IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 1, 2017, accepted January 9, 2018, date of publication February 1, 2018, date of current version April 18, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2800907

Independent Mix Zone for Location Privacy in Vehicular Networks

NAN GUO[1], LINYA MA[2], AND TIANHAN GAO[2]

[1]Computer Science and Engineering College, Northeastern University, Shenyang 110006, China
[2]Software College, Northeastern University, Shenyang 110006, China

Corresponding author: Linya Ma (malinya199303@163.com)

This work was supported by the National Natural Science Foundation of China under Grant 61402095.

ABSTRACT The sensitive information of vehicles is related to location in vehicular networks. Pseudonym change is an effective way to protect the location privacy of vehicles, which is to establish a specific area called mix zone, where at least k number of vehicles change pseudonyms together to obtain k anonymity. However, it depends on the number of collaborative ones in spatiotemporal context. To solve the pseudonym change problem in the low density of vehicles, an independent mix zone scheme, shorted for indMZ, is proposed in this paper. It specifies a pseudonym scheme for the vehicular networks, which consists of the procedures of certification issuance and pseudonym issuance. Each vehicle will have L pseudonyms when it enrolls to a road side units. As a pseudonym is about to be expired, the vehicle can establish a mix zone through beacon messages which are inherently broadcasted in neighborhood periodically. The independent mix zone means that each of the collaborative vehicles will produce some randomized versions of a pseudonym, respectively, and contribute to the desired k-anonymous mix zone. Even in the worst case of zero collaborator, the vehicle can still establish a k anonymous pseudonym change region all by itself. We evaluate indMZ and other mix zone schemes with respective to the performance and strength of location privacy in the low density of vehicular networks. It shows that indMZ can ensure k anonymity with $k/2$ average cost of extended beacon message and be independent on any trusted third party.

INDEX TERMS Vehicular networks, location privacy, mix zone.

I. INTRODUCTION

The rapid development of mobile terminals has increased the wireless data traffic. The growing requirement in high performance mobile communications leads to a fast development of next generation heterogeneous fifth-generation (5G) cellular mobile networks [1]. The 5G networks not only enhance data transmission rate but also improve the chance of connecting much more devices [2]. Vehicular networks are the specific applications of mobile ad hoc networks in the field of intelligent traffic, and are self-organizing, distributed vehicle communication networks [4]. They will have revolutionary development with the application of 5G, where vehicular communications in performance and user experience will be greatly improved [3].

Vehicular networks consist of vehicles and road side units (RSUs), where vehicles communicate with each other (Vehicle-to-Vehicle, V2V) or roadside infrastructures (Vehicle-to-Infrastructure, V2I) during high-speed moving to build a multi-hop communication network [5]. They provide real-time traffic information (such as congestion, accidents, etc.) and state information of vehicle nodes (such as speed, location, direction of travel, etc.) for accident avoidance and traffic route optimization [6]. However, the information can also lead to privacy leakage due to location disclosure.

The location privacy of vehicles consists of three categories. Firstly, communication privacy is related to identity and message of senders and receivers. Secondly, orientation privacy is related to the physical location of vehicles. Finally, route privacy is related to the vehicle's movement [7]. k-anonymous schemes [8]–[12] are proposed to protect the physical location of vehicles and attempt to use a camouflage area that covers other $k-1$ users instead of the target user's real location, thus to make the attacker not identify the target user from k users. Pseudonym is used to protect the identity of senders and receivers. Pseudonym change is to protect the vehicles' movement or trajectory. The most common solution for pseudonym change is to establish a mix zone [13]–[19], where multiple vehicles simultaneously change pseudonyms in an area to confuse the attacker of the association of old and new pseudonyms.

However, in the mix zone schemes [13]–[17], lower density of vehicles and decentralization of the cooperative vehicles are more likely to decrease the strength of location privacy. MPSVLP [18] introduces reputation model to motivate selfish vehicles to cooperate for a mix zone, instead of dealing with low density of vehicles. AVATAR [19] establishes a virtual mix zone for unstable density of vehicles, however, the request region has to be enlarged if the number of participants is less than k. As a tradeoff, broadcasting of footprint signatures brings high communication overhead. Besides, some footprint signatures of remote collaborators in each single virtual mix zone will confuse the V2V communication in the real RSU region.

To solve pseudonym change problem in low density of vehicles, an independent mix zone scheme (shorted for indMZ) is proposed. The main idea is the combination of collaborative mix zone and self-established mix zone. indMZ allows vehicles to generate some randomized versions of a pseudonym, which are indistinguishable to the attacker. This paper is an extension of [20], which proposed to combine the reputation model with virtual mix zone to solve the problem of selfish vehicles. Vehicles use reputation model to motivate others to cooperate and enlarge the request region to establish virtual mix zone to search collaborators as much as possible. Furthermore, in indMZ, we consider the mix zone scheme in low density of vehicles, where the number of collaborative vehicles are less than expectation. The contribution of the paper are specified as follows.

1) It specifies a pseudonym scheme particularly for vehicular networks. When a vehicle registers to the TA, it will obtain a private and public key pair together with a certificate. Later when it moves to a RSU region and enrolls to the RSU, it will obtain L pseudonyms which are unlinkable in different time periods. Furthermore, the pseudonym can later be traced to its identity with the collaboration of RSU and TA if the vehicle is complained. Compared with the existing location privacy schemes, the paper introduces the algorithms to construct pseudonyms.
2) It proposes a novel mix zone establishment scheme indMZ, which allows each of the collaborative vehicles produce some randomized versions of a pseudonym respectively and contribute to the desired k-anonymous mix zone. It also means that the vehicle can establish a k anonymous pseudonym change region all by itself in the worst case of zero collaborator. It is hard for the attacker to associate a randomized pseudonym to a vehicle and even know if there are actually k vehicles participating in pseudonym change either.
3) It applies beacon message to carry the related information of pseudonym change and broadcast in neighborhood. Beacon body is extended with the type of beacon message, pseudonym change time, and the pair of old and new pseudonyms. The relationship between the old and the new pseudonym is encrypted. No extra message is needed to increase communication cost because beacon messages are inherently broadcasted periodically. It also introduces the procedure of session layer before and after pseudonym change, which is accomplished by the procedure of MAC layer in V2V communication.

