*Article*

# Improved Chaff-based CMIX for Solving Location Privacy Issues in VANETs

**Mishri Saleh Al-Marshoud [1], Ali H. Al-Bayatti [1] and Mehmet Sabir Kiraz [1]**

[1] De Montfort University, Cyber Technology Institute, The Gateway, Leicester, LE1 9BH, UK

**Abstract:** Safety application systems in Vehicular Ad-hoc Networks (VANETs) require the dissemination of contextual information about the scale of neighbouring vehicles; therefore, ensuring security and privacy is of utmost importance. Vulnerabilities in the messages and the system's infrastructure introduce the potential for attacks that lessen safety and weaken passengers' privacy. The purpose of short-lived anonymous identities, called "pseudo-identities", is to divide the trip into unlinkable short passages. Researchers have proposed changing pseudo-identities more frequently inside a pre-defined area, called a cryptographic mix-zone (CMIX) to ensure enhanced protection. According to ETSI ITS technical report recommendations, the researchers must consider the low-density scenarios to achieve unlinkability in CMIX. Recently, Christian *et al.* proposed a Chaff-based CMIX scheme that sends fake messages under the consideration of low-density conditions to enhance vehicles' privacy and confuse attackers. To accomplish full unlinkability, in this paper, we first show the following security and privacy vulnerabilities in the Christian *et al.* scheme: Linkability attacks outside the CMIX may occur due to deterministic data sharing during the authentication phase (e.g., duplicate certificates for each communication). Adversaries may inject fake certificates, which breaks Cuckoo Filters' (CFs) updates authenticity, and the injection may be deniable. CMIX symmetric key leakage outside the coverage. We propose a VPKI based protocol to mitigate these issues. First, we use a modified version of Wang et al.'s scheme to provide mutual authentication without revealing the real identity. To this end, the messages of a vehicle are signed with a different pseudo-identity "certificate". Further, the density is increased via the sending of fake messages in low traffic periods to provide unlinkability outside the mix-zone. Second, unlike Christian *et al.* 's scheme, we use the Adaptive Cuckoo Filter (ACF) instead of CF to overcome the false positives' effect on the whole filter. Also, to prevent any alteration of the ACFs, only *RSU*s distribute the updates, and they sign the new fingerprints. Third, the mutual authentication prevents any leakage from the mix zones' symmetric keys by generating a fresh one for each communication through a Diffie-Hellman key exchange.

**Keywords:** authentication; privacy; security; non-repudiation; pseudonym; unlinkability; vehicular ad-hoc networks

**Citation:** Al-Marshoud, M.; Al-Bayatti, A.; Kiraz, M. Improved Chaff-based CMIX for Solving Location Privacy Issues in VANETs. *Electronics* **2021**, *1*, 0. https://doi.org/

Received:
Accepted:
Published:



## 1. Introduction

Intelligent transportation systems (ITS), particularly Vehicular Ad Hoc Networks (VANETs), are constantly growing in importance. Efficiency and security are achieved in VANETs mainly through safety applications and non-safety applications such as entertainment and internet access. In safety applications, beaconing services are necessary because they are essential for ITS effectiveness; otherwise, accidents can occur. Open networks that are accessible by any node are characteristic of VANETs. In general, the two types of communication performed by VANETs are Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I), which communicate through the latest Radio Access Technology (RAT) IEEE 802.11bd for Dedicated Short Range Communications (DSRC) and New Radio NR-V2X for Cellular-V2X (C-V2X). They reduce the packet collisions [1] and they can work in tunnels and confined areas [2]. The On-Board Units (OBUs) of vehicles must transmit Cooperative Awareness Messages (CAMs) as safety messages due to their high mobility, providing real-time information on velocity, location, and heading [3]. In compliance with international standards (i.e., IEEE 1609.2 WG [4] and the European Telecommunications Standards Institute (ETSI) ITS [5]), to ensure the integrity, non-repudiation and authenticity of messages, vehicles and Roadside Units (*RSU*s) are formed with public and private key pairs, in addition to digital signatures. Besides, established safety requirements based on Vehicle Public Key Infrastructure (VPKI) require multiple Certificate Authorities (CAs) to administer certificates for the underlying bodies [6,7]. These CAs permit long-term certificates for vehicles and *RSU*s after registration. Later, they grant certificates based on pseudo-identities and "anonymous credentials" to deter some types of road attacks. However, the standard ETSI [8] body also suggests changing pseudo-identities in combination with modifying all communication stack layer identifiers, such as the Network Access Control (MAC) and the Internet Protocol (IP) addresses [9]. Nevertheless, a passive attacker who gathers information from these CAMs can comfortably perform location tracking by *syntactic linking attack*, referring to the old and new vehicle pseudo-identities. Additionally, adversaries can link pseudo-identities by analysing signed messages' contents, and the adversary can accurately determine the next location of the car. This is defined as a *Semantic linking attack* [10]. We should note that the semantic link attack is more powerful than the syntactic link attack because the adversary produces an attack based on the details included in the security messages used to link the pseudo-identities, which produces better results [11]. Various research works have focused on managing the pseudo-identity change to solve these linking attacks over the last few years. For example, some techniques recommend that vehicles set up a silent period, i.e. their transmitters stay off (do not send messages) for a specific duration after changing their pseudo-identities, although they can still accept and process incoming messages [8]. Nonetheless, while this tends to make tracking very difficult, safety applications may be impaired because vehicles cannot send safety messages during this time. As a consequence, the probability of collision rises for such techniques. An alternative is the idea of a mix-zone, which is predefined as a geographic region (bound to the *RSU* coverage) in which vehicles exchange messages, except for position-related messages since they are in the same place, and they change pseudo-identities within that region. Researchers have suggested improving the privacy strategy for pseudo-identity transition techniques in Cooperative-ITS (C-ITS) [12]. [13] suggested encrypting the exchanged messages inside the mix-zone and called it the CMIX strategy. This relies on a symmetric key to share safety messages within the mix-zone, which ensures that all vehicles can use the same key to avoid linkability within the mix-zone, whereby the *RSU* provides the symmetric key to all vehicles within the mix-zone [8]. Christian *et al.* later considered the density and suggested a CMIX based on Chaff , believing that it would provide location privacy and irresistible security [14]. However, the filter used in Christians *et al.* 's scheme to differentiate between real and fake messages is weak, and an internal adversary may expose the hash table to malicious injections. Additionally, the filter performance disrupts the Chaff messages' concept, which may break the system and make it vulnerable to linking attacks. We believe that the authentication of the transmitted messages and senders' identities must be improved significantly for safety applications to address these problems. Therefore, in our scheme, entities might prove the possession of some secret information preloaded in the OBU of the vehicle.

