A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks

Abdelwahab Boualouache, Sidi-Mohammed Senouci, and Samira Moussaoui

***Abstract*—The initial phase of the deployment of vehicular ad-hoc networks (VANETs) has begun and many research challenges still need to be addressed. Location privacy continues to be in the top of these challenges. Indeed, both academia and industry agreed to apply the pseudonym changing approach as a solution to protect the location privacy of VANETs' users. However, due to the pseudonyms linking attack, a simple changing of pseudonym shown to be inefficient to provide the required protection. For this reason, many pseudonym changing strategies have been suggested to provide an effective pseudonym changing. Unfortunately, the development of an effective pseudonym changing strategy for VANETs is still an open issue. In this paper, we present a comprehensive survey and classification of pseudonym changing strategies. We then discuss and compare them with respect to some relevant criteria. Finally, we highlight some current researches, and open issues and give some future directions.**

***Index Terms*—VANETs, security, location privacy, pseudonym changing.**

I. Introduction

OVER the last decade, Vehicular Ad-Hoc Networks (VANETs) have attracted a lot of interest from both the research community and the automotive industry due to their huge impact on Intelligent Transportation Systems (ITS) [1]. This technology is primarily developed to enhance road safety and provide traffic efficiency. VANETs allow vehicles not only to communicate between them Vehicle-to-Vehicle (V2V), but also with a roadside infrastructure Vehicle-to-Infrastructure (V2I), which enables a variety of interesting applications. These applications can be ranging from safety-related applications, such as collision warning and emergency reporting to non-safety applications like infotainment [2]. Safety-related applications are usually based on beaconing, i.e., the process of periodically broadcasting safety messages. These latter are called Cooperative Awareness Messages (CAMs) in Europe and Basic Safety Messages (BSM) in U.S. [3] and they are broadcast over the DSRC control channel (CCH) with a high frequency ranging from 1 to 10 Hz as suggested by standardization bodies such as IEEE, ETSI, and SAE [4]. Safety messages include sensitive information about the current state of vehicles such as their identifiers, positions, and velocities. The encryption of these messages is not recommended since many VANETs' participants are concerned by them [5]. In addition, decrypting safety messages can add a latency in the processing of them, which may not meet with real-time requirements of safety-related applications [6]. However, due to security threats such as false data injections, disseminated messages modifications, and replay attacks, safety messages must be authenticated.

The aim of safety messages is to make vehicles aware about their surrounding environment, which significantly improves road safety. For example, using these messages, vehicles can expect or detect dangerous situations that can cause serious damages on VANETs such as collisions and accidents. As a result, vehicles can then make decisions to prevent such bad consequences. However, although, safety messages are beneficial for road safety, they may also be exploited by adversaries for unauthorized location tracking of vehicles [7]. Indeed, due to the nature of the wireless medium, a passive adversary can easily eavesdrop all the broadcasted safety messages within its region of interest. It can then collect these safety messages and determine the locations visited by vehicles over time. The location tracking of vehicles could violate drivers privacy since one vehicle is usually associated only with one driver [8]. Therefore, knowing vehicle's position can lead to disclosure critical information about driver's life. For example, having information about of the frequency of driver's visits to a given hospital may raise doubts of the employer about the driver's health [9]. Furthermore, the driver's life can be put at risk if the adversary is a criminal. Protecting the location privacy is thus crucial because the lack of the protection may disturb the deployment of VANET technology.

Several privacy requirements for VANETs are identified in the literature (discussed in Section II-B1). The anonymity is one of the main privacy requirements. It ensures that safety messages are authenticated without attaching the real senders' identifiers. The anonymity is however contracted with the accountability security service, which aims to ensure that the authorities are always able to identify vehicles in case of a misbehaving behavior. Therefore, the privacy in VANETs must be conditional, where vehicles are anonymous to all VANETs' participants except the authorities, which must still track them.

In order to meet these requirements, many anonymous authentication schemes have been proposed. These schemes can generally be divided into three categories [10]: (i) the group-signature-based schemes (e.g., [11]), (ii) pseudonymous authentication schemes (e.g., [12]), and finally (iii) hybrid

Manuscript received January 28, 2017; revised August 11, 2017; accepted October 29, 2017. Date of publication November 8, 2017; date of current version February 26, 2018. *(Corresponding author: Abdelwahab Boualouache.)*

A. Boualouache and S. Moussaoui are with the Department of Computer Science, RIIMA Laboratory, USTHB University, Algiers 16111, Algeria (e-mail: webwahab@gmail.com).

S.-M. Senouci is with DRIVE EA1859, University of Burgundy–Franche-Comté, F58000 Nevers, France.

Digital Object Identifier 10.1109/COMST.2017.2771522

schemes (e.g., [13]). However, both of academia and industry have adopted a pseudonymous authentication scheme to be implemented in the future deployment of VANETs [14]. Indeed, the current security standards IEEE 1609.2 standard [15] and ETSI 102941-v1.1.1 [16] are based on a traditional public infrastructure (PKI). The pseudonyms represent a set of certified public keys (anonymous certificates) stored in the vehicle's On-Board Unit (OBU) [12]. Instead of using one identifier (public key) all the time, a vehicle periodically changes its pseudonym to mitigate the tracking of its positions. Moreover, the change of pseudonym should be accompanied by the change of all the identifiers of communication stack layers such as the MAC and the IP addresses [17]. The pseudonym can then be seen as a fictive vehicle's identifier, where only the authorities can resolve it, i.e., finding the relationship between a given pseudonym and the corresponding real identifier of the vehicle. The location privacy protection using the *pseudonym changing approach* mainly depends on two factors: (i) the frequency of pseudonyms changing, i.e., the higher frequency of pseudonym changing is, the more level of location privacy protection is obtained. However, knowing that the pseudonyms are the identifiers that are used in the inter-vehicular communications, the changing of pseudonyms with a high frequency will certainly has negative effects on the communication performances. Indeed, Schoch *et al.* [18] demonstrated that a high level of packet loss is engendered when incorporating a geographic routing protocol with the changing of pseudonyms (frequency less than 30s), and (ii) the *unlinkability between pseudonyms*, which means that two pseudonyms belong to the same vehicle should not be linked to each other.

Unfortunately, several conducted works to study the efficiency of the pseudonym changing approach (discussed in Section II-D) demonstrated that a simple changing of pseudonym is ineffective to provide the required level of location privacy protection for the VANETs' users. This is due to the pseudonyms linking attack. Indeed, there are two types of pseudonyms linking attack (presented in Section II-E): the syntactic linking and the semantic linking. Many pseudonym changing strategies have been suggested to provide protection against this attack. The aim of a pseudonym changing strategy is to determine where, when, and how vehicles should change their pseudonyms to provide the unlinkablity between them. However, although, the variety of existing the pseudonym changing strategies, there is no strategy suggested by standardization bodies until now [19].

A. Relevant Surveys

Several surveys have been conducted on security and privacy in vehicular networks. Hamida *et al.* [20] reviewed, analyzed, and classified different known attacks and highlighted their security and privacy requirements that should meet for VANETs. Engoulou *et al.* [21] explored recent proposed vehicular security architectures and standardized protocols. Mejri *et al.* [22] studied and compared different suggested cryptographic schemes and evaluated their efficiency. Qu *et al.* [10] highlighted the tradeoff between privacy and security, and discussed and classified different proposed anonymous authentication schemes into three categories including the pseudonym changing approach. Petit *et al.* [23] presented a detailed survey on existing pseudonymous authentication schemes. They compared and classified different existing schemes and identified some open issues. Wagner and Eckhoff [24] gave an interesting systematic survey of technical privacy metrics. They also classified them according to the measured privacy aspect into eight categories. Wagner and Eckhoff [25], identified the privacy metrics usually used to evaluate privacy protection mechanisms for vehicular networks. The pseudonym changing strategy is among the issues of identified in [23]. Indeed, Petit *et al.* [23] gave a general overview of some pseudonym changing strategies and pointed out the absence of a comparison between them. Thus, to complement these efforts and in contrast to [23], this paper particularly presents a comprehensive survey of existing pseudonym changing strategies for VANETs. The paper deeply compares and analyzes these strategies to identify the strengths and weaknesses of each strategy. To the best of our knowledge, we are the first to propose such survey. We hope that this survey will help to take a decision of which strategy should be applied in the future deployment of VANETs and potentially propose new strategies.

B. Contributions

The main contributions of this paper can be summarized as follows:

- We survey and elaborate a taxonomy of pseudonym changing strategies for VANETs.
- We discuss, analyze, and compare the presented strategies.
- We present lessons learned and recommendations for deploying pseudonyms changing strategies.
- We highlight some open challenges on the pseudonym changing strategy issue.