The remainder of the paper is organized as follows. In Section 2, the state-of-the-art mix zone schemes are discussed. In Section 3, vehicular network model, attack model, and a specific pseudonym scheme are introduced. In Section 4, the proposed independent mix zone scheme is presented in detail. The privacy and performance analysis of it is given in Section 5, followed by conclusions in Section 6.

II. RELATED WORKS

To utilize mix zone schemes to protect the location privacy of vehicles in vehicular networks has been attracting a lot of research, which consists of static mix zone and dynamic mix zone.

Palanisamy and Liu [17] proposed the intersection to be a special location of the fixed mix zone. The sequence of vehicles entering into the fixed mix zone is statistically uncorrelated with the sequence of vehicles exiting it. It requires that there are at least k vehicles in a mix zone to ensure the strength of location privacy. However, if the pseudonym of a vehicle is out of date before reaching a mix zone, the identity of it will be completely exposed. In addition, to hide the correlation between entering and exiting a mix zone has to rely on a large number of vehicles, which reduces the applicability of the method. In [14] vehicles randomly select a period of silence and change pseudonyms after it. The choice of mix zone silence period is very flexible. However, the scheme is not suitable for real-time applications such as collision avoidance, traffic guidance because vehicles will not send any message between silent period. Buttyan *et al.* [15] proposed the SLOW scheme under the consideration that the vehicle is less likely to collide at low speed. The vehicle chooses a silent period at low speed and decelerates at the urban traffic light. Silent period is the ideal location at the lights.

Reference [16] is a density-based location privacy protection scheme in which vehicles are allowed to dynamically create mix zones. The idea is that if a vehicle's communication range has other $k - 1$ ones, all these k vehicles will change its pseudonyms in the same time. The strength of location privacy increases with k value. The k value of this scheme is at least 8 which ensures the probability that an attacker will infer the new pseudonym of the target is less than 0.13. However, if the number of vehicles in a single hop range is less than k, pseudonym change may cause identity exposed. In the dynamic mix zone scheme MPSVLP [18], when the pseudonym of a vehicle is about to be expired, a mix zone will be dynamically established, and other vehicles in the mix zone can decide whether cooperate or not. This scheme introduces reputation mechanism to mix zone scheme. The more frequently the vehicle cooperates in pseudonym change, the larger its reputation becomes. However, in the case that the reputation of the target vehicle is higher than the threshold,

TABLE 1. Index of key notations.

Notation	Description
vid	the identity of a vehicle
SK_v/PK_v	the private/public key of a vehicle
SK_{TA}/PK_{TA}	the private/public key of TA
SK_{RSU}/PK_{RSU}	the private/public key of RSU
$seedKey_{RSU}$	the RSU's secret key for pseudonym
$encKey_{RSU}$	the RSU's secret key for encryption
$bcKey_R$	the secret key used in a secure broadcast region, issued by RSU
$HMAC()$	Hash-based Message Authentication Code algorithm
$Enc.Encrypt()$	encryption algorithm
$Dec.Encrypt()$	decryption algorithm
$KeyGen()$	key generation algorithm
$Sig.Sign()$	signature generation algorithm
$Sig.Verify()$	signature verification algorithm
nym_a^{old}	the latest expired pseudonym of the vehicle v_a
nym_a^{new}	the latest changed pseudonym of the vehicle v_a
k	an anonymous set

other ones entering mix zone will all change pseudonyms, which will cause pseudonym wasted. Du *et al.* [19] introduces auction game to the virtual mix zone scheme. The target vehicle broadcasts the collaborator search request, and the cooperative one will give a footprint signature set. Then the target establishes a virtual mix zone by selecting collaborators who send the largest number of signatures. A complex and differentiated auction game is proposed to help vehicles get the best benefits and proved that even if the total number of vehicles is small, more signatures can be obtained. However, the cooperative vehicles need to generate a set of footprint signatures, which requires a higher computation and storage capacity for vehicles.

III. OVERVIEW

The system model and attack model are introduced. The notation related to the proposed scheme is given as Table 1 shows.

A. SYSTEM MODEL

The model of vehicular network consists of three entities, as depicted in Fig. 1, trusted authority (TA), road side units (RSUs), and vehicles. We assume that all vehicles are registered with a central trusted authority (TA), i.e., the Motor Vehicles Division (MVD), before they are approved for driving on the road. A vehicle is equipped with an OBU (OnBoard Unit), a tamper-proof device that stores the secret information, an event data recorder(EDR), and a Global Position System(GPS). In general, vehicles communicate with their neighbors directly within 300m distance. They get state information of the neighbors for safety driving such as cooperative collusion avoidance and traffic route optimization through V2V or V2I applications, and communicate with remote ones by opportunistic routing. RSUs are deployed at regular intervals as infrastructure nodes. They are responsible for vehicles to access to the vehicular network, issuing pseudonyms for vehicles and forwarding messages between TA and them. As a vehicle moves into a new region, the RSU will make authentication. If it succeeds, the RSU will issue a set of pseudonyms and a broadcast key to the vehicle. It means that all vehicles in the same RSU region share a common broadcast key for security communication in MAC layer.

