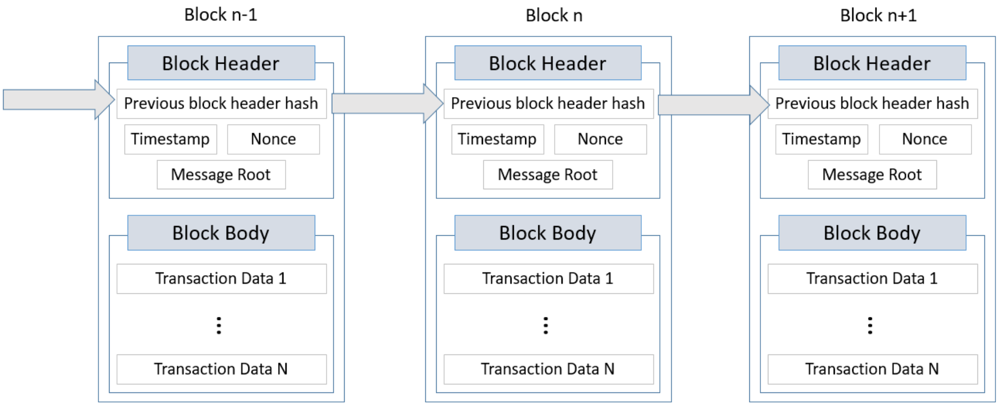

Figure 3. The structure of blocks in blockchain.

3.3. Encryption Scheme

An encryption scheme E = $(\mathsf{KGen}_e, \mathsf{Enc}, \mathsf{Dec})$ consists of three algorithms: key generation KGen_e, encryption Enc, and decryption Dec. The scheme E should satisfy the standard notion of indistinguishability under adaptive chosen-ciphertext attack [32].

For an adversary $\mathcal{A}$, consider an experiment $\mathbf{Exp}_{E,\mathcal{A}}^{\textit{ind-cca-b}}(\lambda)$. First, a public key and the corresponding secret key (encryption and decryption keys) for the scheme E are obtained by executing KGen_e with the security parameter λ and a randomness string r_e (where the length of r_e is bounded by some fixed polynomial $r(\lambda)$) as $(\mathbf{ek}, \mathbf{dk}) \overset{\$}{\leftarrow} \mathsf{KGen}_e(1^\lambda, r_e)$. Let $\mathsf{LR}(m_0, m_1, b)$ a function that returns m_b for a bit b and messages m_0, m_1. We assume the adversary $\mathcal{A}$ never queries $\mathsf{Dec}(\mathbf{dk}, \cdot)$ on a ciphertext previously returned by $\mathsf{Enc}(\mathbf{ek}, \mathsf{LR}(\cdot, \cdot, b))$. We let $\mathbf{Adv}_{E,A}^{\textit{ind-cca}}(\lambda) = |\Pr[\mathbf{Exp}_{E,\mathcal{A}}^{\textit{ind-cca-1}}(\lambda) = 1] - \Pr[\mathbf{Exp}_{E,\mathcal{A}}^{\textit{ind-cca-0}}(\lambda) = 1]|$.

An encryption scheme E is IND-CCA secured if $\mathbf{Adv}_{E,\mathcal{A}}^{\textit{ind-cca}}(\lambda)$ is negligible in λ for any polynomial-time adversary $\mathcal{A}$.

3.4. Digital Signature Schemes

A digital signature scheme DS = $(\mathsf{KGen}_s, \mathsf{Sig}, \mathsf{Vf})$ consists of three algorithms: key generation KGen_s, signing Sig, and verification Vf. The scheme DS should satisfy the standard notion of unforgeability under chosen message attack [32].

For an adversary $\mathcal{A}$, consider an experiment $\mathbf{Exp}_{DS,\mathcal{A}}^{\textit{unforg-cma}}(\lambda)$. First, a public key and the corresponding secret key (verification and signing keys) for the scheme DS is obtained by executing KGen_s with the security parameter λ as $(\mathbf{vk}, \mathbf{sk}) \overset{\$}{\leftarrow} \mathsf{KGen}_s(1^\lambda)$. Then, $\mathbf{vk}$ is given to the adversary, and the adversary can access the signing oracle $\mathsf{Sig}(\mathbf{sk}, \cdot)$ for any number of messages. Finally, the forging adversary $\mathcal{A}$ outputs (m, σ). He wins if σ is a valid signature on the message m and m is not queried so far. We let $\mathbf{Adv}_{DS,\mathcal{A}}^{\textit{unforg-cma}}(\lambda) = \Pr[\mathbf{Exp}_{DS,\mathcal{A}}^{\textit{unforg-cma}}(\lambda) = 1]$.