The rest of the paper is organized as follows. In Section II, we present some necessary background information. A taxonomy of pseudonym changing strategies is presented in Section III. In Sections IV, we discuss, classify and compare the presented strategies. Lessons learned and recommendations are discussed in Section V. Some research challenges are given in Section VI. Finally, Section VII concludes this survey.

II. Background

The purpose of this section is to give the reader the necessary background information to understand the research presented in this paper. Abbreviations used throughout the paper are described in Table I.

A. Vehicular Networks

Vehicular Ad-hoc Networks (VANETs) are considered as a form of mobile ad hoc networks (MANETs) that use wireless communication technologies to connect vehicles either to each other or to fixed infrastructure nodes that are installed alongside the road. Thus, VANETs provide along the road: (i) inter-vehicular communications for intelligent vehicles, and

TABLE I
ABBREVIATIONS USED THROUGHOUT THE PAPER

AS	Anonymity Set
ASR	Adversary's Success Rate
ASS	Anonymity Set Size
CA	Certificate Authority
CCL	Candidate Location List
CGA	Cryptographically Generated Address
CMIX	Cryptographic MIX-zones
CPN	Cooperative PseudoNym
CRL	CertiiňĄcate Revocation List
CS	Control Server
CSMA	Carrier-Sense Multiple Access
DA	Degree of Anonymity
DLP	Density-based Location Privacy
DMLP	Dynamic Mix-Zone for Location Privacy
DSRC	Dedicated Short Range Communications
ECC	Electronic Communications Committee
EDCA	Enhanced Distributed Channel Access
FCC	Federal Communications Commission
GPK	Group Public Key
GS	Group Signatures
HPDM	Hybrid Pseudonyms Distribution Method
ICA	Intersection Collision Avoidance
ITS	Intelligent Transportation System
MANET	Mobile Ad-hoc NETwork
MHT	Multi-Hypotheses Tracking
MTT	Maximum Tracking Time
NNPDA	Nearest Neighbor Probabilistic Data Association
PCC	Pseudonym Changes based on Candidate-Candidate-location-list
PCS	Pseudonym Changing Strategy
PKI	Public Key Infrastructure
PPV	Pseudonym Provider Vehicle
PREXT	PRivacy EXTension for Veins VANET Simulation
REP	Random Encryption Period
RNP	Request New Pseudonym
RSU	Road-Side Unit
SAE	School of Audio Engineering
SLOW	Silence at Low Speeds
SM	Silent Mix zone
SPCP	Synchronized Pseudonym Changing Protocol
Statistics	Statistics on Pseudonym Changes
TA	Trusted Authority
TAPCS	Traffic-Aware Pseudonym Changing Strategy
TGM	Trusted Group Manager
UPCS	Urban Pseudonym Changing Strategy
VANET	Vehicular Ad-hoc NETwork
VLPZ	Vehicular Location Privacy Zone
WAVE	Wireless Access for Vehicular Environment
WSA	WAVE Service Advertisement
WSM	WAVE Short Message
WSMP	WAVE Short Message Protocol

(ii) a connectivity to other networks via road infrastructure gateways.

1) Architecture: VANETs consist of a set of communicating entities organized according to a communication architecture. They include two types of communicating entities: vehicles and roadside entities. Figure 1 shows an example of VANETs involving various communicating entities. Modern vehicles are equipped with a variety of sensors connected to a central computing platform that has both wired and wireless interfaces. The intelligent vehicles are those vehicles that are equipped with OBU. This unit can record, calculate, locate, and send messages over a network interface. On the other hand, roadside entities are called Road Side Units (RSUs). These entities can broadcast notifications to inform the nearby vehicles about, for example, traffic and weather conditions or specific road information such as maximum speed limits and an overtaking authorization. RSUs can also play the role of base stations relaying information sent by vehicles.

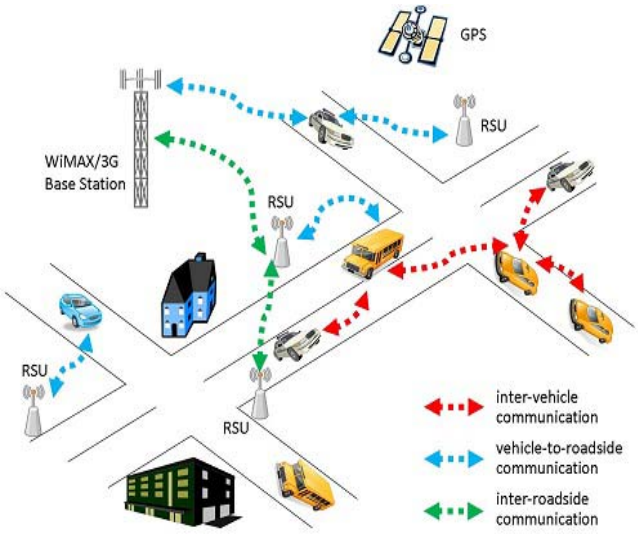

Fig. 1. An example of VANETs [26].

Application and services offered by VANETs use different types of communication:

- *Communication Vehicle-to-Infrastructure (V2I):* This type of communication involves RSUs to which vehicles access for safety, traffic management, and infotainment applications. RSUs are administered by one or more government organizations or by motorway operators. A vehicle that informs the department of roads about an obstacle is considered as an example of V2I communication.
- *Communication Vehicle-to-Vehicle (V2V):* This type of communication involves vehicles only. These then form a wireless network without the need of a centralized coordination entity. This type of communication is plausible and important if some RSUs become unavailable (down or out of the range). In this case, the network should continue to function. Vehicles must then work together to ensure the availability of V2V services. V2V communications can also be used in alert dissemination scenarios like collisions or for cooperative driving.
- *Hybrid:* The combination of the two first types of communication provides an interesting hybrid architecture. Indeed, given that the coverage of the infrastructure is limited, the use of vehicles as relays can help to extend the coverage. In addition, for an economic purpose

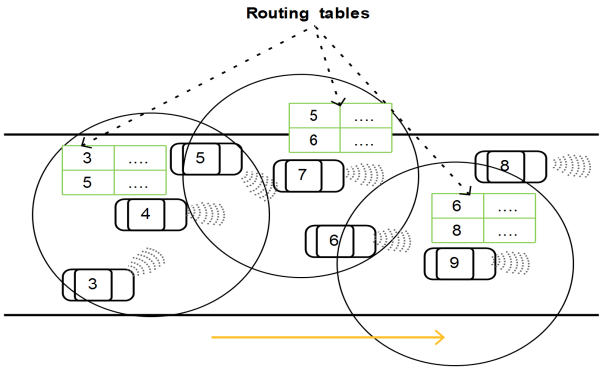

Fig. 2. Building routing tables from safety messages.

using vehicles can reduce the deployment of huge number of RSUs. However, inter-vehicular communications may suffer from routing problems during transmission over long distances. In such situations, the access to the infrastructure can improve the network performances. We can thus notice the complementarity of the two types of communication and the importance of a hybrid architecture.

On the other hand, VANET entities can generate and exchange messages. Indeed, according to the application type and the context, vehicles can send or receive a safety message, an alert message or another type of message.

- *Safety message:* A safety message is generated at regular intervals. Conventionally, each vehicle broadcasts a safety message every 100 ms to 1s. This message, also called beacon, contains the position, the speed, and the direction of the broadcasting vehicle. Thanks to these safety messages, each vehicle can create a local view of its neighborhood. It can also predict and anticipate dangerous situations or traffic congestion. These messages are also used for building routing tables that allow an efficient information dissemination between vehicles as illustrated in Figure 2.
- *Alert message:* An alert message is generated when an event is detected. This may be the detection of an accident, an obstacle or receiving another alert message. The alert must then be transmitted at regular intervals in order to ensure its sustainability. Thus, vehicles that are designated for the retransmission of the alert message will rebroadcast it at regular intervals. In addition, the alert message must have a reduced size in order to be broadcast as quickly as possible. Alert messages particularly include details about the event and parameters of the broadcast area.
- *Other messages:* This type of message contains all the messages that are neither safety nor alert messages. These messages are generally not repeated at regular intervals such as financial transaction messages or E-mails.

2) Applications: VANETs are characterized by a variety of promising applications and services. Several technical reports established by standards bodies and industrial consortiums list dozens of applications that will eventually be deployed in the future. We can distinguish three classes of applications: safety-related, traffic-related, and infotainment. These classes are described as follows:

- *Safety-Related Applications:* The decrease in the number of people injured or killed on the roads is one of the main motivations for the development and the study of VANETs. This category contains all the applications that aim to improve road safety. These applications are then intended to improve the vision field of the driver offering a driving aid to it. The driver can thus anticipate and react to make the driving experience more safer. For example, it can be informed that a vehicle has violated the red traffic light or a pedestrian is crossing the road.
- *Traffic-Related Applications:* This category includes applications that use inter-vehicular communications to share traffic information between vehicles in order to enhance the driver experience and optimize the traffic flow. Different scenarios can be envisaged for this category like the cooperation between vehicles to facilitate the passage of emergency vehicles.
- *Infotainment Applications:* This category includes all applications that provide drivers with information, entertainment and advertisements during their journey such as custom information services, Internet access, and video streaming and file sharing. Since they are about offering luxury services to drivers, these applications are not delay sensitive applications and can tolerate delays.