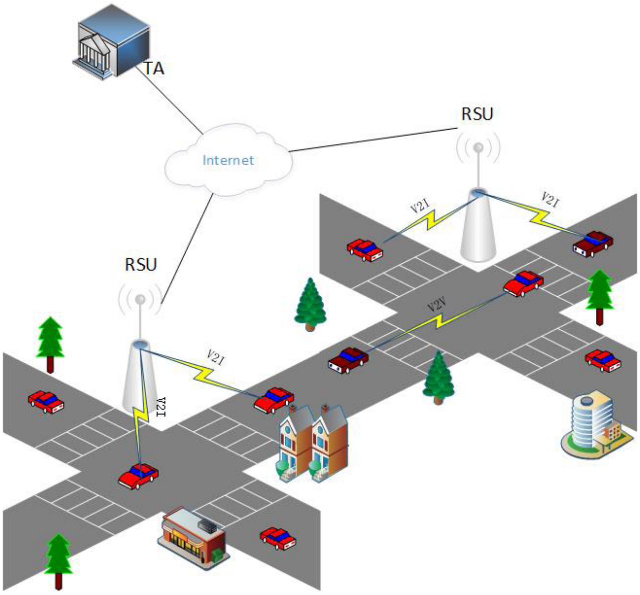


FIGURE 1. Vehicular network model.

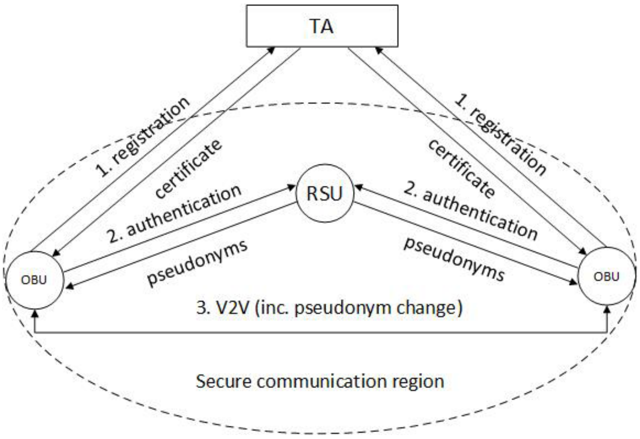


FIGURE 2. Vehicular networks trust model.

The main procedure to establish trust relationships among the entities is depicted as Fig. 2.

- Step 1. As a vehicle wants to register to a vehicular network, it must firstly contact TA and demonstrate the identity. The certificate is deterministically generated based on the identity.
- Step 2. When a vehicle moves into a region, it needs to enroll to the RSU by authentication. If succeed, the RSU will issue a set of pseudonyms to the vehicle for anonymous communication in the region.
- Step 3. The vehicles communicate with the neighbors periodically to get state information for safety driving

and opportunistic routing. Particularly, they will also participate in pseudonym change for location privacy.

1) REGISTRATION

Registration of a vehicle includes registration of the vehicle's license plate number, identity, and any other information needed to uniquely identify the vehicle. Since TA is assumed to be trusted, it is responsible for issuing the security parameters and keys. Precisely, TA issues certificates to vehicles. A certificate *cert* is the proof of a vehicle's public key PK_v which is associated with its identity *vid*. As depicted in **Certification Issuance** algorithm, the TA firstly generates a pair of public/private key, then signs PK_v under its private key SK_{TA} to generate a certificate *cert*.

```
Algorithm 1 Certification Issuance
Input: $vid$
Output: $PK_v, cert$
extract $SK_{TA}$
$(PK_v, SK_v) := KeyGen(vid)$
$cert := Sig.Sign(PK_v, SK_{TA})$
return $PK_v, cert$
```

2) AUTHENTICATION

As a vehicle moves into a region, the RSU will send a randomized message *msg* to it. The vehicle has to sign the message *msg* with the private key SK_v, i.e., $token := Sig.Sign(msg, SK_v)$. As depicted in **Pseudonym Issuance** algorithm, given a certificate *cert* and a presentation token *token*, the RSU verifies *cert* under TA's public key PK_{TA} and *token* under the vehicle's public key PK_v.

If succeed, the RSU will issue L pseudonyms to the vehicle. A pseudonym is defined as $(nym_i, t_i, c_i, ticket_i)$, where nym_i is a pseudorandom number serving as an identifier for a particular time period t_i, $ticket_i$ is a signature on the pseudonym, and c_i is used to trace misbehaving vehicles.

Here Nymble system [21] can be adjusted to unlinkable pseudonyms in our scheme. Precisely, the RSU sets $seed_0$ to a pseudorandom mapping of the vehicle's public key PK_v and the RSU's secret key $seedKey_{RSU}$. Tow cryptographic hash function f and g are used to compute pseudonyms from a particular seed. Without a seed, the sequence of pseudonyms appears unlinkable. To verify the integrity of the vehicle's public key PK_v, the RSU uses HMAC to output a message digest on it with the secret key $seedKey_{RSU}$. Then, the seed-evolution function f is used for linkability window and the seed for the next time period is computed from the seed for the current time period, i.e., $seed_i := f(seed_{i-1})$. The pseudonym nym_i for a time period t_i is evaluated by applying the pseudonym evaluation function g to its corresponding seed $seed_i$, i.e., $nym_i := g(seed_i)$. In particular, c_i contains the first pseudonym nym_0 in the user's sequence of pseudonyms. A vehicle or a sever may complaint to the RSU about a misbehaving vehicle by submitting c_i. The RSU decrypts c_i under $encKey_{RSU}$, then maps nym_0 to the corresponding PK_v, and even collaborate with the TA to retrieve the vehicle's identity.

```
Algorithm 2 Pseudonym Issuance
Input: $PK_v, cert, token, rid$
Output: $nyms$
extract $SK_{RSU}, seedKey_{RSU}, encKey_{RSU}, PK_{TA}$
if $Sig.Verify(cert, PK_{TA})$ and $Sig.Verify(token, PK_v)$ are valid then
    $seed_0 := f(HMAC(PK_v, seedKey_{RSU}))$
    $nym_0 := g(seed_0)$
    for $i$ from 1 to $L$ do
        $seed_i := f(seed_{i-1})$
        $nym_i := g(seed_i)$
        $c_i := Enc.Encrypt(nym_0, seed_i, encKey_{RSU})$
        $ticket_i := Sig.Sign(nym_i||t_i||c_i, SK_{RSU})$
    end for
    $nyms := \{(nym_i, t_i, c_i, ticket_i)\}$ where $i \in [1, L]$
    return $nyms, Enc.Encrypt(bcKey_R)$
end if
```