A digital signature scheme DS is secured against forgeries under chose message attack if $\mathbf{Adv}_{DS,\mathcal{A}}^{\textit{unforg-cma}}(\lambda)$ is negligible in λ for any polynomial-time adversary $\mathcal{A}$.

3.5. Ring Signatures

Ring signature is a digital signature that ensures the signers' privacy satisfying the security notion of user anonymity. Ring signatures were first introduced by Rivest et al. [33]. Each user of the ring signature scheme has a public key ($\mathbf{pk}$) that is publicly known, and a corresponding secret signing key $\mathbf{sk}$. A user s selects a set of public keys of the users in his visibility and make a ring $R = (\mathbf{pk}_1, \ldots, \mathbf{pk}_s, \ldots, \mathbf{pk}_n)$ including his public key $\mathbf{pk}_s$. Then he generates a signature using his secret key $\mathbf{sk}_s$. He presents his signature Σ with the selected ring R. Thus, the verifier knows that the signer is one of the users from R.

Definition 1. *A ring signature scheme is a tuple of two polynomial-time (PPT) algorithms: Sign and Verify. Later, the KeyGen algorithm is introduced to ring signatures to ensure that all the users have identical keys [34].*

- *KeyGen$_r$(1^λ): This algorithm takes as input security parameter λ and outputs a public and secret key pair ($\boldsymbol{pk}, \boldsymbol{sk}$).*
- *Sign$_r$($R, \boldsymbol{sk}_s, M$): This randomized algorithm takes as input a set of public keys $R = (\boldsymbol{pk}_1, \ldots, \boldsymbol{pk}_n)$, a secret signing key $\boldsymbol{sk}_s$, and a message M, where $\boldsymbol{pk}_s \in R$.*
- *Verify$_r$(R, Σ, M): This deterministic algorithm takes as input the ring $R = (\boldsymbol{pk}_1, \ldots, \boldsymbol{pk}_n)$ and a purported signature Σ on M, and outputs either 1 (valid) or 0 (invalid).*

Ring signatures satisfy two security requirements, anonymity and unforgeability.

4. High Level Idea of the Proposal

This section provides the high level idea of the proposal with the discussion of employing each technology.

4.1. Blockchain Based Structure

Our proposal is based on the blockchain structure. Therefore, the proposed system maintains a shared ledger like a typical blockchain. Thus, all the transactions are visible to all PMs. However, only the Central Authority CA can update the CRL. On the other hand, each PM maintains a local CRL called the Local Certificate Revocation List (LCRL) for his security domain, which is synchronized with the CRL. The basic structure of the blockchain-based VANET system is shown in Figure 4.

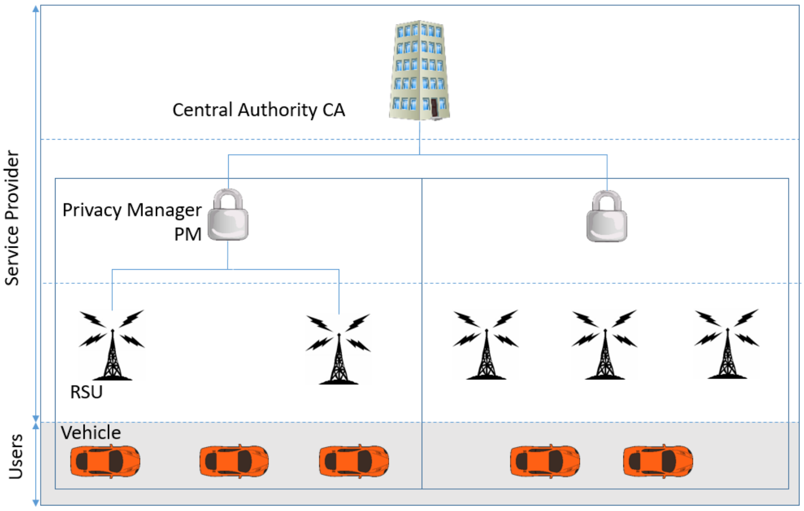

Figure 4. The blockchain structure based VANET.

As depicted in Figure 4, based on the hierarchy of responsibilities, the network consists of four layers. In the top layer, centralized authority CA is involved in the initial registration of the vehicles and revocation of vehicles. Thus, CA issues a set of short-lived pseudonym certificates for a vehicle sufficient for a few years. When a vehicle is registered with CA, CA provides a batch of pseudonym certificates and saves vehicle id *vid* and details of the issued pseudonym certificates in a mapping table. Each certificate has its own expiring time. Thus, safety messages transmitted by vehicles include a pseudonym certificate, a timestamp, and the vehicle's current status. On the other hand, CA is responsible for updating CRL with the revoked vehicles' public keys. Note that, instead of adding the set of pseudonym certificates to the CRL, CA adds the revoking vehicle's vehicle-related key (vehicle-token). Thus, the CRL size is considerably short. Each PM is responsible for its logical coverage area. A PM covers a certain number of RSUs based on the geographical distribution of RSUs. PMs interact and support CA to manage the network, specifically by maintaining a local CRL (LCRL) relating to the revocation processes in his area. It is required to install PMs in suitable geographical places.