3) Technologies and Standards: In order to satisfy the constraints of the VANET applications, a dedicated wireless access technology, called 802.11p, and a set of communication standards have been developed. Indeed, standards bodies both in North America and Europe have defined a family of multiple protocols specifying the operation from the physical to the application layer, and also includes cross-layer aspects such as security or management. In North America, the protocols family is called IEEE WAVE while in Europe it is called ETSI ITS-G5. In this subsection, we describe IEEE 802.11p wireless access technology, also called DSRC and the IEEE WAVE.

4) DSRC Technology: DSRC (Dedicated Short Range Communication) has been proposed as standard for V2V and V2I communications. Specifically, it is a short-range communications service that supports multiple applications requiring low latency and high data rate [27]. DSRC is based on a physical layer and MAC layer defined in the IEEE 802.11p standard. The U.S. FCC (Federal Communications Commission) and the European ECC (Electronic Communications Committee) allocated from 5.85 to 5.925 GHz of spectrum for DSRC. This band is segmented by IEEE and ETSI into 7 channels of 10MH each. These channels are functionally divided into one control channel (CCH) and six service channels (SCHs) as shown in Figure 3. The control channel is used to broadcast status beacons and emergency messages related to road safety, and to advertise services and applications offered on the service channels. The six other channels are dedicated to data transmission of the different services advertised on the control channel.

5) IEEE WAVE: IEEE standard organization has extended its family of 802.11 protocols adding 802.11p [29].

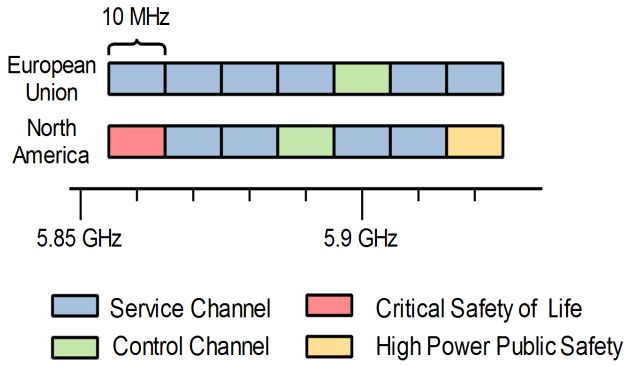

Fig. 3. DSRC Channels reserved for inter-Vehicular communications in North America [27] and Europe [28].

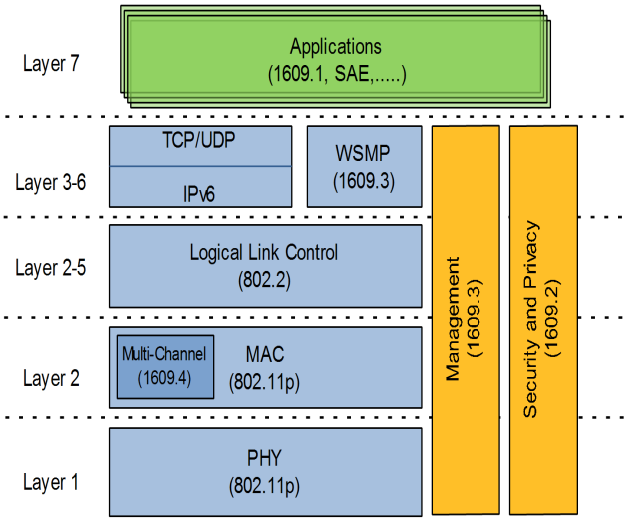

Fig. 4. The DSRC/WAVE model: IEEE 1609.x.

This protocol is mainly based on 802.11a protocol. Indeed, 802.11p modifies the physical and MAC layers of 802.11a to be adapted for VANETs in accordance with the DSRC band. In addition, the IEEE defined 1609.x protocols family, called WAVE (Wireless Access for Vehicular Environment) to access to the wireless medium in VANETs [30]. This family of protocols is structured into four components (1609.1 to 1609.4), which define the architecture, the communication model, the management structure, the security and the physical access in VANETs. As illustrated in Figure 4, 802.11p and WAVE form a complete protocol stack.

- *IEEE 1609.1:* IEEE 1609.1 standard is positioned at the application layer and defines the message formats and the way of storage of data used by the application layer.
- *IEEE 1609.2:* The purpose of this standard is to define the format of secure messages for the system DSRC/WAVE. The standard specifies methods to secure management and application messages. It also describes the procedures to be performed by vehicles to provide security services such as authentication, confidentiality, integrity, and non-repudiation. This standard can be seen as the counterpart to the European standard ETSI 102941-v1.1.1 [16].
- *IEEE 1609.3:* This standard defines the WSM (WAVE Short Message) and its associated exchange protocol, called WSMP (WAVE Short Message Protocol) in order to ensure the functionality of the network and transport layers for safety-related applications. IEEE 1609.3 also defines the WSA Message (WAVE Service Advertisement), which is used to announce the availability of DSRC services in a given location. For example, a WSA can be sent to announce the presence of a traffic information service offered by a RSU.
- *IEEE 802.11p et IEEE 1609.4:* IEEE 802.11p standard defines the physical layer of the DSRC system. It is a customized variant of IEEE 802.11a that combines some parts of the original standard with the 802.11e amendment for the QoS support. On the other hand IEEE 1609.4 standard defines the organization, the scheduling and the use of DSRC channels. This standard has a strong relationship with the sub-layer mechanism EDCA (Enhanced Distributed Channel Access). Indeed, EDCA is based on CSMA/CA channel access method that is used for supporting the IEEE 802.11e standard in WiFi networks. EDCA provides access to the distributed carrier using eight priority levels for users with four access categories (Voice, Video, Best Effort, and Background). This mechanism allows to assign a priority to each message.

B. Location Privacy in Vehicular Networks

Privacy is one of the important human rights that should be protected. The Universal Declaration of the United Nations Human Rights that was introduced in the article 12, in 1948, states that:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." [31].

However, the current technological development has threaten this right and reduced the control of users on their personnel information [32]. When we come to the VANETs, we find that the protection of privacy is an important factor in the public acceptance and the successful deployment of this technology. Many operations may violate the privacy of users in VANETs. Indeed, the private information in VANETs can be classified into two categories: (i) information related to the vehicle such as the position and the registration number, and (ii) information related to the driver and passengers such as the number passengers, their names and their destination [33].

From this, three classes of the privacy protection in VANETs can be distinguished [34]: (i) the vehicle's identity protection, (ii) the vehicle's location protection, and (iii) the protection of the data exchanged in VANETs. The exchanged private data between vehicles and the infrastructure (e.g., financial transactions) or between vehicles themselves (e.g., chat) can easily be protected using encryption mechanisms. For this reason, the protection of the identity and the location are often considered as the primary issues of the field of the privacy protection in VANETs.

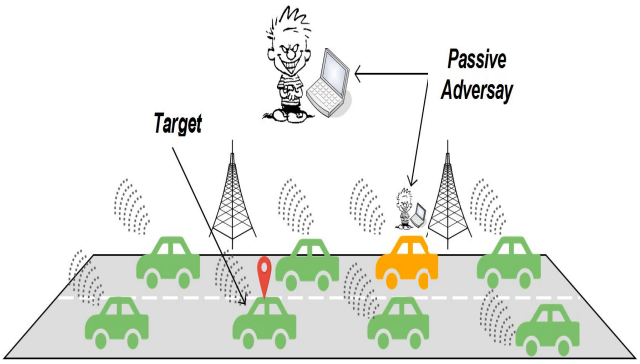

Fig. 5. An illustration of tracking attack.

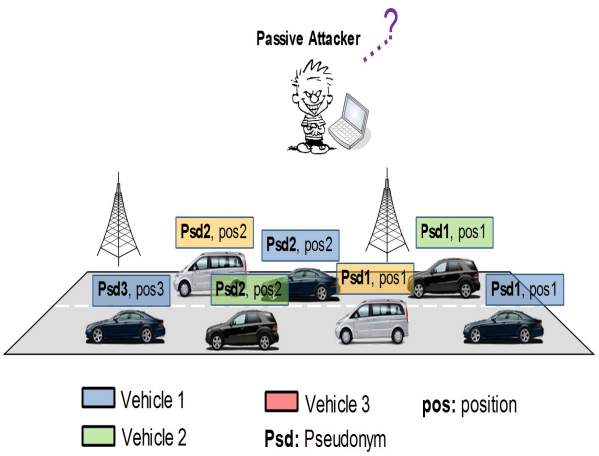

Fig. 6. Pseudonym changing approach.