B. ATTACK MODEL

We assume an external global attacker in our scheme, which might be an untrustworthy LBS provider or an eavesdropper. It is able to trace and identify a vehicle via the location and the characteristics of it, e.g. IP and MAC address, or via disclosed pseudonym in applications. An external attacker has no TA-issued certificate, so it cannot fake legal vehicle to communicate in the region. As a global attacker, it monitors the traffic of IP packages all over the Internet, as well as collects identifying information (e.g., pseudonym) in local traffic of MAC frames in a RSU region. However, the attacker is not supposed to physically trace any target vehicle to determine the traffic flowing in and out. It means that an attacker cannot correlate any traffic to the target vehicle unless it is compromised.

Although the proposed scheme focuses on identification information protection in application layer, it can be also applied to the lower layers to facilitate MAC address changing. Thus, a whole-stack pseudonym changing scheme can be addressed to the location privacy issue in a stronger way. For similarity, the identification information related to MAC address is not concerned in this paper.

IV. INDEPENDENT MIX ZONE ESTABLISHMENT

In this section, we present a novel mix zone scheme to overcome lower density of vehicles or decentralization of the cooperative vehicles problem. The goal is to obtain the k-anonymity of pseudonym changing for a node without dependency on the number of cooperative nodes.

As a pseudonym is expired, the vehicle will change another one. All identifying properties of the layers in the protocol stack have to be preserved for location privacy.

Vehicular networks are expected to offer high degrees of mobility, the inherent properties of which make it possible for vehicles to be anonymous by constantly changing their IP and MAC addresses. However, pseudonym change will put the vehicle at the risk of location privacy leak in such case that there is not enough cooperative ones in the spatial-temporal context. As a result, the association of the old pseudonym and the new one will be determined with non-negligible advantage.

Suppose the number of vehicles whose pseudonyms are being expired around the same time is s, in such case that $s < k$, each of the vehicles will contribute to the k-anonymous pseudonym change in a collaborative fashion. Actually, it will generate $(k - s)/s$ notifications of pseudonym change to the neighbors. In the worst case that only one node is changing pseudonym, k-anonymity will also be obtained only by itself. It is where independent mix zone comes from. The main idea is to use randomization process and symmetric encryption scheme to generate $k - 1$ fake (randomized versions) pseudonyms along with a real one, which are indistinguishable with each other. From the view of attacker, these k notifications of pseudonym change are correctly distributed so that it cannot determine the actual vehicles who had cooperated together. Furthermore, the fake pseudonym acts as a redundant identifier instead of being used in V2V or V2I applications, where the vehicle can determine whether it is a real identifier or not.

The proposed scheme utilizes the beacon message to establish a mix zone, where the message type and time related to establishment, old and new pseudonyms encrypted by the group key are encapsulated in the beacon body. The advantages to take beacon message for mix zone is that it is inherently broadcasted in the RSU region; loading the extended data in beacon body is considered as trivial.

A. BEACON MESSAGE EXTENSION FOR MIX ZONE ESTABLISHMENT

Beacon messages are periodically broadcasted by vehicles to notify their existence to the neighbors and establish connection with RSUs. The beacon message contains the location, speed, driving direction, and other information of vehicles. It is transmitted every 100ms in the range of 300m [22]. The beacon message, defined in 802.11, consists of header, body, and frame check sequence (FCS). To adjust to mix zone establishment, it is extended with three values which are *type*, *time*, and a pair of pseudonyms including the old and the new one, i.e., (nym^{old}, nym^{new}), as Fig. 3 depicts. To establish a mix zone, *type* is to identify three kinds of beacon message defined as follows.

- $type = 01$, common beacon message
- $type = 00$, mix zone establishment message
- $type = 11$, notification message of pseudonym change

In the case that $type = 00$, the value *time* is to indicate the start time of mix zone, while it is ignored as $type = 01$ or $type = 11$. In the case that $type = 11$, there is a pair of the old pseudonym and the new one, i.e., (nym^{old}, nym^{new}), which is encrypted under the group key issued by the RSU. Such cryptography process conducted by the vehicles in the same RSU region produces a secure communication domain.

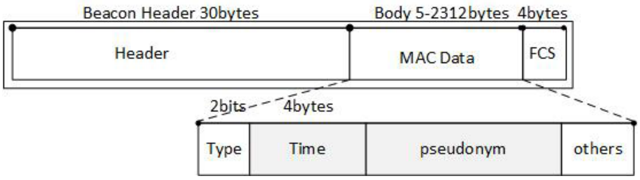


FIGURE 3. Extended beacon message.

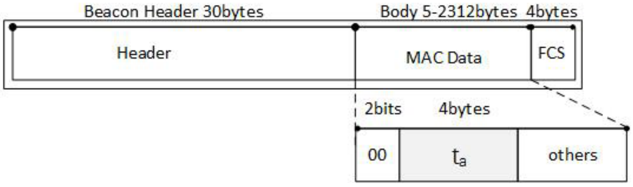


FIGURE 4. Mix zone request broadcast message.

B. MIX ZONE ESTABLISHMENT

The goal of the proposed scheme is to establish a mix zone which appears that a number of k vehicles change their pseudonyms simultaneously in the neighborhood. There may be less than k physical vehicles, but they collaborate to establish a k-anonymous mix zone by creating an independent mix zone respectively. In the worst case that there is only the target to change pseudonym, it can also establish a k-anonymous mix zone without any collaboration of others.