All the PMs obtain a common decryption key from CA, which can be used to decrypt the content of the pseudonym certificate of a vehicle. Thus, when a misbehaving vehicle is found, close PMs can decrypt the currently active pseudonym certificate of the vehicle and add the decrypted detail (certificate-token) to LCRL. This ensures that only the PMs can update LCRL. We assume that PMs periodically update CA with LCRL. As a result, based on the LCRLs, revocation details of vehicles supplied by each PM, CA investigates and updates the CRL with the vehicle-tokens of confirmed misbehaving vehicles. Once the CRL is updated, each PMs' LCRL are emptied releasing certificates of vehicles that are not judged as misbehaved.

In traditional VANET systems, CA investigates and updates CRL with the batch of pseudonym certificates of the misbehaving vehicle. In the proposing blockchain-based system, PMs and other users support revocation. Thus, the revocation process in our proposal is decentralized. In the below section, we discuss the process of local revocation executed by PMs.

4.2. Local Revocation—A Voting Based Revocation

We modify the above blockchain structure-based system to support voting-based local revocation. The PMs manage voting-based revocation. Since PMs do not have the privilege to write on CRL, they cannot update CRL with the identified misbehaving vehicle information. However, until the CA updates CRL after investigating about misbehaving vehicles, other vehicles in the network are in danger. To prevent further damage from the dishonest vehicle until CA punishes him, we propose a voting-based revocation as in the Asghar et al. [14] proposal, but within the local area. However, since the vehicles are not trusted entities, we restrict them from initializing the voting against a vehicle. In our proposal, when misbehavior is detected and informed by a vehicle or an RSU, PM initializes the voting procedure. Thus, any user (vehicles and RSUs) can vote against the targeted vehicle. The PM is responsible for tallying the votes and updating LCRL once the threshold value is reached.

Since the partially trusted PM is responsible for the voting procedure and limiting the further misbehaving of vehicles by revoking the pseudonym certificate, a colluded set of malicious vehicles cannot revoke a vehicle. Since a PM, with the support of vehicles and RSUs, can prevent malicious vehicles from further jeopardizing the system, the proposed system secures the other vehicles. On the other hand, since the local revocation procedure cannot permanently revoke a vehicle, innocent vehicles become active in the system after CA's decision.

However, unless the voting participant anonymity is ensured, vehicles willingly participate in the voting procedure is small. As in other e-voting systems, we should provide user anonymity to secure voters' privacy.

4.3. Preserving the Privacy of Voting Participants

Since voting is publicly available, the targeted vehicle may track the voting parties and attack later. To prevent such kinds of attacks, we can ensure voters' privacy by employing ring signatures. Ring signatures allow a user to be anonymous by employing an ad-hoc group. A user generates a ring signature with a group of valid public keys, including his public key. Ring signatures provide extended anonymity for voting systems [35]. For instance, even though group signatures [36] which share some features of ring signatures also provide user anonymity, an authority can cancel the user anonymity and identify the user. This confirms that ring signature is the better solution for e-voting. Thus, we employ ring signatures for our proposal.

To ensure the voting participants are only from the same security domain, we generate public and secret keys for each vehicle in the privacy domain which can be used for voting. Since the keys are generated once for each vehicle in the privacy domain, PM does not face any bandwidth difficulties. Since the block-related public keys of the vehicles are publicly available, a voting participant can generate a ring signature to be anonymous by using a set of public keys when voting. On the other hand, since the modern ring signatures provide linkability [35,37], no vehicle can double submit a vote.

4.4. Proposed Scheme

According to the discussions given in the above subsection, each vehicle with *vid* obtains a set of short-lived pseudonym certificates from CA at the initial registration. The initial registration is the only process in which a vehicle interacts with CA. Other than vehicles' initial registration, CA is responsible for revoking misbehaving vehicles. Thus, CA updates the CRL by adding misbehaving vehicles' vehicle-token. Only CA can write on CRL. Only privacy managers and other participants can read the CRL. Our proposal is a distributed network. Each privacy domain has a privacy manager PM. The PM initializes voting procedure against a dishonest vehicle in his domain when the PM receives a complaint directly from a vehicle or an RSU. PM issues public and secret keys for the vehicles entering his domain to ensure the anonymous voting procedure. Thus, users can proceed with anonymous voting using ring signatures.