1) Privacy Requirements: The following privacy requirements have been identified for VANETs [35]:

- *Minimum disclosure:* The amount of information revealed by a user should be limited to the necessary information to ensure VANETs' functionalities.
- *Anonymity:* Messages sent by a vehicle should be anonymous within a set of potential vehicles. This requirement contradicts the accountability, which is one of the main security requirement for VANETs. The accountability states that the authorities should be able to identify the origin of any sent message. For this reason, the anonymity should be conditional in VANETs.
- *Unlinkability:* Two messages related to the same vehicle cannot be linked for longtime.
- *Perfect forward privacy:* Resolution or revocation of one credential should not affect the unlinkability of any of the vehicle's other credentials.

2) Tracking Attack: safety-related applications often rely on a beaconing mechanism. Each vehicle periodically broadcasts a safety message that contains sensitive information about the vehicle such as its identifier, position, and velocity. These safety messages are broadcast with a high frequency ranging from 1 to 10 Hz as mandated by standards bodies [23].

However, as illustrated in Figure 5, due to the nature of the wireless medium, a passive adversary can easily know locations visited by vehicles over time by eavesdropping broadcast safety messages. This compromises the privacy of drivers since the relationship between a vehicle and its driver is strong. Safety messages should then be authenticated in anonymous way. However, location privacy must be conditional to allow the identification and the revocation of malicious vehicles from the system [37]. Indeed, vehicles should be anonymous to each other and identified by authorities. Many anonymous authentication mechanisms have thus been proposed to meet this requirement. These mechanisms are presented in the next subsection.

3) Protection Mechanisms: The existing anonymous authentication mechanisms are classified into three approaches [10]: (i) the pseudonym changing approach, (ii) the group signatures approach, and (iii) the hybrid approach. In the following subsections, we describe each of these approaches. However, we focus more on the pseudonym changing because this approach was adopted by the current security standards [19], and the strategies discussed in this paper are based on it.

- *Pseudonym Changing Approach:* In the context of VANETs, the pseudonym is defined as a fictitious identifier of a vehicle [38]. The pseudonym can be pre-generated or generated on demand [39], [40]. However, we distinguish two types of pseudonym: not disposable pseudonym for a permanent use [8], and the disposable pseudonym for a temporary use for a specified period of time [40]. As illustrated in Figure 6, this approach is based on the periodic change of the pseudonym. Each vehicle uses a set of pseudonyms, and each pseudonym is used for a limited period of time. After expiry of this period, the vehicle changes its pseudonym and only the authorities can know the link between the real identifier of the vehicle and its pseudonyms. In Section II-C, we describe the implementation of the pseudonym changing approach in the current vehicular security standards.
- *Group Signatures Approach:* In this approach, the network is decomposed into groups. In each group, there is a trusted group manager (TGM), members can dynamically join or leave the group. The group signatures approach (GS) allows any group member to sign a message on behalf of the group using its private key without revealing its identifier. Any pair of signatures generated by the same group member cannot be linked together by any entity except the trusted group manager. The TGM is a central trusted entity and is almost identical to a CA. However, the TGM does not issue certificates for the nodes but instead it issues GS private keys (gsk_V^i) for the group members and a single Group Public Key (GPK) for all the group members. GS schemes suffer from a large computation overhead in the signature verification process, which limits the number of certificates that can be verified in a given duration. We notice that there are few studies based on this approach in the literature (e.g., [11]).
- *Hybrid Approach:* The hybrid approach is a combination between the pseudonym changing approach and the group signature approach. In this approach, each vehicle V is equipped with a private key (gsk_V) and a group public

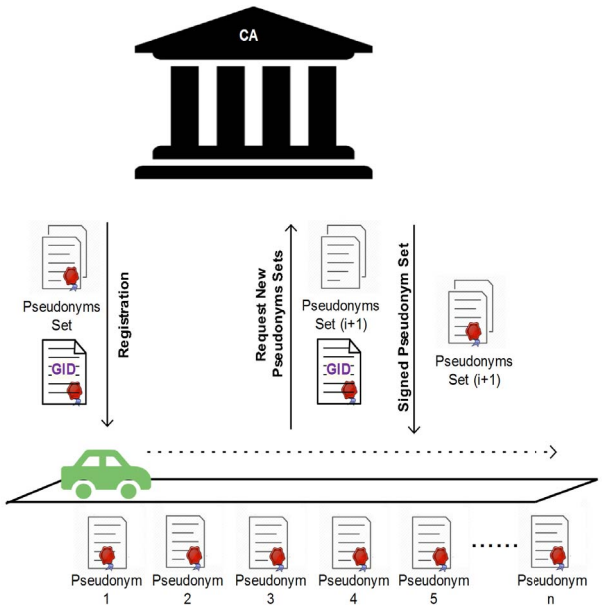

Fig. 7. Simplified view of the Public Key Infrastructure (PKI) described by IEEE and ETSI.

key (gpk_{CA}). Instead of generating the group signatures to authenticate its messages, each vehicle generates its own set of public keys (pseudonyms) (K_V^i) and the corresponding private keys (k_V^i). The vehicle then uses gsk_V for the generation of a group signature $\sum_{CA,V}(k_V^i)$ for each pseudonym. It also generates a certificate $Cert_{CA}^H(K_V^i)$ for each pseudonym. Before sending a message, the vehicle digitally signs it by a private key k_V^i that corresponds to the pseudonym K_V^i, a certificate $Cert_{CA}^H(K_V^i)$ is attached to each sent message. This approach inherits the problem of the large computation overhead in the signature verification process from the group signatures approach [13], [41].

C. Pseudonym Changing Approach

To secure VANETs, the current vehicular security standards IEEE 1609.2 [15] and ETSI 102941-v1.1.1 [16] describe the deployment of a security architecture based on a Public Key Infrastructure (PKI), as illustrated in Figure 7. CA is the Certificate Authority, which may belong to the governmental transport authorities or simply to one of the vehicle manufacturers, and takes in charge the management of the certificates. To ensure the authentication and anonymity at the same time, each registered vehicle is initially equipped by a set of M pseudonyms and a base identifier (GID). A pseudonym is a public key certified by the CA, which does not reveal any information about the real identifier of the vehicle V. For each pseudonym K_V^i of this set, the CA provides a certificate $Cert_{CA}(K_V^i)$ that includes its own digital signature on the pseudonym K_V^i. Before sending a message, the vehicle digitally signs it by a private key k_V^i corresponding to the pseudonym K_V^i. To enable the validation of the message, the certificate corresponding to the pseudonym K_V^i of the signatory is attached to each sent message.

A receiving vehicle has to check whether K_V^i is a valid pseudonym by checking the signature in $Cert_{CA}(K_V^i)$ using the CA public key and verifying if all other necessary fields of $Cert_{CA}(K_V^i)$ are valid. Then, it needs to check if the signature for the message ($\sigma_{k_V^i}$) is correct. To allow the unlinkability of the broadcasted safety messages, each pseudonym is used for a short period. For example, [39] estimated that a vehicle needs about 43800 pseudonyms if it is used for two hours a day in average. Therefore, before the consumption of all the pseudonyms of the set **i**, the vehicle uses its base identifier (GID) to request a new signed set of pseudonyms **i+1** from CA. This process is called the pseudonym refilling or the pseudonym sets distribution and the performed exchanges between the CA and the vehicle during this process are encrypted. Furthermore, as vehicles can be sold or broken, and their OBUs could be compromised, it is then necessary that CA must be able to revoke their pseudonyms [42]. This process is called the certificate revocation and can be achieved by distributing a list of revoked certificates called Certificate Revocation List (CRL). In addition, CA is the only entity that can perform the operation of the resolution of the pseudonym, i.e., revealing the real identifiers of the vehicle V from its pseudonym K_V^i in a case of investigations.

D. Studies on the Efficiency of Pseudonym Changing

Several studies have been conducted on the effectiveness of pseudonym changes. Table II summarizes some of these studies according to: (i) the used tracking technique, and (ii) the ratio of successful tracking. Buttyán *et al.* [43] studied the impact of the adversary power on the effectiveness of pseudonym changing. The used technique to track vehicles is based on a Bayesian decision algorithm. The obtained results have shown that if the adversary only controls the half of road intersections then the success tracking probability reaches 90%. Wiedersheim *et al.* [46] used an advanced tracking method called Multi-Hypothesis-Tracking (MHT) [44] incorporating with the Kalman filter [47] to track vehicles. They claimed that a global passive adversary can effectively track vehicles with accuracy of almost 100%. Emara *et al.* [7] showed that the tracking can effectively be done (more than 90%) even using a simple tracking method, called the Nearest Neighbor Probabilistic Data Association (NNPDA) [48]. In a recent study presented in Black Hat conference Petit *et al.* [45] demonstrated through real-world experiments using ITS hardware that the location tracking of vehicles can easily be performed. Indeed, they found that the tracking success is achieved 40% using only two sniffing stations, and 90% if 8 sniffing stations are used.