Suppose the number of collaborative vehicles including the target is s where $s < k$, each of them broadcasts to the neighbors $(k - s)/s$ notifications of pseudonym change. As a result, a mix zone is established with k indistinguishable new pseudonyms cooperated by s physical vehicles. The attacker will lose to locate the target in the mix zone. Furthermore, the proposed scheme moves forward to V2V or V2I applications. Any vehicle receiving notifications of pseudonym change from neighbors retrieves the real pseudonym for only once.

1) COLLABORATIVE PROCESS

Suppose the pseudonym of the vehicle v_a is about to be expired, it firstly produces a mix zone request broadcast message with $type = 00$ and $time = t_a$, as depicted in Fig. 4. Then it collects other mix zone request messages in the neighborhood. Let τ be the number of vehicles that broadcast mix zone request messages, the vehicle v_a finally produces a notification broadcast message to the neighbors with a new pseudonym nym_a^{new}.

After collecting the collaborative vehicles, each of them selects a new pseudonym from pseudonym pool in the session layer on time t_a, which will be retrieved from the session header in MAC layer.

Algorithm 3 MixZoneReq

```
Input: $t_a, \epsilon$
Output: mix zone request broadcast message $broadcastMsg_{req}, \tau$
$\tau \leftarrow 1$
$broadcastMsg_{req} := (type = 00, time = t_a)$
generate a beacon message on $broadcastMsg_{req}$ and broadcast it to the neighbors
repeat read each of the received beacon message $broadcastMsg_{req_i}$
    if $type_i = 00$ and $|time_i - t_a| \leq \epsilon$ then
        $\tau{+}{+}$
    end if
until $T > t_a$
```

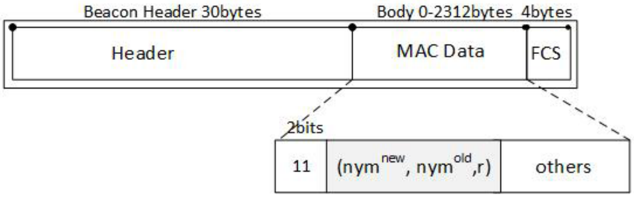


FIGURE 5. Notification of Pseudonym change if $\tau \geq k$.

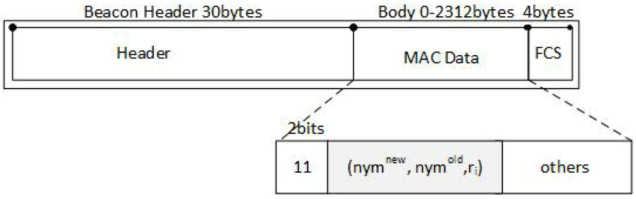


FIGURE 6. Notification of Pseudonym change if $\tau < k$.

2) INDEPENDENT PROCESS

To the given number of the collaborative vehicles collected in **MixZoneEST** algorithm, i.e., τ. In the case that $\tau \geq k$, v_a directly generates the notification message as depicted in Fig. 5, where $type = 11$ and the pair of pseudonyms $(nym_a^{new}, nym_a^{old})$ are encrypted under the group key.

In the case that $\tau < k$, each of the collaborative vehicles will contribute to k-anonymous pseudonym change by generating k/τ redundant notifications, which seems like k/τ fake vehicles from the view of the neighbors. For example, the vehicle v_a picks k/τ random values $r_i \in N^*$, $i \in [0, k/\tau]$. Then it generates k/τ notification messages as depicted in Fig. 6, where the related values *type*, *time*, and k/τ pairs of pseudonyms $\{(nym_a^{new}, nym_a^{old}, r_i)\}$ are encrypted under the group key. Finally, v_a broadcasts the k/τ notification messages to the neighbors one by one, which are indistinguishable with each other due to randomization of pseudonym pairs.

For any vehicle that receives the notification message, it firstly retrieves the values nym_a^{new} and nym_a^{old} under the group key. If nym_a^{new} has already been received, the message is discarded. Otherwise, it gives nym_a^{new} and nym_a^{old} to the session layer.

Algorithm 4 NymChangeNotify

```
Input: $nym_a^{old}, nym_a^{new}, k, \tau, bcKey_R, t_a$
Output: pseudonym change notification broadcast message $broadcastMsg_{notify}$
if $\tau \geq k$ then
    select a random number $r \in N^*$ and encrypt the pair of pseudonyms, i.e., $[nym_a^{new}, nym_a^{old}, r] := Enc.Encrypt(nym_a^{new} || nym_a^{old} || r, bcKey_R)$
    generate a beacon message on $broadcastMsg_{notify}$, where $broadcastMsg_{notify} \leftarrow (type = 11, [nym_a^{new}, nym_a^{old}, r])$ and broadcast it to neighbors
else
    select random numbers $r_i \in N^*$ and $i \in [0, k/\tau]$
    for $i = 0 \rightarrow k/\tau$ do
        encrypt the pair of pseudonyms, i.e., $[nym_a^{new}, nym_a^{old}, r_i] := Enc.Encrypt(nym_a^{new} || nym_a^{old} || r_i, bcKey_R)$
        generate a beacon message on $broadcastMsg_{notify_i}$, where $broadcastMsg_{notify} := (type = 11, [nym_a^{new}, nym_a^{old}, r])$ and broadcast it to neighbors
    end for
end if
```

Algorithm 5 NotifyHandler

```
Input: pseudonym change notification broadcast message $broadcastMsg_{notify}$
Output: $nym_a^{new}, nym_a^{old}$
retrieve the related values from $broadcastMsg_{notify}$, i.e., $(nym_a^{new}, nym_a^{old}, r) := Enc.Decrypt([nym_a^{new}, nym_a^{old}, r], bcKey_R)$
if $nym_a^{new}$ has been cached then
    terminate
else
    give $(nym_a^{new}, nym_a^{old})$ to the session layer
end if
```

After authenticating nym_a^{new} and nym_a^{old} under the public key of RSU, the receiving vehicle will establish a new session with nym_a^{new} and terminate the old one with nym_a^{old}.