We depict our proposal, blockchain structure-based VANET in Figure 5 and explain each step below.

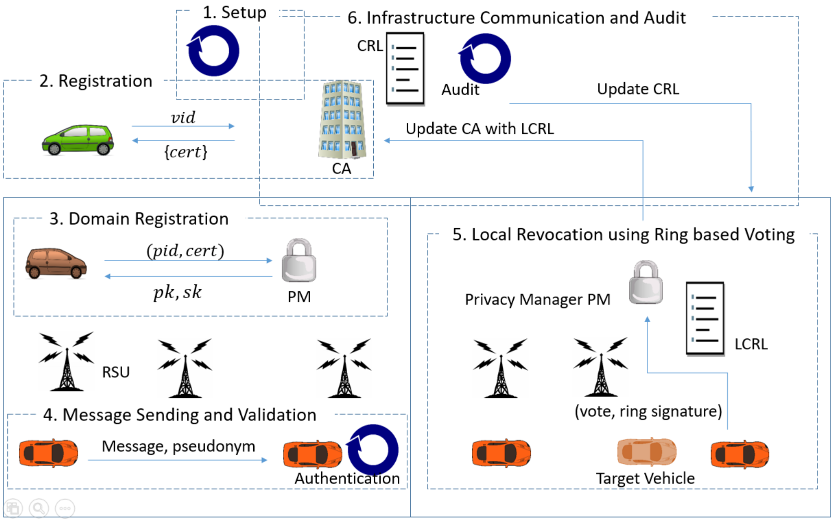

Figure 5. Overview of the Proposed Scheme.

1. Setup: Network consists of PMs who has one security domain. Each PM oversees a certain amount of RSUs based on the geographical establishment of RSUs. CA generates an encryption–decryption key pair ($\mathbf{ek}_{PM}, \mathbf{dk}_{PM}$) and gives the decryption key ($\mathbf{dk}_{PM}$) to the established PMs. Moreover, CA initializes and broadcasts CRL and LCRLs.
2. Registration: A new vehicle who wants to join the network has its vehicle id vid interact with CA, and CA issues a set of short-lived pseudonym certificates ($\{cert\}$) to the vehicle. CA maintains a mapping table of vid and pseudonyms $\{cert\}$.
3. Domain-Registration: When a vehicle i enters to an area, the relevant PM obtains pseudonym certificate ID (pid) of the vehicle, which is currently in the active status and issues a public and secret key pair ($\mathbf{pk}_i, \mathbf{sk}_i$) to the vehicle.
4. Message Sending and Validation: A vehicle transmits a message M by signing the message using the secret signing key of a valid pseudonym and appending the pseudonym certificate $cert$. The message receiving party (another vehicle or RSU) authenticates the sender and accepts the message if authentication is passed. The receiver verifies the sender's certificate first against the LCRL and then against the CRL.
5. Local Revocation using Ring based Voting: When a PM observes or receives a complaint against misbehavior of a vehicle, it initiates voting against that vehicle. Thus, any vehicle that agrees with the voting procedure can send his vote which is signed anonymously using ring signatures. A user i creates a ring R with other users' public keys and his public key $\mathbf{pk}_i$, and generates a ring signature Σ using the relevant secret key $\mathbf{sk}_i$. Once the vote count reaches the decided threshold value t, PM obtains the targeted vehicle's certificate-token and adds the token to the local revocation list $LCRL$.
6. Infrastructure Communication and Audit: Periodically, PMs sends LCRLs to CA with other information. Then, CA investigates, permanently revokes mischievous vehicles, and updates CRL with the vehicle-token. Once the CRL is updated, PMs obtain the copy of CRL, and their LCRL becomes empty because actual misbehavior is punished and added to CRL by CA. Thus, PMs should release the innocent vehicles whose certificates are in LCRL.

5. Construction of the Proposed Scheme

In this section, we give the construction of the proposing scheme. The construction of the scheme is given in Algorithm 1. We construct the scheme from a digital signature scheme DS = $(\mathsf{K}_s, \mathsf{Sig}, \mathsf{Vf})$ and a PKE scheme E = $(\mathsf{KGen}_e, \mathsf{Enc}, \mathsf{Dec})$. Let n be the number of security domain of the network at present, and m is the size of the pseudonym set.