The results of all these studies confirmed that vehicle's positions can be tracked even with the frequently changing of pseudonyms. This can be done using the pseudonyms linking attack. This attack is presented in the next subsection.

E. Pseudonyms Linking Attack

Two types of pseudonyms linking attack have been identified by Buttyán *et al.* [49]. These types are described in the following subsections.

TABLE II
STUDIES ON THE EFFICIENCY OF PSEUDONYM CHANGING

Name of paper	Used tracking technique	Ratio of successful tracking
Buttyán et al. [43]	Bayesian decision algorithm	90%
Wiedersheim et al. [44]	Multi-Hypothesis-Tracking incorporating with the Kalman filter	100%.
Emara et al. [7]	Neighbor Probabilistic Data Association	more than 90%
Petit et al. [45]	Real-world experiments	90% (8 sniffing stations)

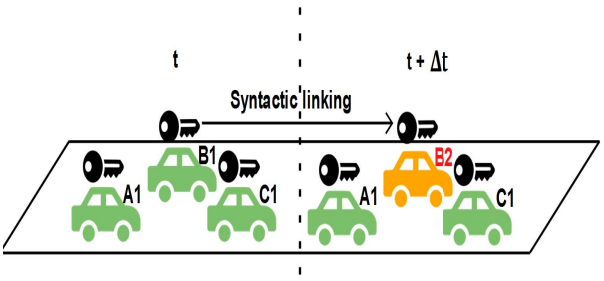

Fig. 8. The syntactic linking of pseudonyms [50].

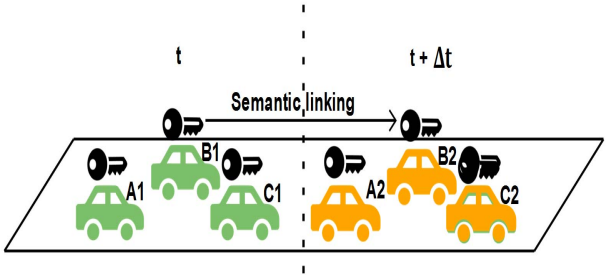

Fig. 9. The semantic linking of pseudonyms [50].

1) Syntactic Linking: Figure 8 illustrates the syntactic linking of pseudonyms case. If during Δt only one vehicle (B) changes its pseudonym (from *B1* to *B2*) among the three vehicles that running on the road, the adversary can then easily link the pseudonyms *B1* and *B2*. The protection against this type of attack can be performed through using a mechanism to synchronize the changes of pseudonyms between vehicles.

2) Semantic Linking: Figure 9 illustrates the semantic linking of pseudonyms. This type of attack is more powerful than the syntactic linking of pseudonyms because the adversary relies on the information included in safety messages to link the pseudonyms. For example, the adversary can predict the next position of the vehicle using a tracking method like [7], [46]. Then, based on this prediction the adversary can link the pseudonyms *B1* and *B2* even if the three vehicles (A, B and C), illustrated in Figure 9, change their pseudonyms at the same time. The protection against this type of attack can only be done by preventing the adversary to get access to safety messages for some periods of time.

F. Privacy Metrics

A variety of metrics have been proposed to evaluate the level of the location privacy protection achieved by a pseudonym changing strategy. Wagner and Eckhoff [25] reviewed the different metrics used in this context. In the following, we present the most used metrics:

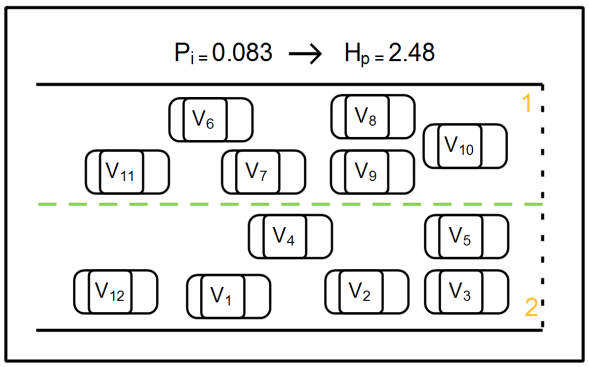

Fig. 10. An illustration of tracking attack.

- *Anonymity set size:* The anonymity set, denoted by AS, is defined as the set of vehicles that are indistinguishable from the target with the set including the target itself [51]. The size of the anonymity set |AS | is then the number of vehicles that the anonymity set includes. The size of the anonymity set represents the level of the location privacy protection achieved, which should be greater than 1 in this case. However, this metric assumes that all vehicles of the anonymity set are equally likely to be the target. Therefore, as discussed in [52], the prior knowledge of the adversary that makes some vehicles more likely to be the target than the others cannot be described using this metric. For this reason, the entropy is suggested as a metric [52].
- *Entropy of the anonymity set size:* The entropy is a concept coming from the information theory that expresses the uncertainty in a random variable. In contrast to the anonymity set size, the entropy of the anonymity set, denoted by H_p, allows expressing the adversary's knowledge about each vehicle of the anonymity set. The entropy is calculated using the following formula [53]:

$$H_p = -\sum_{i=1}^{|AS|} p_i \log_2 p_i$$

where p_i refers to the probability of a vehicle i being the target. If all vehicles have a same probability to be the target, i.e., the probabilities are uniformly distributed over the anonymity set, the entropy then achieves its maximum

TABLE III
STRENGTHS AND WEAKNESSES OF PRIVACY METRICS

Metric	Privacy aspect	Strengths	Weaknesses
Anonymity set size	Uncertainty	- Simple to compute.	- Prior knowledge is not considered.
Entropy of the anonymity set size		- Prior knowledge is considered	- Inference probabilities are difficult to calculate
The degree of anonymity		- Prior knowledge is considered - Obtained information can be measured	
Adversary's success rate	Adversary's success	- An evident measure of the tracking probability	- Depends on the used tracking algorithm - A huge computation resources may be consumed
Maximum tracking time	Time	- An evident measure of the tracking time.	
Statistics on pseudonym changes	Statics	- Information about the use of pseudonym can be obtained	- Privacy protection is not evaluated

value, denoted by H_{max}, which is given by:

$$\forall i : p_i = \frac{1}{\mid AS \mid}, H_{pmax} = -\sum_{i=1}^{|AS|} p_i \log_2 p_i = \log_2 |AS|.$$

Figure 10 illustrates a simple example on how to compute the entropy. We assume a 2-lanes road contains 12 vehicles. If we consider that all vehicles have the same probability (p_i = 1/12) to be the target, the entropy is then equal to 2.48.

- *Degree of anonymity:* If we assume that the adversary has no prior knowledge about vehicles of the anonymity set, the obtained information can then be measured using the following difference: H_{max} - H_p. Reference [53] proposed the degree of anonymity d, which a normalized value of (H_{max} - H_p) in the range [0,1]. The degree of anonymity is then computed using the following formula:

$$d = 1 - \frac{H_{max} - H}{H_{max}} = \frac{H}{H_{max}}$$

- *Adversary's success rate:* The adversary's success rate is generally defined according to the proposed pseudonym changing strategy. It represents the ratio of vehicles that could still be tracked by the adversary after executing the strategy.
- *Maximum tracking time:* The maximum tracking time measures the maximum duration of time that the adversary could link the pseudonyms of vehicles.
- *Statistics on pseudonym changes:* This can include information about changed pseudonyms such as their total number and the number of successful changes.

Table III gives the measured privacy aspect [24] and summarizes the strengths and weaknesses of each metric. The anonymity set size is simple to calculate. However, it does not take the prior knowledge of the adversary into the account. This feature is, in contrast, considered both in the entropy and the degree of anonymity. In addition, this latter allows to calculate the amount information obtained by the adversary. However, the probabilities of vehicles for being the target are difficult to compute in the entropy and the degree of anonymity. In the other hand, the adversary's success rate and maximum tracking time are more evident metrics. The first one calculates the tracking probability while the second one calculates the maximum tracking time for vehicles. However the problem with these two metrics is that the obtained results strongly depend on the used tracking algorithm that could consume huge computation resources. Finally, statistics on pseudonym changes metric gives interesting information about the use of pseudonyms like their numbers. But, this metric does not give any information about the efficiency of the proposed protection mechanism.