### *1.1. Our Contributions*

In this paper, we first revisit the Christian *et al.* 's CMIX-based scheme [14] and then point out the following security and privacy issues: 1) Linkability attacks during the communication outside the mix-zone, 2) unreliable Cuckoo Filters' (CFs) updates (in the low-density of the traffic), which breaks the privacy and safety of the whole system, and 3) mix-zones' encryption key leakage, which allows any compromised vehicle to break the safety of the system. We then propose an improved version that is resistant to these issues. To comply with Christian *et al.* 's scheme, we utilise a modified version of [15] by replacing digital certificates with an Identity Based Signature. In summary, our scheme provides the following features:

- We use Adaptive Cuckoo Filter(ACF) instead of CF, as in [14], to mitigate the effect of false positives that may impact the performance of the filter; this enhances the system in sending Chaff messages to confuse eavesdropping adversaries that exploit traffic flow to breach unlinkability. We also use the pseudo-identity generation concept from [15], which has non-malleability to hide the certificates of actual vehicles.
- We provide unforgeability and non-repudiation by adding an $RSU$ signature and timestamp in each message, in particular, on the new fingerprinted Chaff messages before inserting them into the ACF. Hence, to preclude any possibility of malicious injections, we also remove the ACFs forwarding task from vehicles, like [14]; in our scheme, $RSU$s are the sole authority to distribute them.
- We modify the mutual authentication between $RSU$s and vehicles based on certificates instead of IDs, as in [15], before generating the symmetric key of a mix-zone, as the generation of a shared key follows the Diffie-Hellman key exchange method to provide confidentiality and privacy by preventing any key leakage.

These features allow our protocol to achieve unlinkability, unforgeability, and mutual authentication.

### *1.2. Roadmap*

The rest of the paper is structured as follows: Section 2 presents the VANETs architecture and our scheme's design goals. Section 3 reviews the related work on location privacy that aims to achieve unlinkability. In Section 4, we present the security and privacy model of the improved Chaff-based CMIX. In Section 5, we introduce our improved CMIX scheme. Section 6 gives a comprehensive security analysis. Section 7 is dedicated to a comparison between our scheme and similar schemes in the literature. Finally, Section 8 concludes the paper.

## 2. Background

### *2.1. VPKI Architecture*

The heterogeneous VANET architecture primarily consists of three bodies, i.e. vehicles, $RSU$s and CAs. The vehicle is also called an OBU, a transceiver board placed on the vehicle to exchange information with CAs, $RSU$s and other vehicles. Each $RSU$ and vehicle has credentials and private keys for safe and secure communication. CAs register and certify the public keys to vehicles and $RSU$s. $RSU$s are used to monitor road traffic and minimise accidents. They also provide access points for vehicles and other $RSU$s to disseminate information securely and effectively. Although $RSU$s use wire-based communication, vehicles use wireless communication between each other and with $RSU$s. Note that this protocol can be executed in tunnels and other confined areas due to this communications features; see Figure 1 for a standard VANET architecture. In general, the VPKI should have the following list of CAs [8,14]:

1. The root CA (RCA) 1 is at the top of the hierarchy, serving as a governance body that certifies other intermediate authorities.
2. The long-term CA ($LTCA$) 1 is an intermediary authority that is responsible for vehicle registration and long-term certificate issuance for vehicles and $RSU$s.
3. The resolution authority (RA) 1 is a central authority that can address a pseudo-identity and thereby validate the long-term identity of the vehicle in the event of a fraudulent act by communicating with the $LTCA$ and the $PCA$.
4. The pseudo-identity CA ($PCA$) 1 is an intermediary authority responsible for issuing pseudo-identities for registered vehicles.

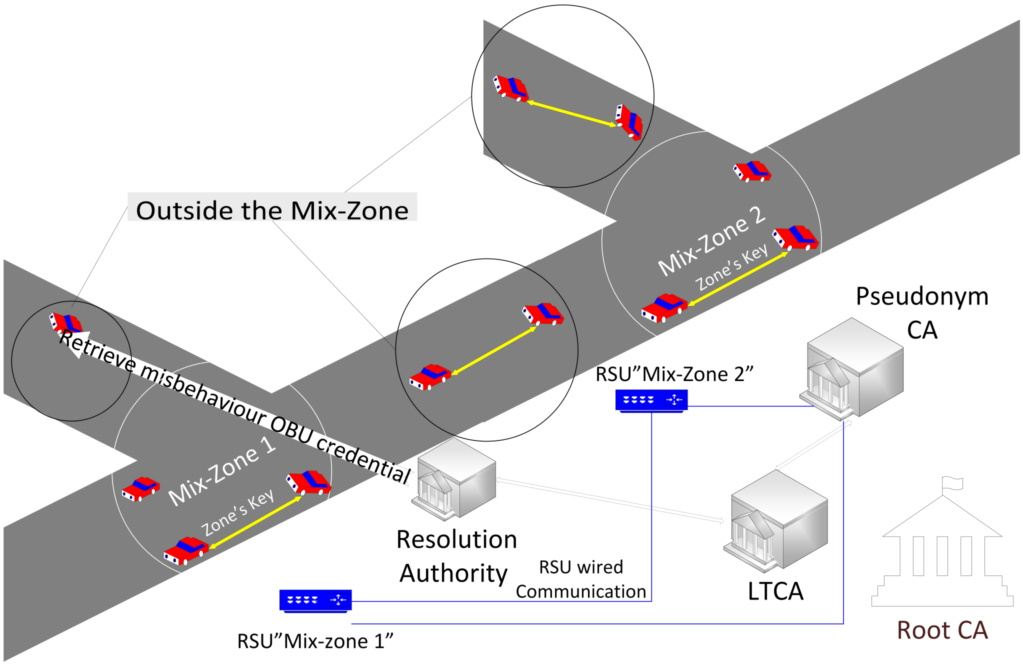


**Figure 1.** Our C-ITS PKI High-Level Architecture: 1) RCA is a government entity, and it is responsible for managing all subordinate CAs. 2) $LTCA$ is responsible for entity registration and issuing certificates. 3) RA is responsible for retrieving misbehaving entities' credentials. 4) $PCA$ is responsible for pseudonym issuance. Moreover, $RSU$s are responsible for vehicles entering/leaving the mix-zones. There are two types of communication: 1) Through a shared key that is distributed by $RSU$s inside the mix-zone [8]. 2) Anonymous communication, which is performed outside the mix-zone .

Also, the RCA manages various domains through cross-certification. There is only one $LTCA$ in each domain, and vehicles must register in the home domain. However, they may cross domains and communicate with foreign $LTCA$s to gain pseudo-identities. As far as the $PCA$ is concerned, it may be involved in one or even several domains. Therefore, if the vehicle requires a pseudo-identity, the $LTCA$ can only offer one authentication ticket per vehicle, and the authorisation will be with the certificate gained from the $LTCA$. In PKI-based systems, even though the use of pseudo-identities as anonymised certificates guarantees the anonymity of the identity [16], it cannot guarantee the privacy of the position. For example, a vehicle has to change its pseudo-identity during its trip. However, the eavesdropping monitor with two observation points in the same road will link the changing of a moving vehicle's pseudo-identity.