Algorithm 1: Algorithms of the scheme

```
$\mathsf{Setup}(1^\lambda) \rightarrow (\mathbf{pk}_{sys}, \mathbf{sk}_{CA}, \mathbf{ek}_{BM}, \mathbf{dk}_{BM}, CRL, \{LCRL\}_n)$
$(\mathbf{vk}, \mathbf{sk}) \leftarrow \mathsf{KGen}_s(1^\lambda)$; $(\mathbf{ek}, \mathbf{dk}) \leftarrow \mathsf{KGen}_e(1^\lambda)$; $CRL = 0$; $\{LCRL\}_n = 0$;
Return $\mathbf{pk}_{sys} = (\lambda\mathbf{vk}), \mathbf{sk}_{CA} = \mathbf{sk}, \mathbf{ek}_{BM} = \mathbf{ek}, \mathbf{dk}_{BM} = \mathbf{dk}, CRL, \{LCRL\}_n$.
$\mathsf{Registration}(\mathbf{pk}_{sys}, vid, \mathbf{sk}_{CA}) \rightarrow (\{pid,cert\}_m, mapTab)$
Parse $\mathbf{pk}_{sys}$ as $(\lambda, \mathbf{vk}), \mathbf{vk})$; $r_{vid} \leftarrow \{0,1\}^{r(\lambda)}$; $(\mathbf{ek}_v, \mathbf{dk}_v) \leftarrow \mathsf{KGen}_e(1^\lambda; r_{vid})$;
For $1 \leq j \leq m$:
Select $pid^j$ and $r_c^j \leftarrow \{0,1\}^{r(\lambda)}$; Select a active time period $T_c^j$;
  $(\mathbf{ek}_c^j, \mathbf{dk}_c^j) \leftarrow \mathsf{KGen}_e(1^\lambda; r_{pid})$;   $(\mathbf{vk}_c^j, \mathbf{sk}_c^j) \leftarrow \mathsf{KGen}_s(1^\lambda)$;
$cert - token_c^j \leftarrow \mathsf{Enc}_{\mathbf{ek}_c^j}(pid^j; r_c^j)$; $cert - token_b^j \leftarrow \mathsf{Enc}_{\mathbf{ek}_{BM}^j}(\mathbf{dk}_c^j; r_c^j))$;
$cert - token^j \leftarrow (cert - token_c^j, cert - token_b^j)$;
$vehi - token^j \leftarrow \mathsf{Enc}_{\mathbf{ek}_v^j}(pid^j; r_c^j)$;
$\Sigma_{cert}^j = \mathsf{Sig}_{\mathbf{sk}_{CA}}(pid^j, \mathbf{vk}_c^j, T_c^j, cert - token^j, vehi - token^j)$;
$cert - message^j = pid^j, \mathbf{vk}_c^j, T_c^j, cert - token^j, vehi - token^j$;
$cert^j = (\Sigma_{cert}^j, cert - message^j)$;
  $mapTab = mapTab \cup (vid^j, \mathbf{ek}_v^j, \mathbf{dk}_v^j, pid^j, cert^j, \mathbf{ek}_c^j, \mathbf{dk}_c^j, \mathbf{vk}_c^j, \mathbf{sk}_c^j)$;
Return $(\{pid, cert, \mathbf{sk}_c\}_m, mapTab)$;
$\mathsf{Block\text{-}Registration}(\mathbf{pk}_{sys}, \mathbf{dk}_{BM}, (pid, cert), current - time) \rightarrow (\mathbf{pk}, \mathbf{sk})$
Parse $\mathbf{pk}_{sys}$ as $(\lambda, \mathbf{vk})$;
Parse $cert$ as $(\Sigma_{cert}, cert - message)$;
If $\mathsf{Verifyf}_{\mathbf{vk}}(\Sigma_{cert}, cert - message)$ = 0 then return 0;
Parse $cert - message$ as $pid, \mathbf{vk}_c, T_c, cert - token, vehi - token$
If $T_c$ is note valid against current-time then return 0;
$(\mathbf{pk}_r, \mathbf{sk}_r) \leftarrow \mathsf{KeyGen}_r(1^\lambda)$;
Return $(\mathbf{pk}_r, \mathbf{sk}_r)$
$\mathsf{Message\ Sending\ and\ Validation}(\mathbf{pk}_{sys}, M, \mathbf{sk}_c, (pid, cert), LCRL, CRL) \rightarrow status$
Parse $\mathbf{pk}_{sys}$ as $(\lambda, \mathbf{vk})$;
Sender: Return $(\mathsf{Sig}_{\mathbf{sk}_c}(M) = \sigma, (pid, cert))$
Receiver:
$status = accept$;
Parse $cert$ as $(\Sigma_{cert}, cert - message)$;
Parse $cert - message$ as $pid, \mathbf{vk}_c, T_c, cert - token, vehi - token$
If $T_c$ is note valid against current-time then $status = reject$;
If $\mathsf{Vf}_{\mathbf{vk}_c}(\sigma, M) = 0$, then $status = reject$;
If $\mathsf{Vf}_{\mathbf{vk}}(\Sigma_{cert}, cert - message) = 0$ then $status = reject$;
If $LCRL \neq 0$ then For $\mathbf{dk}_c' \in LCRL$: If $pid = \mathsf{Dec}_{\mathbf{dk}_c'}(cert - token)$ then $status = reject$;
If $CRL \neq 0$ then For $\mathbf{dk}_v' \in CRL$: If $pid = \mathsf{Dec}_{\mathbf{dk}_v'}(vehi - token)$ then $status = reject$;
Return $status$
$\mathsf{Local\ Revocation\ using\ Ring\ based\ Voting}(\mathbf{pk}_{sys}, \mathbf{dk}_{BM}, (pid, cert), \{\mathbf{pk}\}_n, LCRL) \rightarrow LCRL$
User $i$: $R = (\mathbf{pk}_1, \ldots, \mathbf{pk}_i, \ldots, \mathbf{pk}_n)$; $\mathsf{Sign}_r(R, \mathbf{sk}_s, < pid, vote >)$;
Block-Manager:
If vote count satisfies the threshold value then do the followings.
Parse $cert$ as $(\Sigma_{cert}, cert - message)$;
Parse $cert - message$ as $pid, \mathbf{vk}_c, T_c, cert - token, vehi - token$
Parse $cert - token$ as $cert - token_c, cert - token_b$;
$\mathbf{dk}_c \leftarrow \mathsf{Enc}_{\mathbf{dk}_{BM}}(cert - token_b)$;
Return $LCRL = LCLR \cup \mathbf{dk}_c$
$\mathsf{Infrastructure\ Communication\ and\ Audit}(\mathbf{sk}_{CA}, LCRL, mapTab) \rightarrow CRL$
For $1 \leq j \leq LCRL$: Parse $LCRL[j]$ as $\mathbf{dk}_c^j$;
If $pid \in mapTab[\mathbf{dk}_c^j]$ is dishonest then, $CRL = CRL \cup (\mathbf{dk}_v \leftarrow mapTab[\mathbf{dk}_c^j])$
Return CRL
```