G. Adversary Model

Due to the complexity of the VANET system, different attacks can be performed by different types of adversary. The potential types of adversary in VANETs have been extensively studied in the literature. Reference [39] identified the following types of adversary:

- *Global vs. Local:* Compared to a local adversary, a global adversary has an overall coverage of the VANET. It can then eavesdrop every message diffused by any vehicle.
- *Active vs. Passive:* An active adversary is more dangerous than a passive adversary since it can alter or inject messages, while a passive attacker can only eavesdrop messages.
- *Internal vs. External:* An internal adversary is an authenticated member of the VANETs system. An external adversary is considered as an intruder.

A location privacy adversary model aims to track the target vehicle by eavesdropping all communications of any vehicle within a region of interest. For this reason, researchers often consider the global passive adversary to study the location privacy in VANETs. Reference [54] pointed out that due to the cost of eavesdropping the global coverage, is hard to be achieved. Petit *et al.* [45] defined more realistic adversary called mid-sized adversary. The coverage of this adversary is larger than a local passive adversary and less than a global passive adversary. In another words, it can cover a limited number of areas without getting the full coverage. The authors also suggested to take into the account the tracking period to evaluate the power of this adversary. The tracking period represents time that the adversary try to link the pseudonyms of vehicles. Based on this latter parameter, the authors distinguished tree tracking types:

- *Short-term tracking:* The adversary tries to track vehicles only for a couple of seconds.
- *Mid-term tracking:* The adversary tries to track vehicles for a single trip, which can go from a couple of minutes to a couple of hours.
- *Long-term tracking:* In this case the period in which the adversary tries to track vehicles is extended to several days.

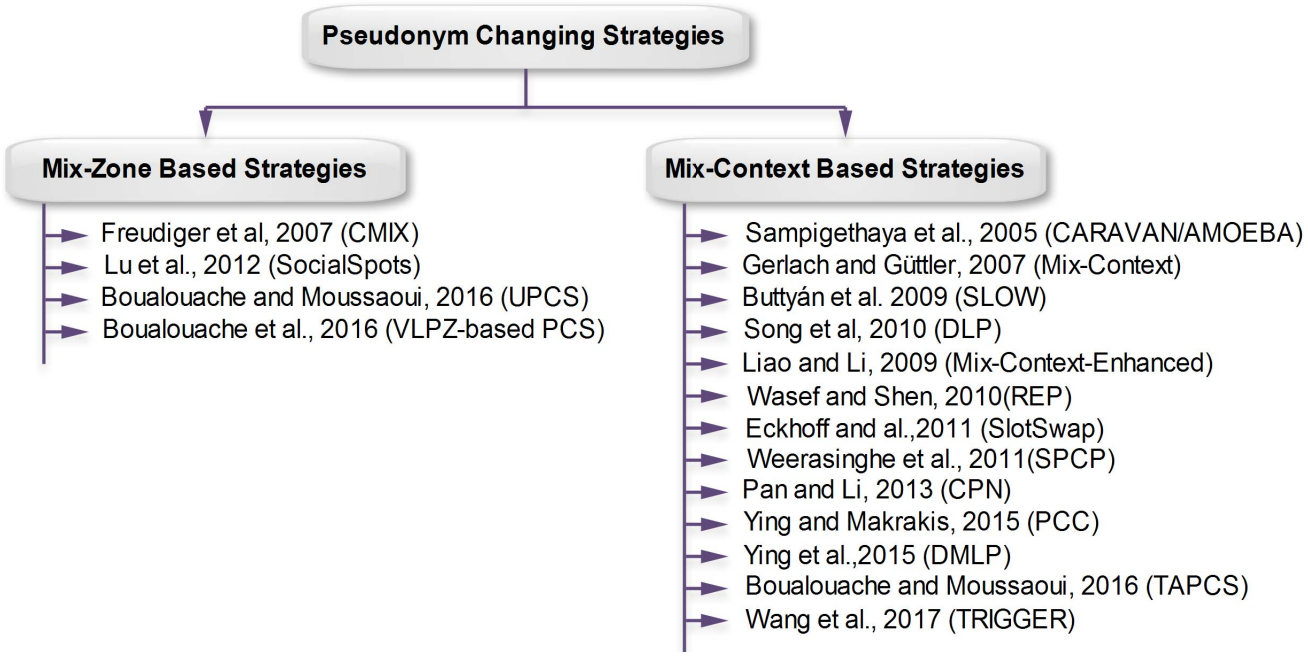

Fig. 11. Pseudonym changing strategies taxonomy.

III. Pseudonym Changing Strategies: A Taxonomy

The main purpose of a pseudonym changing strategy is to determine where and when a vehicle should change its pseudonyms to achieve the unlinkablity between them. Many pseudonym changing strategies have been proposed to provide protection against the pseudonyms linking attack. In Figure 11, we propose a taxonomy of existing pseudonym changing strategies for vehicular ad-hoc networks. We divide these strategies into two categories: (i) mix-zone-based strategies, and (ii) mix-context-based strategies.

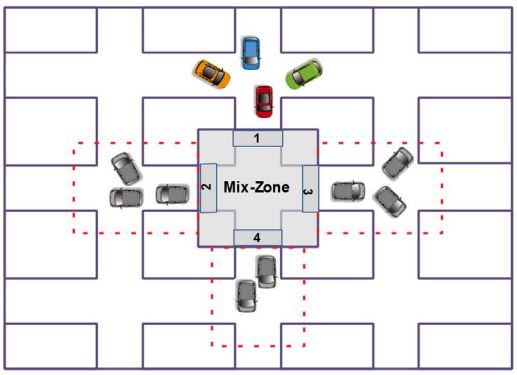

Fig. 12. Mix-zone concept.

A. Mix-Zone-Based Strategies

In mix-zone-based strategies, vehicles change their pseudonyms on predefined road areas, called mix zones. The concept is first proposed by Beresford and Stajano [55] in the context of pervasive computing. Buttyán *et al.* [43] studied the location privacy protection against a limited adversary model that can only control a limited number of places of the vehicular area. They then considered the regions that are not controlled by the adversary as mix zones.

Figure 12 illustrates a mix zone installed at a road intersection. If a vehicle enters the zone from the port 1, changes its pseudonym inside the mix zone, and after that exits it from one the port 2,3,4 the adversary could confused due of this.

The first implementation of the mix-zone concept proposed by Freudiger *et al.* [56]. The authors proposed a protocol for creating CMIX (Cryptographic MIX) zones. A CMIX zone is a road area where safety messages are encrypted. The authors suggested placing these mix zones at road intersections. Vehicles change their pseudonyms inside a CMIX zone and use a shared key distributed by a RSU to encrypt their safety messages. Each intersection is equipped by a RSU, which periodically broadcasts a notification to inform vehicles the existence of a CMIX zone. When a vehicle receives such notification, it sends a message to the RSU to request the encryption key. As soon as the RSU receives the request, it provides the encryption key to the vehicle and waits for an acknowledgment from it. If the vehicle well received the key, it sends the acknowledgment to the RSU, and starts the encryption of its safety messages using this key. It must also change its pseudonym within the CMIX zone. The main reason for encrypting safety messages is to prevent the considered external adversary from reading their content. The authors also pointed out the problem of vehicles entering to a CMIX zone that did not receive a notification for the RSU yet. Indeed, these vehicles are not able to decrypt the safety messages coming from the CMIX zone. For this reason, they proposed that the encryption key should be forwarded from the vehicles that are already inside the CMIX zone to the vehicles entering to it.

Besides of this, several works have been conducted to propose the optimal deployment of CMIX zones over the road's intersections (e.g., [57]–[61]). In these works some optimization techniques such as the multi-objective optimization, heuristics, and the game-theoretic approach are used to find the optimal deployment of CMIX zones to achieve high levels of location privacy protection.

Lu *et al.* [40], [62] suggested to change the pseudonym at Social Spots, which are simply public places areas such as signalized intersections, when traffic light turns to red, and parking lots near a shopping mall. Two simple pseudonyms changing strategies are then proposed in these papers: (i) all vehicles stopped in front of the red traffic light at signalized intersections, change their pseudonym together when the traffic light turns green, and (ii) each vehicle stopped at a free parking lot near a shopping mall, changes its pseudonym just before leaving the parking lot.

Boualouache and Moussaoui [63], [64] proposed a strategy adapted for the urban environment, called Urban Pseudonym Changing Strategy (UPCS). This strategy is based on the creation silent mix zones at signalized intersections only while the traffic light is red. The authors suggested that vehicles can either change or exchange their pseudonyms inside these silent mix zones. The signalized intersection is then equipped by a RSU, which starts broadcasting notifications only if the traffic light turns to red. Each notification includes the position of the beginning of the silent mix zone, denoted by P_{sm}. If a vehicle receives such notification, it compares its position with P_{sm}. If a vehicle finds itself inside the silent mix zone, it immediately stops broadcasting safety messages. Two techniques can be used inside the silent mix zone. Indeed, the vehicle can either simply change its pseudonym or exchange it with other vehicle. The exchange of pseudonyms is performed using the swapping protocol, where each time, the RSU chooses randomly two vehicles to exchange their pseudonyms and informs the CA about each performed exchange to keep the accountability. All the messages used in the exchanging are encrypted.