### *2.2. Design Goals*

The proposed work should satisfy security and privacy preservation through the following goals:

- **Authentication:** Authentication: There are two forms of authentication: mutual authentication and message authentication. Mutual authentication demands the ability of two entities to identify each other at a specified session. Message authentication confirms the integrity of the messages and proves that they are generated from authorised vehicles and have not been unmodified through the transmission.
- **Nonrepudiation:** This property applies to a case in which the recipient is willing to show to a third party that the sender cannot dispute responsibility for the messages' generation. It prevents the attacker from forging messages with other identities.

In a particular scenario of VANET low density, we aim to achieve essential properties.

- **Unlinkability:** The certificate and information in the messages have to be unlinkable for privacy protection, even if identical vehicles change certificates or the exact vehicle sends new messages with new data, so that an adversary can never discover shared properties in several messages and then link them to a specific vehicle and trace its location. The change time to time in each communication and in the mix-zone on pseudo-identity rather than real identity. Also, certificates in the communication have a relation with the pseudo-identity.

## 3. Related Work

Several types of research have been published on pseudo-identity unlinkability and vehicle privacy in ITS. This section includes our review of the most recent works on location privacy, which is also a significant element that needs to be considered [17], as well as pseudo-identity change management in VANETs. Due to the data transmission in VANETs for safety applications and the amplification in broadcasting technology, messages can be made open to adversaries; thus, it is easy to listen to the correspondence channels via the ITS infrastructure [18–20]. In this context, researchers have attempted to prevent the attacks related to linking the communications' information. Various studies have focused on unlinkability accomplishment by optimising the pseudo-identity change management mechanism to retain vital details, such as position and trajectory. However, we are now seeing that various literature schemes suffer from a vulnerability to linkability attacks that breach privacy.

Note that the following parameters are listed in the ETSI ITS technical report [8] on pseudo-identity change management as not adequate for different reasons, namely: 1) fixed parameters, 2) silent period, 3) randomness, and 4) CMIX. Eckhoff *et al.* [21] suggested allowing a pool of pseudo-identities for each vehicle to use within one week, whereby each pseudo-identity will be valid for ten minutes without overlapping, which is a fixed parameters scheme. It will deter attacks, such as Sybil attacks, and address the trade-off between privacy and safety. However, the use of fixed parameters is straightforward, and this allows the adversary to know the parameter values of a given vehicle, making it easier to trace them. Choosing randomness dependent on fixed parameters, such as randomly changing the pseudo-identity every five minutes plus or minus one minute, helps deter the attacker from detecting a change in the pseudo-identity. However, it is still possible to link attacks when a few vehicles change their pseudo-identities while others retain their old ones. Besides, an attacker can track vehicles effortlessly by using trajectory predictability algorithms, such as Kalman filters [22], especially when the density is not high or when a few vehicles change their pseudo-identities while others maintain theirs [8]. Some researchers propose shutting off the wireless transmitter at an unspecified point and changing pseudo-identities during the silent period [10,23–27]. Vehicles would have adequate protection during this time, but this would dramatically limit protection due to the non-broadcasting series of CAMs, which would lead to an increase in vehicles accidents.

In addition to the silent period, Buttyan *et al.* propose changing the pseudo-identity when the vehicle's speed is less than 30 km/h [26]; however, this does not take into account low-density situations that lead to linking attacks. On the other side, Boualouache *et al.* in [10] suggested a Vehicular Location Privacy Zone (VLPZ) to regulate service stations (e.g. diesel, fuel and charging stations or toll booths). However, syntactic linking attacks can easily occur due to the lack of coordination caused by the silent period [28], and the attackers may track the pseudo-identity change [22]. Additionally, the link attack's impact worsens in low-density situations due to the simplicity of analysing a low number of vehicles. Conversely, the mix-zones concept does not need to limit the feasibility of safety applications. Initially, the mix-zone approach was proposed by Beresford *et al.* [12], leading to the use of a pre-defined geographical region to change pseudo-identities. These zones have a CA hierarchy, and the semi-honest *RSU*s dominate the mix-zone. Freudiger *et al.* enhanced the scheme by inserting a symmetric key to encrypt messages among vehicles within the mix-zone and called it a CMIX [13]. While CMIX-based systems are sensitive to linking attacks, they depend heavily on vehicle traffic, vehicle arrival, speeds, and probable vehicle movements through mixed zones. These schemes are also vulnerable to linking attacks in low-density [8] scenarios. Lu *et al.* [29] proposed changing pseudo-identities at social spots, i.e. a public space, which gives the benefit of traffic to confuse the attacker. For example, vehicles stopped at traffic lights can change their pseudo-identities when these turn green, and in shopping mall parking, vehicles can change their pseudo-identities before they exit. However, this scheme is simplistic and inadequate to guarantee unlinkability because high density does not guarantee that certificates can be linked and traced back to identity. The authors in [30] proposed a context-based system to use credibility scores sent in order to cause synchronous pseudo-identity changes; those scores are part of the periodic safety beacons, thus increasing the anonymity set. With the same, i.e. context-based, approach Liu *et al.* [31] presented another pseudo-identity change management technique, which is an entirely uncoordinated pseudo-identities change in distributed networks after a random delay to allow regular and unlinkable changes, whereby they suppose that the anonymity can be accomplished at trivial throughput loss is in large networks. Zhao *et al.* [32] proposed a pseudo-identity changing game that is mixed-context and was developed by examining the relationship between changing the pseudo-identity, expense, and privacy. Moreover, Zeng and Xu [33] suggested pseudo-identity changing privacy preservation authentication based on a mixed-context. However, attackers could easily threaten these systems if the density is low, as with traffic-based techniques.

Furthermore, a dynamic zone-based pseudo-identity change management [34] has recently been proposed to set up a temporary on-demand swap zone in which a vehicle will randomly pick and exchange a pseudo-identity with another vehicle without a group manager. This change adapts to reduce the contact cost of establishing pseudo-identity swap zones based on the environment.

Benarous *et al.* 's [35] proposal based on two main factors: the strategies of "hiding inside the crowd" and "location obfuscation". When the vehicle either exits a particular geographical area or the pseudo-identity reaches its expiry, it must change it. This change management holds the count of the neighbouring vehicles, and if the pre-defined neighbour threshold matches the current neighbours, then it changes pseudo-identity with other vehicles cooperatively. Otherwise, for the vehicle to change its pseudo-identity, the vehicle obfuscates its location and turns the speed to zero. The downside is that the unreliable broadcasting of speed and location information poses questions regarding safety applications. In 2018, Christian *et al.* [14] introduced a development for CMIX by adding Chaff messages (representing vehicles on the road) to stabilise the density in low-density scenarios in CMIX. Hence, the Chaff-based CMIX protocol alleviates Freudiger *et al.* 's CMIX scheme's weaknesses in low-density situations by confusing the attacker to strengthen the CMIX scheme. As ETSI ITS confirmed the importance of considering the low density as mentioned in their report "the higher the density of vehicles, the more efficient the mix-zone is against tracking." [8]. Moreover, this scenario is possible in the peak and off peak hours daily. Furthermore, the lock down in Coronavirus Disease of 2019 (COVID-19) pandemic rises the chances of low-density scenarios in different countries. In fact, this emphasizes the value of Christian *et al.* 's scheme. However, their Chaff-based CMIX scheme has some issues that could break the system.