6. Security Discussion

In this section, we discuss the security challenges in certificate issuing and revocation processes.

The underlying encryption scheme (E) satisfies the key privacy, and the underlying digital signature scheme (DS) satisfies the unforgeability.

6.1. Security of Certificate Issuing Process

Certificate issuing is done by the certificate authority CA (central authority). The certificate issuing process is the only time a vehicle interacts with CA. When a vehicle leaves the manufacturing process, it obtains a unique vid, and the vehicle interacts CA with vid. Since the algorithm Registration takes as inputs the CA's secret signing key, only the trusted CA can execute Registration. Thus, only CA knows the vehicle ids. Moreover, since the CA signs each certificate, no outsider can generate a valid certificate. Based on the assumption that CA is a trusted party, the certificate issuing process is secured.

6.2. Security of the Revocation Process

There are two revocation processes in our proposal. The global revocation is done by the trusted party CA. He collects information from each privacy manager. On the other hand, CA conducts an audit process periodically collecting the local revocations from privacy managers and executing an investigation process before updating CRL. Since the CA can access $mapTable$, he can efficiently check vehicles' behavior and update CRL with the vehicle id vid. Thus, global revocation is trustworthy. Privacy managers execute the local revocation. Since the privacy manager has limited authority, he can only know the current pseudonym certificate id of a dishonest vehicle. Thereby, CA controls the authority of the privacy manager. Since other parties are not considered trusted, CA allows privacy managers to revoke vehicles temporally in their domains. Privacy managers are responsible for executing voting against a vehicle and counting votes. We believe privacy managers will not cheat on the voting process. On the other hand, privacy managers update CA with LCRL and evidence of vehicles' misbehaviors. Thus, CA can process auditing efficiently.

The above discussion shows that the revocation process in our proposal is secured.

7. Conclusions

In this paper, we proposed a blockchain structure-based VANET with a certificate management scheme. Our proposal manages dishonest vehicles at the local and global levels. Local revocation ensures that the misbehaving vehicle's action is paused until that vehicle is judged via global revocation. Since the revocation lists are short, the authentication process is efficient. On the other hand, since we conduct a ring signature-based voting process for the local revocation, based on the majority decision, the revocation is done, and voting parties' privacy is secured. Moreover, since only CA knows vehicles' ids, the vehicles' privacy is preserved. Our proposal provides efficiency and security via blockchain structure, encryption schemes, digital signatures, and ring signatures.