Boualouache *et al.* [50] proposed a pseudonym changing strategy based on a designed roadside infrastructure, called the Vehicular Location Privacy Zone (VLPZ). The design of a VLPZ is similar to existing roadside infrastructures such as gas stations, electric vehicles charging stations, and toll booths. A basic VLPZ consists of two points: (i) one entry point called *the router*, and (ii) one exit point called the *aggregator*; and a limited number of lanes l where $l > 1$. Vehicles arrive to a VLPZ, one after another, on one lane. When a vehicle reaches *the router*, it stops broadcasting safety messages and heads for a VLPZ's lane randomly and privately assigned by *the router*. Vehicles can reside inside a VLPZ for a random period of time. For example, if a VLPZ is deployed in a gaz station, this period is the time taken by the driver to fill the fuel tank of its vehicle. Vehicles must change their pseudonyms before they exit the VLPZ through the aggregator. However, the exit order is different from the entering order since the residency periods of vehicles are random. The main use of multiple lanes in this strategy is to confuse the adversary. Indeed, if a vehicle stops sending safety messages before entering a VLPZ, the adversary cannot neither know the lane to which the vehicle is headed nor predict the exit time of the vehicle from the VLPZ. Thus, the FIFO attack cannot be performed since the exit order and the entering order are different.

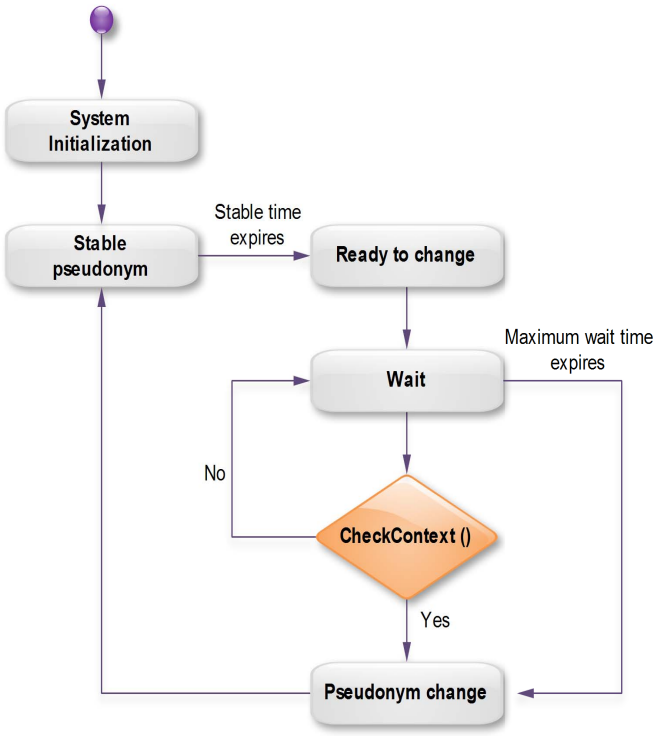

Fig. 13. A general state diagram of a mix-context-based strategy [66], [67].

B. Mix-Context-Based Strategies

In contrast to mix-zone-based strategies, in mix-context-based strategies, each vehicle independently determines where and when to change its pseudonym. This concept is first introduced in the context of wireless networks in general [65]. The concept is called a user-centric approach and suggests that mobiles users should be able to control their location privacy protection. Reference [66] adapted this concept for VANETs. Indeed, the authors defined the mix-context as any situation or opportunity helps the vehicle to increase its location privacy protection using the changing of pseudonym mechanism. Precisely, the mix-context is defined as any situation or opportunity to synchronize the change of pseudonyms between vehicles. The vehicle then changes its pseudonym only if the mix-context is found.

Figure 13 illustrates a general state diagram of a mix-context based strategy. The vehicle is initially equipped by a set of pseudonyms. Each pseudonym is used for a limited period of time, which is called the stable time. The stable time should be greater than a certain threshold to not affect safety-related applications [18]. After the expiration of the stable time, the vehicle then moves to *ready to change* state. It initializes a timer and starts looking for a mix context. If the mix context is found, the vehicle immediately changes its pseudonym.

However, if the mix-context is not found after a certain threshold of time determined by the system designer, the vehicle is forced to change its pseudonym.

Gerlach and Güttler [66] considered the direction and the number of vehicles in the communication range as mix context parameters. The vehicle changes its pseudonym only if it detects k neighboring vehicles at a distance smaller than the minimal distance and have a similar direction with it within its communication range. The minimal distance is considered equal to 4.25 meters in their simulations. Song *et al.* [68], [69] proposed the Density-based Location Privacy (DLP) strategy, which is based on a zone known as K-density zone to change the pseudonym. The vehicle changes its pseudonym within the K-density zone, if (k-1) neighbors are found over the communication range.

Liao and Li [67] proposed an improvement of [66]. The authors proposed to add the speed, the distance between vehicles and the road segment in the mix context. They also proposed to insert a bit (flag) in the safety message, which indicates the willingness of a vehicle to change its pseudonym. The vehicle then changes its pseudonym if it found k neighboring vehicles have similar status to itself and whose flags equal to 1. The purpose of these improvements is to increase the probability that many vehicles simultaneously change their pseudonyms.

Pan and Li [70], [71] proposed Cooperative Pseudonym strategy (CPN). They first assume that vehicles' broadcasts are synchronized with a same time slot using GPS clocks. Vehicles thus send their beacons in the same time. Each vehicle regularly updates its list of neighboring vehicles $L = \{0, \ldots .N\}$. As illustrated in Algorithm 1, a vehicle v changes its pseudonym if it found at least k neighboring vehicles ready to change their pseudonyms or if one of its neighboring vehicles (L_i) has at least k neighboring vehicles ready to change their pseudonyms. In another words, on the one hand, the vehicle v cooperates with its neighbors if one of them has k or more neighbors ready to change their pseudonyms. On the other hand, if v has k neighbors ready to change their pseudonyms, they will cooperate with it, if none of them has k neighbors ready to change their pseudonyms. The implementation of this strategy is recently detailed in [72]. The authors proposed to insert two flags into safety messages: (i) Waitflag: that is used to announce that the vehicle is waiting to change its pseudonym (wait status), and (ii) Readyflag: that is used to announce that the vehicle is ready to change its pseudonym in the next time slot (ready status). Waitflag is initially set to 0 to indicate that the vehicle is in the wait status. If the pseudonym stable time is expired, the vehicle then checks if its Readyflag or the Readyflag of any its neighboring vehicles is equal to 1. If so, the vehicle changes its pseudonym and sets its Waitflag and Readyflag to 0. Otherwise, the vehicle checks if there are K neighboring vehicles with Waitflag equal to 1. If so, the vehicle sets its Readyflag to 1 for expressing its readiness to change its pseudonym in the next time slot.

Ying and Makrakis [73] proposed a pseudonym changing strategy based on a Candidate-location-list, called PCC. As Pan and Li [71] assumed that the vehicles' broadcasts are synchronized with a same time slot. They also assume that safety

Algorithm 1: Cooperative Pseudonym Strategy (CPN)

```
Data: List neighboring vehicles L = {0, ....N}
Result: Pseudonym Changing
Initialize;
if (Ready_to_change(L) >= k) then
    change the pseudonym;
else
    if (nb_neighboring(L_i) >= k) then
        change the pseudonym;
    end
end
```

messages could be sent in a multi-hops way and pseudonyms could be reused more than one time. The authors proposed to insert new five fields into each safety message: (i) *sa1*: the address of the vehicle that generates the message, (ii) *sa2*: the address of the vehicle that rebroadcasts the message, (iii) *hop*: the number of hops between the source and the receiver, which is initially set at 0 and incremented each time the safety message is rebroadcast, (iv) *MaxLiveTime*: the lifetime of the message, and finally (v) *ChStot*: that indicates on which time slot the vehicle should change its pseudonym. These additional information aim to allow a vehicle to track the time slots on which other vehicles change their pseudonyms. Each vehicle then stores some information about received safety messages in a Candidate Location List (CCL) for a limited storage time (*MaxLiveTime*). Each entry of the CCL contains the following fields: *ID*, *hop*, *ChSlot*, *MaxLiveTime*, *Position*, and *Timestamp*, where *ID* and *Position* are respectively current pseudonym and position of the vehicle, and *Timestamp* is the time when the entry is inserted or updated. If a vehicle receives a safety message, it first checks if the value of *hope* is less than *MaxHopThreshold*. If so, the vehicle then inserts an entry for this message, increases the value of *hop* by 1, and rebroadcasts the message again. In addition, if the vehicle receives a safety message with a value of *hope* less than the value of *hope* saved in its CCL, it then updates the corresponding entry.