## 4. Security and Privacy Issues of Christian *et al.* 's Chaff-based CMIX scheme

Christian *et al.* [14] proposed a protocol using Chaff messages in low-density scenarios to increase the number of fake vehicles which prevents linkability attacks. However, there is a security vulnerability their protocol which is run outside the mix-zone. More concretely, the signature and the certificate are not encrypted in the following message which allows attackers to break the unlinkability:

$$C_{PS_{VID_j}} = Enc_{PK_{VID_j}}(sk_r, CF_r, Sign_{RSU_i}), t_j, Sign_{PS_{VID_j}}, Cert_{PS_{VID_j}}$$

where $PS_{VID_j}$ is the pseudo-identity of the $j$-th vehicle $VID_j$, $PK_{VID_j}$ is the public key of $PS_{VID_j}$ while $Enc_{PK_{VID_j}}$ denotes message encryption with the specified key, $sk_r$ is the symmetric key of the $r$-th mix-zone, $CF_r$ is the CF of the $r$-th mix-zone, $Cert_{PS_{VID_j}}$ is the $VID_j$'s certificate, and $Sign_{RSU_i}$, $Sign_{PS_{VID_j}}$ denote $RSU_i$'s and $VID_j$'s signatures. Also, the message contains non-encrypted values, namely the timestamp $t_j$, the sender's signature $Sign_{VID_j}(M_{V2R})$, and the certificate $Cert_{VID_j}$. Nevertheless, sending these messages outside the mix-zone leads to the following security issues:

- **The privacy of vehicles can be compromised.** Vehicles update their pseudo-identity once they move from one mix-zone to another. However, outside mix-zones, while they communicate with other vehicles securely, they also send $Cert_{VID_j}$ and $Sign_{VID_j}$ separately. Therefore, it is trivial for the adversary to link the old and the new pseudo-identities, meaning they can identify the sender, which breaks the unlinkability property.
- **Unreliable CFs update.** To update the CF, vehicles forward the $CF_i$ as a new version in a ciphertext; Christian *et al.* argue that the signature of $RSU_i$ is attached to prevent forgery attacks. It is possible for malicious vehicles to inject real pseudo-identities and send them to the $RSU_i$ inside the mix-zone or other vehicles, subsequently denying this malicious activity . Moreover, if an adversary compromises the $RSU_i$ and tries to tamper with the CF, the vehicles will discard messages from these finger-printed pseudo-identities, which leads to accidents by affecting safety applications.
- **The secret key of the mix-zones can cause leakage.** The ciphertext $C$ contains the encryption key $sk_r$, which must only be used in the specified area. The receiving of this key outside the mix-zone by an external unauthorised vehicle (i.e., the mix-zone is compromised ) threatens the security of the communication. Hence, an attacker would be able to communicate maliciously with honest vehicles outside the specified area, which would break the system's safety.

Besides, we should note here that Mitzenmacher *et al.* [36] specified a drawback that may affect the CF's performance. In particular, they should that the false positives that can occur in a CF may affect the search for an element inside these hash tables. To fix this, they proposed a technique that identified the element that caused false positives, then removed it and re-inserted it again differently. Then, if they searched for that element, it would be found. Undoubtedly, the performance of the filter in a Chaff-based scheme plays a vital role. Thus, we are using ACF rather than CF in our scheme.

## 5. Our Improved Chaff-based CMIX scheme

We are now ready to describe our VPKI based scheme. We utilise a modified version of Wang *et al.* 's Identity Based Signature (IBS) construction by replacing IDs with certificates to comply with Christian *et al.* 's protocol [15]. The setup is as follows:

### *5.1. Setup*

Let $\mathbb{G}_1$, $\mathbb{G}_2$ be cyclic groups of prime order $q$, and $g_1, g_2$ be generators of $\mathbb{G}_1$, $\mathbb{G}_2$, respectively. Let also $H_1, H_2, H_3, H_4$ be hash functions where

$$H_1 : \{0,1\}^* \to \mathbb{G}_1,$$
$$H_2 : \mathbb{G}_2 \to \mathbb{K},$$
$$H_3 : \{0,1\}^* \to \{0,1\}^\ell,$$
$$H_4 : \{0,1\}^* \to \mathbb{Z}_q^*$$

$\mathbb{K}$ is a keyspace, and $\ell$ is a security parameter while $\mathbb{Z}_q^*$ is the multiplicate group (which is a list of integers modulo $q$ and are co-prime with $q$.). Let also $RSU_i$ and $VID_j$

be the long-term identities of the $i$-th $RSU$ and the $j$-th vehicle, respectively. Also, denote $PS_{VID_j}$ for the pseudo-identity of the $j$-th vehicle. Let $(pk_{LTCA}, sk_{LTCA})$ be a public and private key pair, and $msk_{LTCA}$ be the master secret key of $LTCA$. During the setup of $RSU$ and vehicle, $LTCA$ first chooses $x, y, z \in_R \mathbb{Z}_q^*$ and computes $X = g_1^x$, $Y = g_1^y$ and $Z = g_1^z$. $LTCA$ maintains a public list $List_{pub}$ and a private list $List_{priv}$ for $PCA$ and $RSU$. As we describe below, $RSU_i$ is going to maintain $List_{pub}$ for having mutual authentication, while $PCA$ is going to maintain $List_{priv}$ for tracking the authentication details of registered vehicles. Next, we describe the setup of the $RSU$ and vehicles:

- **RSU setup:** $LTCA$ generates $sk_{RSU_i}$ from $(msk_{LTCA}, RSU_i)$ in $\mathbb{K}$ and sends it to $RSU_i$. $LTCA$ also generates $Cert_{RSU_i} = Sign_{sk_{LTCA}}(pk_{RSU_i})$, where $pk_{RSU_i}$ is the public key with respect to $sk_{RSU_i}$. $RSU_i$ then computes $R_i = g_1^{r_i}$ and $E_i = g_2^{e_i}$, where $r_i, e_i \in_R \mathbb{Z}_q^*$, and stores the tuple $(PP_i, R_i, E_i)$ for later to securely communicate with the vehicles entering the mix-zone.
- **Vehicle Setup:** Whenever a vehicle $VID_j$ enters to a new $LTCA$ region, $LTCA$ first generates $sk_{VID_j}$ from $(msk_{LTCA}, VID_j)$ in $\mathbb{K}$ and sends it to $VID_j$. $LTCA$ also generates $Cert_{VID_j} = Sign_{sk_{LTCA}}(pk_{VID_j})$, where $pk_{VID_j}$ is the public key with respect to $sk_{VID_j}$. $VID_j$ stores $((pk_{VID_j}, sk_{VID_j}), Cert_{VID_j})$. $LTCA$ also incorporates the tuple $\{Cert_{VID_j}, H_j, A_j, r_j, P_j, T_j\}$ into $List_{priv}$ in $PCA$ and $\{A_j, P_j, T_j\}$ into List $List_{pub}$ that is accessible for $RSU_i$, and when $Tj$ expires in each, $PCA$ forces the vehicles to refresh their authentication keys. The $LTCA$ also loads existing $RSU$s' certificates to the vehicle. Next,
    1. $VID_j$ picks $a_j' \in_R \mathbb{Z}_q^*$ and then computes its authentication key $a_j = H_4(a_j', t_j)$, where $t_i$ is the timestamp.
    2. $VID_j$ computes $H_j = H_1(Cert_{VID_j}, a_j)$, $A_j = g_1^{a_j}$, and sends $(M, Sign_{VID_j}(M)$, $Cert_{VID_j})$ to $LTCA$, where $M = (Cert_{VID_j}, H_j, A_j)$. The authentication key $a_j$ is saved in $VID_j$.
    3. $LTCA$ generates a challenge $R_j = g_1^{r_j}$ and a dynamic password $P_j = A_j^{r_j}$, where $r_j \in_R \mathbb{Z}_q^*$. The challenge $R_j$ is sent to $VID_j$, which stores it locally.
    4. $LTCA$ maintains the tuple $\{Cert_{VID_j}, H_j, A_j, r_j, P_j, T_j\}$, where $T_j$ is the expiration date.
- **PCA Setup:** $LTCA$ generates $sk_{PCA}$ from $(msk_{LTCA}, PCA)$ in $\mathbb{K}$ and sends it to $PCA$. $LTCA$ also generates $Cert_{PCA} = Sign_{sk_{LTCA}}(pk_{PCA})$, where $pk_{PCA}$ is the public key with respect to $sk_{PCA}$. Also, $LTCA$ sends $x, y, z, \in_R \mathbb{Z}_q^*$ and $List_{priv}$ to $PCA$. Then, $PCA$ generates the public parameters $s, \hat{r}_j, r_j^*, e_j \in_R \mathbb{Z}_q^*$.
- **RA Setup:** $LTCA$ sends $x, y, z, \in_R \mathbb{Z}_q^*$, $List_{priv}$ and the registered $RSU$s identities to $RA$, while $PCA$ sends $s \in_R \mathbb{Z}_q^*$ and $PS_j$. Therefore, these values help $RA$ to detect any malicious vehicles or $RSU$s.

Note that $LTCA$ obligates vehicles to update their authentication keys if $T_j$ is expired.

### *5.2. Mutual Authentication*

The authentication between $RSU$s and vehicles starts once the vehicles are in the transmission range of the $RSU$s. In the following, we describe the protocol between $RSU$ and vehicles.

1. $RSU_i$ broadcasts $\mathcal{B}$=$(M_{R2V}, Sign_{RSU_i}(M_{R2V}), Cert_{RSU_i})$, where $M_{R2V} = (PP_i, ACF_i$, $R_i, E_i, t_i)$, where $R_i$ along $t_i$ is the timestamp and $E_i$ is used to generate symmetric keys and $ACF_i$ is the ACF of $RSU_i$.
2. A vehicle $VID_j$ entering the transmission range receives $\mathcal{B}$ and validates the signature $Sign_{RSU_i}(M_{R2V})$. If not verified, it aborts the protocol. Otherwise, $VID_j$ stores $\mathcal{B}$.
3. $VID_j$ next computes
    (a) $P_j = R_j^{a_j}$ and $P_i = R_i^{a_j}$.

(b) $F_j = g_2^{f_j}$ and $K = H_2(E_i^{f_j})$, where $f_j \in_R \mathbb{Z}_q^*$.

(c) $C_j = Enc_K(M_{VR}, Sign_{VID_j}(M_{VR}),$ $Cert_{VID_j}, F_j, t_j)$, where $M_{VR} = (P_j, P_i, H_3(Cert_{RSU_i}, P_j, P_i, F_j, t_i, ACF_j)$ and sends $C$ to $RSU_i$.

4. $RSU_i$ now computes the symmetric key $K = H_2(F_j^{e_i})$ and decrypts $C$. Next, $RSU_i$

(a) first validates the signature $Sign_{VID_j}(M_{VR})$, and aborts if it is not valid.

(b) aborts the protocol if $H'_{VR} \neq H_3(Cert_{RSU_i}, P'_j, P'_i, F_j, t_i)$, where $M'_{VR} = (P'_j, P'_i, H'_{VR})$.

(c) verifies $ACF_i$ and aborts if it is not valid.

(d) searches for a tuple $\{A', P', T'\}$ in $List_{pub}$, where $P' = P'_j$.

(e) aborts the validation if the tuple is expired or it is not in $List_{pub}$, or it has more than one tuple.

(f) computes $P''_i = (A')^{r_i}$.

(g) If $P''_i = P'_i$ then $VID_j$ will be authenticated to $RSU_i$ without revealing its identity.

### *5.3. Privacy Preservation: Pseudo-Identity Generation and Updating Authentication key*

Our scheme provides privacy preservation by focusing on pseudo-identity generation to achieve untraceability and the update of the authentication key to accomplish full unlinkability.

#### 5.3.1. Pseudo-identity Generation for Vehicles

To preserve privacy and untraceability between vehicles, they need to use pseudo-identities rather than their real identities. As mentioned previously, $PCA$s are responsible for pseudo-identity generation. After $VID_j$ is in the transmission range of $RSU_i$, the vehicle generates pseudo-identity as follows:

- $VID_j$ computes the pseudo-identity of itself as $PS_{VID_j} = (S, \Pi_0, \Pi_1) = (g_1^s, H_1($ $Cert_{VID_j}, a_j)X^s, Y^s Z^{\theta s})$, where $s \in_R \mathbb{Z}_q^*$ and $\theta = H_4(g_1^s, H_1(Cert_{VID_j}, a_j)X^s)$ [1].
- $PCA$ manages the generation of fake pseudo-identities $Chaff_{PS_j}$ and fingerprints them $FP(Chaff_{PS_j})$ and signs them $Sign_{RSU_i}(FP(Chaff_{PS_j}))$ before inserting them into the ACFs. Then, $RSU_i$ signs the whole ACF $Sign_{RSU_i}(ACF_i)$ to provide non-depuration and distributes it to the vehicles.

$RA$ can detect the real identity of the vehicle if it has malicious activities, as follows. Let $VID_j$ be a malicious vehicle and its pseudo-identity be $PS_j$. The $RA$ obtains $(S, \Pi_0, \Pi_1)$ and computes $\theta = H_4(S, \Pi_0), \Pi'_1 = S^{y+\theta z}$. It then checks whether $\Pi'_1 \stackrel{?}{=} \Pi$. The pseudo-identity is invalid if they are not equal. Otherwise, $RA$ computes $H = \Pi / S^x$. If $\{Cert_{VID_j}, H_j, A_j, r_j, P_j, T_j\}$ is valid in $List_{priv}$ and $H_j = H$, then $RA$ attempts to find the $Cert_{VID_j}$ from its database and learns the real identity of $VID_j$. For privacy reasons, the real identity of the vehicle $VID_j$ must be hidden from other $RSU$s and vehicles.