C. V2V APPLICATION SCENARIO

Once the new session is connected with the new pseudonym, the vehicle will communicate with the neighbors in V2V applications. The state-of-the-art of mix zone schemes have not addressed for application scenarios, however, k-anonymous pseudonym change will be compromised if the actual number of vehicles participating in V2V communications with new pseudonyms is less than k. Suppose v_a sends a message to v_b, it retrieves nym_a^{new} as the sender pseudonym and nym_b^{new} as the receiver pseudonym. Then it generates

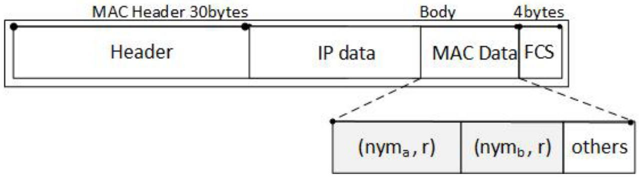


FIGURE 7. V2V application scenario.

a pair of randomized sender and receiver pseudonyms encrypted under the group key, i.e., $[nym_a^{new}, r]_{bcKey_R}$ and $[nym_b^{new}, r]_{bcKey_R}$ respectively in MAC layer, where $r \in N^*$, as Fig. 7 depicts.

For any vehicle that receives the message, it retrieves the receiver pseudonym nym_b^{new} under the group key. If it is the actual receiver, the sender pseudonym nym_a^{new} will be also retrieved, and then given to the upper layer.

V. PRIVACY AND PERFORMANCE ANALYSIS

The proposed indMZ scheme gives an upper bound complexity of mix zone establishment, the worst case of which is none of vehicles collaborates with the target vehicle, i.e., $\tau = 1$. A k-anonymous independent mix zone is established all by the target vehicle itself with the number of k extended beacon message, i.e., $broadcastMsg_{notify}$, as tradeoff. The neighbors of the target vehicle need to deal with each of the extended beacon message $broadcastMsg_{notify}$. Precisely, each of them will run decryption algorithm to retrieve (nym^{old}, nym^{new}) for k times.

Compared with other mix zone schemes, the proposed indMZ scheme encapsulates mix zone request and notification of pseudonym change both in beacon message. The inherent periodically-broadcasting feature of beacon message facilitates k-anonymous mix zone establishment without extra decapsulation of other structured messages.

The target vehicle just needs to select random numbers with the new pseudonym to simulate collaborative vehicles, without any waste of precious pseudonym or dependency on any trusted third party.

A. LOCATION PRIVACY ANALYSIS

Concerned about k-anonymous mix zone for location privacy, we compare the proposed indMZ scheme with MPSVLP [18] and AVATAR [19]. Location privacy is the degree of confusion vehicles changing pseudonyms. Due to the low density of vehicles and the possible existence of selfish vehicles, there may be not enough vehicles that want to change pseudonyms. MPSVLP scheme uses reputation model to motivate selfish vehicles to cooperate, but it cannot definitely solve the problem of low density vehicles. The target vehicle cannot assure a privacy-preserving mix zone. In AVATAR scheme, the vehicle enlarges request region to seek cooperation with vehicles in the distance. It also uses footprint signatures to construct virtual vehicles to achieve the desired location privacy. Instead, the indMZ scheme allows the vehicle to produce a k-anonymous mix zone totally by itself, no matter if there is a collaborative vehicle or not.

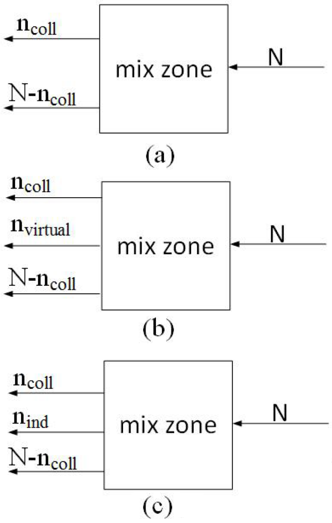


FIGURE 8. Comparison on mix zone establishment schemes. (a) MPSVLP: $n_{coll} = k < N$. (b) AVATAR: $n_{coll} + n_{virtual} = k$. (c) indMZ: $n_{ind} + n_{coll} = k$.

Suppose a vehicle establishes a mix zone, the radius of which is 300m and the total number of vehicles in which is N, and the number of collaborative vehicles participating in the mix zone is n_{coll}. We just analyze the worse case that $n_{coll} < k$ due to low density of vehicles, as depicted in Fig. 8.

In MPSVLP scheme, vehicles decide whether cooperate or not according to the vehicle's reputation and its own reputation. The reputation mechanism will motivate the vehicles to collaborate, however, when the total number of vehicles in the region is less than k, i.e., $N < k$, the mix zone cannot be motivated. In AVATAR scheme, suppose the request vehicle collects n_{coll} collaborators in the region, it will keep expanding the search range to establishes a virtual mix zone with the number of $n_{virtual}$ collaborators until $n_{coll} + n_{virtual} = k$; while in the proposed indMZ scheme, each of the collaborative vehicles will produce $(k - n_{coll})/n_{coll}$ randomized versions of the new pseudonym respectively, i.e. the total number of them n_{ind} equal to $k - n_{coll}$.

In summary, to establish a k-anonymous mix zone, MPSVLP needs to deploy control servers to help the vehicle to broadcast request messages to search collaborators, AVATAR relies on vehicles farther away, while indMZ needs the smallest collaborators (even zero) and communication cost to achieve the same level of location privacy.