Author Contributions: Project administration, H.Y.; Supervision, C.-M.C. and K.S.; Writing-original draft, M.N.S.P.; Writing-review and editing, T.N. and M.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Zhang, D.; Zhang, T.; Liu, X. Novel self-adaptive routing service algorithm for application in VANET. *Appl. Intell.* **2019**, *49*, 1866–1879. [CrossRef]
2. World Health Organization. *Death on the Roads. Based on the WHO Global Status Report on Road Safety 2018*; World Health Organization: Geneva, Switzerland, 2018. Available online: https://extranet.who.int/roadsafety/death-on-the-roads/#deaths (accessed on 10 January 2022).
3. World Health Organization. *Global Status Report on Road Safety 2018*; World Health Organization: Geneva, Switzerland, 2018. Available online: http://apps.who.int/iris/bitstream/handle/10665/277370/WHO-NMH-NVI-18.20-eng.pdf?ua=1 (accessed on 18 August 2021).
4. Fiore, M.; Casetti, C.; Chiasserini, C.F. Information sharing in VANETs. In *Advances in Vehicular Ad-Hoc Networks: Developments and Challenges*; IGI Global: Hershey, PA, USA, 2010; pp. 75–96.
5. Abassi, R. VANET security and forensics: Challenges and opportunities. *Wiley Interdiscip. Rev. Forensic Sci.* **2019**, *1*, e1324. [CrossRef]
6. Kargl, F.; Papadimitratos, P.; Buttyan, L.; Müter, M.; Schoch, E.; Wiedersheim, B.; Thong, T.V.; Calandriello, G.; Held, A.; Kung, A.; et al. Secure vehicular communication systems: implementation, performance, and research challenges. *IEEE Commun. Mag.* **2008**, *46*, 110–118. [CrossRef]
7. Petit, J.; Schaub, F.; Feiri, M.; Kargl, F. Pseudonym schemes in vehicular networks: A survey. *IEEE Commun. Surv. Tutor.* **2014**, *17*, 228–255. [CrossRef]
8. Saini, I.; Saad, S.; Jaekel, A. Evaluating the effectiveness of pseudonym changing strategies for location privacy in vehicular ad-hoc network. *Secur. Priv.* **2019**, e68, [CrossRef]
9. Sheikh, M.S.; Liang, J.; Wang, W. Security and privacy in vehicular ad hoc network and vehicle cloud computing: A survey. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 5129620. [CrossRef]
10. Hubaux, J.P.; Capkun, S.; Luo, J. The security and privacy of smart vehicles. *IEEE Secur. Priv.* **2004**, *2*, 49–55. [CrossRef]
11. Verheul, E.; Hicks, C.; Garcia, F.D. Ifal: Issue first activate later certificates for v2x. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, 17–19 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 279–293.
12. Simplicio, M.A., Jr.; Cominetti, E.L.; Patil, H.K.; Ricardini, J.E.; Silva, M.V.M. ACPC: Efficient revocation of pseudonym certificates using activation codes. *Ad Hoc Netw.* **2019**, *90*, 101708. [CrossRef]
13. Bao, S.; Lei, A.; Cruickshank, H.; Sun, Z.; Asuquo, P.; Hathal, W. A pseudonym certificate management scheme based on blockchain for internet of vehicles. In Proceedings of the 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Fukuoka, Japan, 5–8 August 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 28–35.
14. Asghar, M.; Pan, L.; Doss, R. An efficient voting based decentralized revocation protocol for vehicular ad hoc networks. *Digit. Commun. Netw.* **2020**, *6*, 422–432. [CrossRef]
15. Arboit, G.; Crépeau, C.; Davis, C.R.; Maheswaran, M. A localized certificate revocation scheme for mobile ad hoc networks. *Ad Hoc Netw.* **2008**, *6*, 17–31. [CrossRef]
16. Khan, T.; Ahmad, N.; Cao, Y.; Jalal, S.A.; Asif, M.; Cruichshank, H. Certificate revocation in vehicular ad hoc networks techniques and protocols: A survey. *Sci. China Inf. Sci.* **2017**, *60*, 100301. [CrossRef]
17. Parno, B.; Perrig, A. Challenges in securing vehicular networks. In Proceedings of the Workshop on hot topics in networks (HotNets-IV), College Park, MD, USA, 14–15 November 2005; pp. 1–6.
18. Förster, D.; Kargl, F.; Löhr, H. PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET). In Proceedings of the 2014 IEEE Vehicular Networking Conference (VNC), Paderborn, Germany, 3–5 December 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 25–32.
19. Schaub, F.; Ma, Z.; Kargl, F. Privacy requirements in vehicular communication systems. In Proceedings of the 2009 International Conference on Computational Science and Engineering, Vancouver, BC, Canada, 29–31 August 2009; IEEE: Piscataway, NJ, USA, 2009; Volume 3, pp. 139–145.
20. Shrestha, R.; Bajracharya, R.; Shrestha, A.P.; Nam, S.Y. A new type of blockchain for secure message exchange in VANET. *Digit. Commun. Netw.* **2020**, *6*, 177–186. [CrossRef]
21. Ravi, N.; Verma, S.; Kavita; Zaman, N.Z.; Talib, M.N. Securing VANET Using Blockchain Technology. *J. Phys. Conf. Ser.* **2021**, *1979*, 012035. [CrossRef]
22. Whyte, W.; Weimerskirch, A.; Kumar, V.; Hehn, T. A security credential management system for V2V communications. In Proceedings of the 2013 IEEE Vehicular Networking Conference, Boston, MA, USA, 16–18 December 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 1–8.
23. Kolleda, J.; Frank, L.; Andrews, S.; Poling, T.; Fitzpatrick, D.; Marousek, J.; Hamilton, B.A. National Security Credential Management System (SCMS) Deployment Support: Scms Baseline Summary Report. 2018. Available online: https://rosap.ntl.bts.gov/view/dot/36397 (accessed on 20 December 2021).
24. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]