#### 5.3.2. Unlinkability through Updating Authentication Key

In order to provide unlinkability, the system must update the authentication key and the ACF regularly. Assume that the tuple $(Cert_{VID_j}, H_j, A_j, r_j, P_j, T_j)$ has expired based on the expiration date $T_j$. Here below, to update the authentication key, $PCA$ and the vehicle $VID_j$ run the protocol.

1. $PCA$

[1] Note that the pseudo-identity of $VID_j$ is equal to the encryption of $H_1(Cert_{VID_j}, a_j)$ through the Cramer-Shoup encryption scheme [37], which is non-malleable and secure against adaptive chosen-ciphertext attack (CCA2)

(a) first generates a pseudo-identity $PS_j = (A_j, H_j A_j^x, A_j^{y+\theta z})$ for vehicle $VID_j$, where $\theta = H_4(A_j, H_j A_j^x)$.
(b) computes $\hat{R}_j = g_1^{\hat{r}_j}, R_j^* = g_1^{r_j^*}, E_j = g_2^{e_j}$, where $\hat{r}_j, r_j^*, e_j \in_R \mathbb{Z}_q^*$. $\hat{R}_j$ is used for the targeted vehicle $VID_j$, $R_j^*$ is used for $VID_j$, and $E_j$ is used to generate a shared key.
(c) computes a signature $Sign_{PCA}(M_{PCA})$, where $sk_{PCA}$ = generated from $(msk_{PCA}, PS_j)$ and $M_{PCA} = (PS_j, \hat{R}_j, R_j^*, \hat{t}_j)$, and $\hat{t}_j$ is a timestamp.
(d) broadcasts $\mathcal{B}' = (M_{PCA}, Sign_{PCA}(M_{PCA}), Cert_{PCA})$.

2. $VID_j$
   (a) receives $\mathcal{B}'$.
   (b) validates the signature $Sign_{PCA}(M_{PCA})$ using $pk_{PCA}$.
   (c) checks the freshness of the timestamp $\hat{t}_j$.
   (d) checks if $PS_j \stackrel{?}{=} (g_1^{a_j}, H_1(Cert_{VID_j}, a_j)X^{a_j}, Y^{a_j}Z^{\theta a})$, where $\theta = H_4(g_1^{a_j}, H_1 (Cert_{VID_j}, a_j)X^{a_j})$ with $a_j$ being the authentication key. Note that only the $VID_j$ that holds $a_j$ can compute this pseudo-identity.
   (e) updates the authentication key by computing $a_j^* = H_4(a_j, t_j), A_j^* = g_1^{a_j^*}, H_j^* = H_1(Cert_{VID_j}, a_j^*), F = g_2^f, K' = H_2(E^f)$ and $\hat{P}_j = \hat{R}^{a_j}$, where $a_j^*, f \in_R \mathbb{Z}_q^*$.
   (f) sends $C_j = Enc_{K'}(M_{PCA}, Sign_{VID_j}(M_{PCA}), Cert_{VID_j}), F, t_j)$, where $M_{PCA} = (A_j^*, \hat{P}_j, H_j^*, H_3(Cert_{PCA}, A_j^*, \hat{P}_j, t_j))$ to $PCA$.
3. $PCA$
   (a) first decrypts $C_j$ and obtains $M'_{PCA}, Sign_{VID_j}(M'_{PCA}), Cert_{VID_j}), F, t_j$, where $M'_{PCA} = (A', \hat{P}'_j, \hat{H}_j^*, H'_{PCA})$.
   (b) validates $Sign_{VID_j}(M'_{PCA})$.
   (c) aborts if $H'_{PCA} \neq H_3(Cert_{PCA}, A', \hat{P}'_j, t_j)$.
   (d) computes $P'_j = A_j^{\hat{r}_j}$ and aborts if $\hat{P}'_j \neq P'_j$.
   (e) computes $P_j^* = (A')^{r_j^*}$ and updates $\{Cert_{VID_j}, A_j, H_j, r_j, P_j, T_j\}$ with $\{Cert_{VID_j}, A_j^*, \hat{H}_j^*, r_j^*, P_j^*, T_j^*\}$ in $List_{priv}$, where the expiration time is $T_j^*$.
   (f) The tuple $\{A_j, P_j, T_j\}$ is updated with $\{A_j^*, P_j^*, T_j^*\}$ in $List_{pub}$.
   (g) computes $\overline{R_j} = g_1^{\overline{r_j}}, \overline{P_j} = (A')^{\overline{r_j}}$, where $\overline{r_j} \in_R \mathbb{Z}_q^*$,
   (h) broadcasts $(\overline{M}_{PCA}, \overline{t_{PCA}}, Sign_{PCA}(\overline{M}_{PCA}), Cert_{PCA})$, where $\overline{t_{PCA}}$ is a timestamp and $\overline{M}_{PCA} = (PS_A, \overline{P_j}, \overline{R_j})$.
4. $VID_j$ receives and checks the validity of the message. If the signature $Sign_{PCA}(\overline{M}_{PCA})$ is valid and the timestamp $\bar{t}$ is fresh, then it computes $\overline{P_j}' = \overline{R}^{a_j^*}$.
5. $VID_j$ aborts if $\overline{P_j} \neq \overline{P_j}'$. Otherwise, the current authentication key $a_j$ and challenge $R_j$ are replaced with $a_j^*$ and $R_j^*$, respectively.

## 6. Security Analysis

We are now ready to provide a security analysis of our scheme.

### *6.1. Mutual Authentication*

During the mutual authentication, the vehicle $VID_j$ validates $Sign_{RSU_i}(M_{R2V})$ and $Cert_{RSU_i}$ which are received from the broadcast message by $RSU_i$, i.e. $\mathcal{B}$=$(M_{R2V}, Sign_{RSU_i} (M_{R2V}), Cert_{RSU_i})$. Therefore, authentication is provided through signatures and certificates as long as $LTCA$ is honest. Next, to be able to generate a shared key, $VID_j$ first computes its $P_j = A_j^{r_j}$ and $P_i = A_j^{r_i}$, where $R_i = g_1^{r_i}$ is sent by $RSU_i$. Then, the

$RSU_i$ can recover $P_j = A_j^{r_j}$ from $\{A_j, P_j, T_j\}$ in the list $List_{pub}$. Hence, even if $R_i$ and $A_j$ given to other entities, to generate valid $P_i$ and $P_j$ they must know either $a_j$ of $VID_j$ or $r_i$ of $RSU_i$. However, since these private values are only known by $VID_j$, $RSU_i$ and certificates are used for authentication, no adversary can compute the shared key due to the underlying Computational Diffie-Hellman (CDH) problem. Therefore, our scheme provides message confidentially inside the mix-zone.

### *6.2. Non-repudiation*

Every message generated by the vehicle $VID_j$ or $RSU_i$ uses the digital signature as evidence of non-repudiation. Also, digital certificates, which are issued by $LTCA$, contain an expiration date. Therefore, $Sign_{VID_j}$ already involves the timestamp $t_j$ and the receiver checks whether the $Cert_{VID_j}$ is valid or not for the pseudo-identity $PS_j$. Thus, if $VID_j$ or $RSU_i$ behaves maliciously, $RA$ can easily detect and revoke their certificates. Hence, non-repudiation is guaranteed.