Suppose an attacker trace the target vehicle v_a in the current pseudonym nym_a^{old}. When it is about to be expired, the target vehicle sends the request message $broadcastMsg_{req}$ to the neighbors. As depicted in Fig. 9(a), suppose there are s collaborative vehicles, where $s < k$. Considering the mix zone established by the indMZ scheme, each of the collaborative vehicles produces $(k - s)/s$ notify messages $broadcastMsg_{notify}$ to contribute to the mix zone,

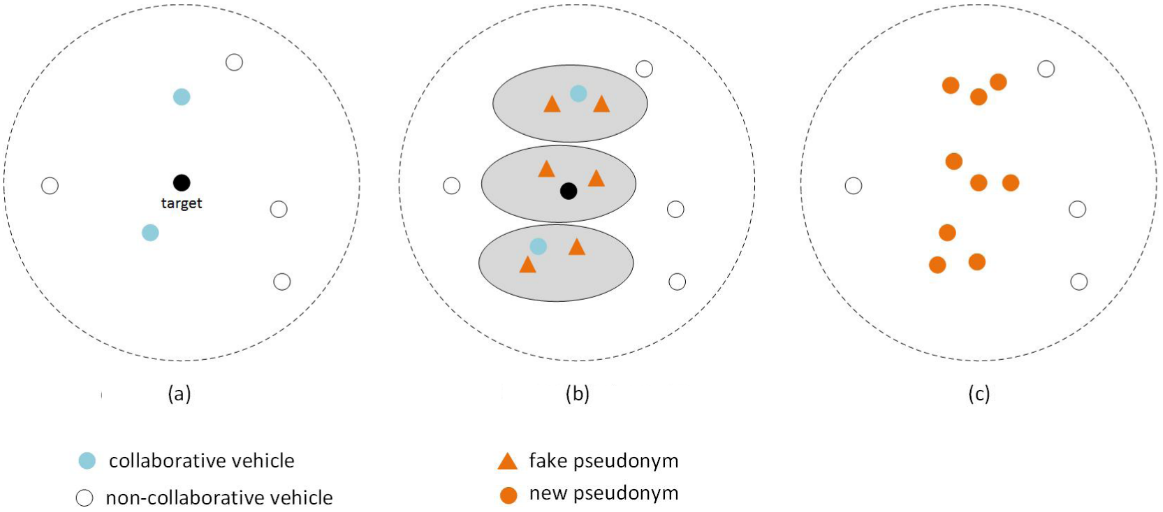


FIGURE 9. **Location privacy analysis. (a) Collaborative process. (b) Independent process. (c) Indistinguishable *K* pseudonym changes.**

as depicted in Fig. 9(b). As a result, the view of an attacker is depicted in Fig. 9(c) where there are k indistinguishable new pseudonyms in the region. The advantage for the attacker to determine the target vehicle from k indistinguishable new pseudonyms is $1/k$.

B. PERFORMANCE ANALYSIS

Assume that the length of the broadcast message in three schemes is the same, we consider the total times of sending and receiving broadcast messages by a vehicle.

In MPSVLP scheme, control servers need to be deployed in vehicular networks to assist vehicles in mix zone establishment, where the vehicle sends the encrypted request and the control server broadcasts it according to the expected location privacy. If other vehicles want to cooperate, they will response to the control server and change their pseudonyms. Such dependency on control server mitigates broadcast cost among vehicles but still needs two times of broadcast by the control server; at the meanwhile, it also increases communication cost between vehicles and the control server.

In AVATAR scheme, the vehicle broadcasts the request message by itself. It may enlarge the broadcast region and resend request message due to low density of vehicles. Let the times of resending be k' which is uncertain until the vehicle collects k collaborators. The vehicles that want to collaborate will generate several footprint signatures and send them to the request vehicle which then sends the footprint signatures to all collaborators as rewards for their cooperation. Therefore, the broadcasting of message is at least $(1 + k)$ and at most $k' + k$, as depicted in Table 2.

In indMZ, the vehicle encapsulates the request in beacon message, which is inherently broadcasted periodically in the region. After pseudonym change, the vehicle encrypts new pseudonym and its randomized versions. Moreover, the vehicle broadcasts *broadcastMsg*$_{notify}$ to notify pseudonym change to the neighbors. The total number of broadcast messages to deal with is at least one and at most $(1 + k)$.

TABLE 2. **Performance analysis.**

	Broadcast cost of worst case, best case	Crypto. cost	TTP-dependent
MPSVLP	$0, 0$	encryption	√
AVATAR	$k' + k, 1 + k$	signature, encryption	×
indMZ	$1 + k, 1$	encryption	×

VI. CONCLUSION

To solve the pseudonym change problem in the low density of vehicles, an independent mix zone scheme *indMZ* is proposed in the paper. It specifies a pseudonym scheme for vehicular networks. Each vehicle will have L pseudonyms when it enrolls to a RSU. As a pseudonym is about to be expired, the vehicle can establish an independent mix zone which means that the vehicle can still establish a k anonymous pseudonym change region even if the number of collaborative ones is less than k; in the worst case it will establish a mix zone all by itself. Beacon message is adopted to carry the related information of pseudonym change, which are inherently broadcasted in neighborhood periodically. We evaluate indMZ and other mix zone schemes with respective to performance and location privacy strength in the low density of vehicular networks. It shows that to ensure a k anonymous pseudonym change region, the proposed indMZ scheme takes the average $k/2$ broadcast cost without rely on any other trusted third party. Our future work is to consider authentication after pseudonym change and revocation of pseudonym if the vehicle is complained.

REFERENCES

[1] Y. Qi *et al.*, "5G over-the-air measurement challenges: Overview," *IEEE Trans. Electromagn. Compat.*, vol. 59, no. 6, pp. 1661–1670, Dec. 2017.