25. Papadimitratos, P.; Mezzour, G.; Hubaux, J.P. Certificate revocation list distribution in vehicular communication systems. In Proceedings of the Fifth ACM International Workshop on VehiculAr Inter-NETworking, New York, NY, USA, 15 September 2008; pp. 86–87.
26. Laberteaux, K.P.; Haas, J.J.; Hu, Y.C. Security certificate revocation list distribution for VANET. In Proceedings of the Fifth ACM International Workshop on VehiculAr Inter-NETworking, San Francisco, CA, USA, 15 September 2008; pp. 88–89.
27. Wasef, A.; Shen, X. EMAP: Expedite message authentication protocol for vehicular ad hoc networks. *IEEE Trans. Mob. Comput.* **2011**, *12*, 78–89. [CrossRef]
28. Raya, M.; Papadimitratos, P.; Aad, I.; Jungels, D.; Hubaux, J.P. Eviction of misbehaving and faulty nodes in vehicular networks. *IEEE J. Sel. Areas Commun.* **2007**, *25*, 1557–1568. [CrossRef]
29. Wasef, A.; Shen, X. EDR: Efficient decentralized revocation protocol for vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* **2009**, *58*, 5214–5224. [CrossRef]
30. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* **2008**, 21260. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 5 January 2022).
31. Wang, C.; Cheng, X.; Li, J.; He, Y.; Xiao, K. A survey: applications of blockchain in the Internet of Vehicles. *Eurasip J. Wirel. Commun. Netw.* **2021**, *2021*, 77. [CrossRef]
32. Bellare, M.; Shi, H.; Zhang, C. Foundations of group signatures: The case of dynamic groups. In *Cryptographers' Track at the RSA Conference, Proceedings of the The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, 14–18 February 2005*; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3376, pp. 136–153.
33. Rivest, R.L.; Shamir, A.; Tauman, Y. How to leak a secret. In Proceedings of the ASIACRYPT, Gold Coast, Australia, 9–13 December 2001; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2248, pp. 552–565.
34. Bender, A.; Katz, J.; Morselli, R. Ring signatures: Stronger definitions, and constructions without random oracles. In *Theory of Cryptography Conference, Proceedings of the 3rd Theory of Cryptography Conference, TCC 2006, New York, NY, USA, 4–7 March 2006*; Springer: Berlin/Heidelberg, Germany, 2006; Volume 3876, pp. 60–79.
35. Liu, J.K.; Wei, V.K.; Wong, D.S. Linkable spontaneous anonymous group signature for ad hoc groups. In *Australasian Conference on Information Security and Privacy, Proceedings of the 9th Australasian Conference, ACISP 2004, Sydney, Australia, 13–15 July 2004*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 325–335.
36. Chaum, D.; Van Heyst, E. Group signatures. In Proceedings of the EUROCRYPT 1991, LNCS, Brighton, UK, 8–11 April 1991; Springer: Berlin/Heidelberg, Germany, 1991; Volume 547, pp. 257–265.
37. Fujisaki, E.; Suzuki, K. Traceable ring signature. In *International Workshop on Public Key Cryptography, Proceedings of the 10th International Conference on Practice and Theory in Public-Key Cryptography, Beijing, China, 16–20 April 2007*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 181–200.