### *6.3. Unlinkability*

Our scheme preserves privacy by signing the messages with different pseudo-identities. The real identity is secretly hidden in these messages because $PS_j = (g_1^{a_j}, H_1(Cert_{VID_j}, a_j)X^{a_j}, Y^{a_j}Z^{\theta a})$ is computed by the authentication key $a_j$ where $\theta = H_4(g_1^{a_j}, H_1(Cert_{VID_j}, a_j)X^{a_j})$. Note that this key is only accessible by $VID_j$. For accountability reasons, $RA$ can compute $PS_j = (A_j, H_jA_j^x, A_j^{y+\theta z})$ for the vehicle $VID_j$ where $\theta = H_4(A_j, H_jA_j^x)$ because the public parameters $x, y, z \in_R \mathbb{Z}_q^*$ are known by all the certificate authorities $LTCA$, $RA$, and $PCA$. Hence, no adversaries can obtain the real identity from the ciphertext $H_1(Cert_{VID_j}, a_j)$. Moreover, we also prevent information leakage by providing mutual authentication and sending Chaff messages on the road to mitigate the risk of linkability attacks by eavesdropping adversaries due to the low-density traffic. Therefore, our scheme provides unlinkability.

| | **Our scheme** | [14] | [21] | [13] | [15] | [10] | [35] |
|---|---|---|---|---|---|---|---|
| **Sufficient density** | ✓ | ✓ | × | × | × | × | × |
| **Unlinkability** | ✓ | × | × | × | ✓ | ✓ | ✓ |
| **Mutual authentication** | ✓ | × | × | × | ✓ | × | × |
| **Non-repudiation** | ✓ | × | ✓ | ✓ | × | ✓ | × |
| **Cryptographic Mix-zone** | ✓ | ✓ | × | ✓ | × | × | × |
| **Outside mix-zone privacy** | ✓ | × | × | × | × | × | × |
| **No interference with safety applications** | ✓ | × | ✓ | ✓ | × | × | × |

Table 1: A Comparison of proposed and existing schemes

### *6.4. Defence against compromised RSU*

In the proposed system, we assume that the CAs are fully trusted while the $RSU$s and the vehicles are semi-trusted which means that they are trusted but cannot know some sensitive and private data of the vehicles. Thus, $LTCA$ generates the private key $sk_{RSU_i}$ and the $Cert_{RSU_i}$ based on its master key. Therefore, if $RSU_i$s corrupted, it can be detected through the credentials generated by $LTCA$ which can immediately revoke the $RSU$'s certificate. Moreover, the corrupted $RSU_i$ can also manipulate the $ACF$. This manipulation impairs the safety application and can cause accidents. However, in our scheme, $RSU_i$ signs the fingerprinted Chaff $Sign_{RSU_i}(FP(Chaff_{PS_j}))$, which helps to detect the $RSU_i$ in case it has malicious activities.

## 7. A Comparison of proposed and existing schemes

In the previous section, we focused on three desired properties, namely mutual authentication, non-repudiation and unlinkability. Besides, it is also essential to show that our scheme is robust against low density. Note that previous studies have not given much attention to low density scenario. The comparison in Table 1 shows more factors related to existing VANETs' location privacy schemes. Moreover, it summarises that our scheme overcomes the vulnerabilities of [14] which are presented in Section 4. Here we illustrate a security and privacy vulnerabilities in a related existing schemes:

- Unlinkability: The fixed parameters schemes like [21] or schemes using the randomness such as [31] are vulnerable to linkability attacks. Besides, most of the existing works does not consider the traffic variability, which may help the attackers to break the unlinkability.
- Non-repudiation: Some schemes relies on identity changes after a random delay, if malicious vehicles do not change the pseudo-identity intentionally, then they will break the system. The randomness and the delay will break the non-repudiation. Also, in [35] that based on location obfuscation and hiding in the silent period. The location obfuscation means the vehicle can turn the speed to zero and obfuscate the position while changing the pseud-identity. Hence, it affects the safety applications. Thus, if a malicious vehicle tried to harm those applications purposely, it can deny it because the location obfuscation is part of the system. The non-repudiation issues of [14] are related to the quality of *CF* that can breach the system. Besides, the scheme in [15], is considering the *RSU* as fully trusted; without a digital signature in the communication, it can deny any malicious activities.
- CMIX: The schemes tends to the CMIX are [13,14] and our scheme. The concept of cryptography in a mix-zone around *RSU* is efficient, but it is associated with road density. The higher the density, the better against tracking.
- No interference with safety application: The necessity of updating the information via messages without any interruption, like silent period, assures the safety application quality. Scheme such as [10,35] using the silent period with different structure. However, this threatens the safety application technologies as reported in [8] technical report. Furthermore, other schemes like [14] that added filter for Chaff messages may weaken the safety application technologies if the filter has been corrupted. Also, in [15] that relies on *RSU*, if it is compromised, it will be easy to abuse the safety application and jeopardize the passengers' safety.

[14] evaluated the performance of their system using three metrics: chaff pseudonym pool size, the number of simultaneously active chaff pseudonyms, and the RSU signature generation overhead. We are consuming more overhead because our system requires mutual authentication as we are using DDH. However, they did not measure the overhead of the filter's hash tables. Our scheme uses *ACF* which also uses hash functions while it has a lower false-positive rate compared to *CF*. The *ACF* can find the elements that caused the false-positives after they occur, delete and re-insert them again in the hash table. Hence, it will help to find them in the search more efficiently than *CF* [36].

## 8. Conclusion

In this paper, we have investigated Christian *et al.* 's Chaff-based CMIX scheme [14] that concentrated on low-density situations as essential and possible scenarios daily. However, their scheme is not sound in achieving security and privacy. Furthermore, the scheme cannot resist linkability attacks in vehicles communication, CF malicious injections, which affect safety applications, and the leakage of mix-zones' symmetric keys to unauthorised vehicles. To overcome the weaknesses of Christian *et al.* 's scheme, we have utilised a version of [15] by using certificates instead of IDs to accomplish mutual authentication to enhance the security and privacy of the legitimate entities. Furthermore, we accomplish unlinkability by preventing low-density exploitation via increasing the density securely and by generating unlinkable pseudo-identities for each message based on an unexampled secret authentication key. Moreover, we increase the efficiency of the Chaff messages by using ACF to overcome the CF disadvantages. To prevent malicious injection in ACFs, the $RSU$ signs the new fingerprinted Chaff pseudo-identities and keeps the distribution for $RSU$s only. We apply a Diffie-Hellman key exchange method after the mutual authentication to prevent unauthorised vehicles from symmetric key access to mitigate any leakage of the mix-zone symmetric key. In future work, we believe that we have to evaluate our scheme and provide performance evaluation results to make the work more convincing. Also, we will investigate our scheme efficiency in tunnels and confined area.