[2] I. F. Akyildiz, S. Nie, S.-C. Lin, and M. Chandrasekaran, "5G roadmap: 10 key enabling technologies," *Comput. Netw.*, vol. 106, pp. 17–48, Sep. 2016.

[3] R. Gopi and A. Rajesh, "Securing video cloud storage by ERBAC mechanisms in 5G enabled vehicular networks," *Cluster Comput.*, vol. 20, no. 4, pp. 3489–3497, 2017.

[4] H. E. Ming-Xing, W. Zhu, L. I. Xiao, D. W. Luo, and J. X. Zhao, "Privacy-preserving authentication protocols in vehicular ad hoc networks," *J. Xihua Univ.*, vol. 31, no. 4, pp. V1-437–V1-442, 2012.

[5] T. Yang, L. B. Kong, and J. B. Hu, "Survey on vehicular networks privacy protecting," *J. Comput. Res. Develop.*, vol. 54, pp. 178–185, 2012.

[6] R. G/ Engoulou, M. Bellaïche, and S. Pierre, "Vehicular network security surveys," *Comput. Commun.*, vol. 44, no. 5, pp. 1–13, 2014.

[7] A. K. Tyagi and N. Sreenath, "Location privacy preserving techniques for location based services over road networks," in *Proc. Int. Conf. Commun. Signal Process.*, 2015, pp. 1319–1326.

[8] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," *IEEE Trans. Mobile Comput.*, vol. 7, no. 1, pp. 1–18, Jan. 2008.

[9] F. Sebé-Feixas, "Privacy in vehicular networks and location-based services," *URV Chairs—Summer Courses*. Span, Jun. 2007.

[10] C. Caballero-Gil, J. Molina-Gil, J. Hernández-Serrano, O. León, and M. Soriano-Ibanez, "Providing k-anonymity and revocation in ubiquitous VANETs," *Ad Hoc Netw.*, vol. 36, no. P2, pp. 482–494, 2015.

[11] A. Solanas and A. Martínez-Ballesté, "Privacy protection in location-based services through a public-key privacy homomorphism," in *Public Key Infrastructure*, Berlin, Germany: Springer, vol. 4582. 2007, pp. 362–368.

[12] A. Solanas and A. Martínez-Ballesté, "A TTP-free protocol for location privacy in location-based services," *Comput. Commun.*, vol. 31, no. 6, pp. 1181–1191, 2008.

[13] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Comput.*, vol. 2, no. 1, pp. 46–55, Jan./Mar. 2003.

[14] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *Proc. IEEE Wireless Commun. Netw. Conf.*, vol. 2. Mar. 2005, pp. 1187–1192.

[15] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "SLOW: A Practical pseudonym changing scheme for location privacy in VANETs," in *Proc. Veh. Netw. Conf. (VNC)*, Oct. 2009, pp. 1–8.

[16] J.-H. Song, V. W. S. Wong, and V. C. M. Leung, "Wireless location privacy protection in vehicular ad-hoc networks," *Mobile Netw. Appl.*, vol. 15, no. 1, pp. 160–171, 2010.

[17] B. Palanisamy and L. Liu, "MobiMix: Protecting location privacy with mix-zones over road networks," in *Proc. IEEE Int. Conf. Data Eng.*, Apr. 2011, pp. 494–505.

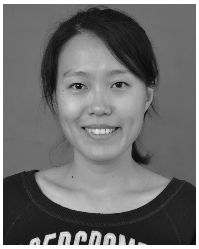
[18] B. Ying, D. Makrakis, and Z. Hou, "Motivation for protecting selfish vehicles' location privacy in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 12, pp. 5631–5641, Dec. 2015.

[19] S. Du, H. Zhu, X. Li, K. Ota, and M. Dong, "MixZone in motion: Achieving dynamically cooperative location privacy protection in delay-tolerant networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 9, pp. 4565–4575, Nov. 2013.

[20] G. Nan, M. Linya, and G. Tihan, "A location privacy-preserving scheme for vehicular networks based on virtual mix zone," in *Proc. Res. Briefs Inf. Commun. Technol. Evol. (ReBICTE)*, vol. 3. 2017, Art. no. 10.

[21] P. P. Tsang, A. Kapadia, C. Cornelius, and S. W. Smith, "Nymble: Blocking misbehaving users in anonymizing networks," *IEEE Trans. Depend. Sec. Comput.*, vol. 8, no. 2, pp. 256–269, Mar./Apr. 2011.

[22] P. Papadimitratos *et al.*, "Secure vehicular communication systems: Design and architecture," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.



NAN GUO received the B.E. degree in computer science and technology, and the M.E. and Ph.D. degrees in computer application technology from Northeastern University, China, in 1999, 2001, and 2005, respectively. She joined Northeastern University in 2005, where she has been an Associate Professor since 2008. She was a Visiting Scholar with the Department of Computer Science, Purdue University, USA, from 2010 to 2011. Her research interests include security and privacy in vehicular network and social network, and digital identity management.

LINYA MA received the B.E. degree from the Software College, Northeastern University, in 2016. She is currently pursuing the master's degree with the Graduate School, Software College, Northeastern University. Her research interests include wireless mesh network security, vehicular networks security, and vehicular networks privacy.

TIANHAN GAO received the B.E. degree in computer science and technology, and the M.E. and Ph.D. degrees in computer application technology from Northeastern University, China, in 1999, 2001, and 2006, respectively. He joined the Software College, Northeastern University, in 2006, as a Lecturer, where he received an early promotion to an Associate Professor in 2010. He was a Visiting Scholar with the Department of Computer Science, Purdue University, from 2011 to 2012. He received the doctoral tutor qualification in 2016. He has authored or co-authored of over 50 research publications. His primary research interests include next-generation network security, wireless mesh network security, security and privacy in ubiquitous computing, and virtual reality.