## References

1. G. Naik, B. Choudhury, J.-M. Park, IEEE 802.11 bd & 5G NR V2X: Evolution of Radio Access Technologies for V2X Communications, IEEE Access 7 (2019) 70169–70184.
2. A. Chehri, H. Chehri, N. Hakim, R. Saadane Realistic 5.9 GHz DSRC vehicle-to-vehicle wireless communication protocols for cooperative collision warning in underground mining, Smart Transportation Systems 2020, Springer (2020).
3. Z. Doukha, S. Moussaoui, An SDMA-Based Mechanism for Accurate and Efficient Neighborhood-Discovery Link-Layer Service, IEEE Transactions on Vehicular Technology 65 (2) (2015) 603–613.
4. I. V. Technology, IEEE Standard for Wireless Access in Wireless Access in Vehicular Environments (WAVE)– Networking Services (2016).
5. T. ETSI, Intelligent transport systems (its); vehicular communications; basic set of applications; definitions, Tech. Rep. ETSI TR 102 6382009 (2009).
6. E. ITS, Intelligent transport systems (its); Security; Trust and Privacy Management; Definitions, Tech. Spec. ETSI 102 9412012 (2012).
7. I. V. Technology, IEEE standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages (2013).
8. E. ITS, Intelligent transport systems (its); Pre-Standardization Study on Pseudonym Change Management, Tech. Rep. ETSI 103 4152018(2018).
9. P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, M. Raya, Architecture for Secure and Private Vehicular Communications, in: 2007 7th International Conference on ITS Telecommunications, IEEE, 2007, pp. 1–6.
10. A. Boualouache, S.-M. Senouci, S. Moussaoui, VLPZ: The vehicular Location Privacy Zone, Procedia Computer Science 83 (2016) 369–376.
11. A. Boualouache, S.-M. Senouci, S. Moussaoui, A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks, IEEE Communications Surveys & Tutorials 20 (1) (2017) 770–790.
12. A. R. Beresford, F. Stajano, Location Privacy in Pervasive Computing, IEEE Pervasive Computing (1) (2003) 46–55.
13. J. Freudiger, M. Raya, M. Falegyhazi, P. Papadimitratos, J.-P. Hubaux, Mix-Zones for Location Privacy in Vehicular Networks, ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS) (2007).
14. C. Vaas, M. Khodaei, P. Papadimitratos, I. Martinovic, Nowhere to hide? Mix-Zones for Private Pseudonym Change using Chaff Vehicles, in: 2018 IEEE Vehicular Networking Conference (VNC), IEEE, 2018, pp. 1–8.
15. B. Wang, Y. Wang, R. Chen, A Practical Authentication Framework for VANETs, Security and Communication Networks 2019 (2019).
16. Z. Yang, K. Yang, L. Lei, K. Zheng, V. C. Leung, Blockchain-based decentralized trust management in vehicular networks, IEEE Internet of Things Journal 6 (2) (2018) 1495–1505.
17. J. Huang, D. Fang, Y. Qian, R. Q. Hu, Recent advances and challenges in security and privacy for v2x communications, IEEE Open Journal of Vehicular Technology 1 (2020) 244–266.
18. J. Bellatti, A. Brunner, J. Lewis, P. Annadata, W. Eltarjaman, R. Dewri, R. Thurimella, Driving Habits Data: Location Privacy Implications and Solutions, IEEE Security & Privacy (1) (2017) 12–20.
19. S. Narain, T. D. Vo-Huu, K. Block, G. Noubir, Inferring User Routes and Locations Using Zero-Permission Mobile Sensors, in: IEEE Symposium on Security and Privacy (SP), IEEE, 2016, pp. 397–413.

20. X. Gao, B. Firner, S. Sugrim, V. Kaiser-Pendergrast, Y. Yang, J. Lindqvist, Elastic Pathing: Your Speed is Enough to Track You, in: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, 2014, pp. 975–986.
21. D. Eckhoff, C. Sommer, Readjusting the Privacy Goals in Vehicular Ad-Hoc Networks: A Safety-Preserving Solution Using Non-Overlapping Time-Slotted Pseudonym Pools, Computer Communications 122 (2018) 118–128.
22. K. Emara, W. Woerndl, J. Schlichter, CAPS: Context-Aware Privacy Scheme for VANET Safety Applications, in: Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks, 2015, pp. 1–12.
23. K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, K. Sezaki, CARAVAN: Providing location privacy for VANET, AD-a459 198, 2005.
24. K. Sampigethaya, M. Li, L. Huang, R. Poovendran, AMOEBA: Robust Location Privacy Scheme for VANET, IEEE Journal on Selected Areas in communications 25 (8) (2007) 1569–1589.
25. L. Huang, K. Matsuura, H. Yamane, K. Sezaki, Enhancing wireless location privacy using silent period, in: IEEE Wireless Communications and Networking Conference, 2005, Vol. 2, IEEE, 2005, pp. 1187–1192.
26. L. Buttyán, T. Holczer, A. Weimerskirch, W. Whyte, SLOW: A Practical Pseudonym Changing Scheme for Location Privacy in VANETs, in: 2009 IEEE Vehicular Networking Conference (VNC), IEEE, 2009, pp. 1–8.
27. A. Boualouache, S. Moussaoui, S2SI: A Practical Pseudonym Changing Strategy for Location Privacy in VANETs, in: 2014 International Conference on Advanced Networking Distributed Systems and Applications, IEEE, 2014, pp. 70–75.
28. M. Khodaei, H. Noroozi, P. Papadimitratos, Privacy Preservation through Uniformity, in: Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks, 2018, pp. 279–280.
29. 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) (2011) 86–96.
30. L. M. Santos-Jaimes, E. d. S. Moreira, Pseudonym change strategy based on the reputation of the neighbouring vehicles in vanets, DYNA 86 (211) (2019) 157–166.
31. Z. Liu, L. Zhang, W. Ni, I. B. Collings, Uncoordinated pseudonym changes for privacy preserving in distributed networks, IEEE Transactions on Mobile Computing 19 (6) (2019) 1465–1477.
32. Z. Zhao, A. Ye, L. Meng, Q. Zhang, Pseudonym changing for vehicles in vanets: A game-theoretic analysis based approach, in: 2019 International Conference on Networking and Network Applications (NaNA), IEEE, 2019, pp. 70–74.
33. M. Zeng, H. Xu, Mix-context-based pseudonym changing privacy preserving authentication in vanets, Mobile Information Systems 2019 (2019).
34. M. Yang, Y. Feng, X. Fu, Q. Qian, Location privacy preserving scheme based on dynamic pseudonym swap zone for internet of vehicles, International Journal of Distributed Sensor Networks 15 (7) (2019) 1550147719865508.
35. L. Benarous, B. Kadri, S. Boudjit, Alloyed pseudonym change strategy for location privacy in vanets, in: 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), IEEE, 2020, pp. 1–6.
36. M. Mitzenmacher, S. Pontarelli, P. Reviriego, Adaptive cuckoo filters in: (2020) J. Exp. Algorithmics 25, 1, Article 1.1 (March 2020), 20 pages.
37. R. Cramer, V. Shoup, Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2002, pp. 45–64.