Thus, the PCC strategy is executed as follows. The vehicle initially sets the value *ChStot* to -1. Based on the prediction on the movement of vehicles, it periodically calculates the distance between itself and each vehicle saved in its CCL. It then chooses at least k vehicles that have minimum distances from it. h_{max} is defined as the maximum value of *hop* of these vehicles. If a vehicle's pseudonym expires at time slot i, the vehicle should then broadcast a safety message with *ChSlot* equals to i+1 at time slot i-h_{max}. If a vehicle receives such message, it rebroadcasts it and changes its pseudonym at time slot i+1. However, if during the lifetime of the current pseudonym, the vehicle receives several safety messages with different values of *ChSlot*, it changes its pseudonym at the minimum value of *ChSlot* and does not change it again until its expiration.

Sampigethaya *et al.* [51], [74] adopted the use of the random silence periods concept [75]. The authors proposed that vehicles turn their radio transmitters off (stop sending safety messages) for a limited random period of time each time

when they are going to change their pseudonyms. The aim of this random silence period is to try to confuse the adversary. Indeed, If at same time two vehicles at least turn their radio transmitters off for a random period of time and change their pseudonyms during this period, the adversary could then be confused [76], [77].

Buttyán *et al.* [49] proposed a simple pseudonym changing strategy, called SLOW (Silence at low speeds). This strategy uses the radio silence concept. Indeed, the authors suggested that vehicles turn their radio transmissions off when their speeds are less than 30Km/h and change their pseudonyms during the radio silence. Ying *et al.* [79], [80] proposed a pseudonym changing strategy, called DMLP (Dynamic Mix-Zone for Location Privacy in Vehicular Networks). This strategy aims to dynamically create CMIX zones, i.e., the vehicle establishes a CMIX zone where and when it is needed. The authors introduced new entities in the VANET system architecture, called Control Servers (CSs). CSs are responsible to control and coordinate the change of pseudonyms processes between vehicles. Each CS is connected to a set of RSUs that cover a certain area. Each pseudonym is used by a vehicle for Δt. If a vehicle v wants to create a DMLP, it should send a Request New Pseudonym (RNP) message to CS close to the expiration of its current pseudonym. The vehicle v broadcasts the last message with the old pseudonym at t and waits for the period of time (τ) to change its pseudonym before begins broadcasting safety messages. τ is the period of time that takes the vehicle to create a dynamic mix zone. The dynamic mix zone is created as follows. If the CS receives a RNP message, it first determines the length (l) of the zone that will be created. After that it sends a COMMAND message to the relevant RSUs that exist in the zone. As soon as a RSU, receives such message, it immediately rebroadcasts it to the vehicles within its communication range. If a vehicle receives a COMMAND message, it starts encrypting safety messages, changes its pseudonym and sends a RNP message to the CS. The concerned vehicles are still encrypting safety messages for T_{EP}, which is $T_{EP} \leq \Delta t$.

Wasef and Shen [81] suggested random encryption periods (REPs). When the vehicle decides to change its pseudonym, it sends a request to its neighbors for starting a REP. During a REP, the safety messages are encrypted using a shared group key. A REP is considered successful if at least one of the neighbors also changes its pseudonym and its speed or its direction. Eckhoff *et al.* [8], [82] proposed a pseudonym changing strategy called SlotSwap. In this strategy, vehicles are equipped with GPS clocks and a limited number of pseudonyms. Each pseudonym is used for exactly 10 min and the pool of pseudonyms is reused each week. Vehicles change their pseudonyms at the same time according to GPS signals. The authors also pointed out that pseudonyms can be linked due to the use of the same pseudonym each week in the same period. For this reason, they proposed the exchanging of pseudonyms technique, which is inspired by [65]. Vehicles can then exchange their pseudonyms through encrypted channels.

Wang *et al.* [83] proposed TRIGGER, a pseudonym changing strategy that relies completely on the exchange of pseudonyms between vehicles. When the stable pseudonym time is expired, the vehicle then starts seeking for candidate vehicles to exchange its pseudonym with them. A neighboring vehicle is considered as a candidate only if the trigger is found, i.e., the candidate vehicle should have the same heading and small differences both in position and velocity with the vehicle requesting to exchange its pseudonym (A). If candidate vehicles are found, the vehicle (A) then sends a pseudonym exchanging request to the RSU. This latter then: (i) checks the validly of the request, (i) randomly choses the candidate vehicle (B) that will be involved in the exchange, and (iii) forwards the request to the CA to execute the operation. Finally, the vehicles (A) and (B) just have to wait their new pseudonyms.

Weerasinghe *et al.* [84] proposed a strategy called SPCP (Synchronized Pseudonym Changing Protocol). In SPCP, vehicles are self-organized as groups. Each group is managed by a group leader, which randomly decides when to change the pseudonyms of group's members. All members are then informed about the time when the pseudonym changing process will occur. During this process each member the group identifier as a temporal pseudonym and each vehicle quits the group should also changes its pseudonym.

Boualouache and Moussaoui [85] proposed a strategy, called TAPCS (Traffic-Aware Pseudonym Changing Strategy). In TAPCS, vehicles continuously monitor the road traffic's status to find a good place where the silent mix zone (SM) can be created. This strategy is mainly based on a privacy-preserving traffic congestion detection protocol that acts as a trigger of the strategy and consists of fives phases. (i) Traffic Congestion Detection Phase: In this phase, every vehicle continuously monitors its speed. If its speed is still lower than a certain threshold for a certain period of time, the vehicle reports a potential traffic congestion and broadcasts a congestion message. The detection of the traffic congestion is confirmed only if the vehicle receives a specific number of traffic congestion confirmations from the surrounding vehicles. (ii) TAPC strategy's Initiator Election Phase: After detecting the traffic congestion, a first initiator of the strategy should be elected. If the vehicle did not receive any initiation message from one of the surrounding vehicles and confirms the existence of traffic congestion, it stops broadcasting safety messages for a random time, changes its pseudonym, broadcasts an initiation message, and waits for a certain delay time. During this time, it stores each received initiation message. In the end of this time, the vehicle checks if it has the minimum distance relative to the event caused the traffic congestion. If so, the vehicle assigns itself as an initiator for the strategy. (iii) Silent Mix Zone Creation Phase: Just after its election, the initiator stops broadcasting safety messages, changes its pseudonym and starts broadcasting notifications, which contain the position and the direction of the initiator and the threshold of speed below of which vehicles stop broadcasting safety messages. If a vehicle receives such notification, it checks if it is situated in the same direction behind the initiator and its speed is lower than the speed threshold included in the notification, if so the vehicle then stops broadcasting safety messages and changes its pseudonym during this time. At this level, a silence mix zone is created where no safety message is broadcast inside

this zone. The size of this zone is equal to the communication range of the initiator. (iv) Silent Mix Zone Extension Phase: The SM zone should be extended to ensure the strategy process. Therefore, before the zone will be filled by vehicles, a new initiator should be elected among vehicles already inside the zone. To do this each vehicle inside the zone computes the distance between its position and the position of the old initiator. If the calculated distance belongs to a defined interval of distance, the vehicle executes the initiator election phase as described in phase (ii). The width of this interval is set by the system administrator according to some parameters such as the communication range, the mobility and the speed of vehicles. If the new initiator is elected, the previous one stops broadcasting notifications as soon as receives the first notification from the new initiator. and finally (v) End of Traffic Congestion Detection Phase : The extension of the SM zone process continues until the end of the traffic congestion; which is detected by the first initiator. Indeed, when its speed is still higher than the speed threshold for a certain period of time, it then broadcasts the end of congestion message. This message will be rebroadcast by each elected initiator. If a vehicle receives this message, it restarts broadcasting safety messages again.

C. Summary

In this section, we provide a summary to get an overview of the presented pseudonym changing strategies. Table IV summarizes characteristics and the methods used to evaluate the presented strategies. The parameters of this summary are presented as follows:

- *Category:* indicates to which category the strategy belongs.
- *Mode:* indicates whether the strategy needs the infrastructure to work or not.
- *Radio Silence:* indicates whether the strategy uses the radio silence or not.
- *Encryp:* indicates whether the strategy uses the encryption or not.
- *Pseudo Exchange:* indicates whether the strategy uses the exchanging of pseudonyms or not.
- *Evaluation Metric:* indicates which metric is used to evaluate the level of the location privacy protection achieved by the strategy. These metrics are described in Section II-F and abbreviated in Table I.
- *Evaluation Method:* indicates which method is used to evaluate the level of the location privacy protection achieved by the strategy.

IV. Comparison & Discussion

In this section, we discuss the effectiveness of pseudonym changing strategies. We based our analyses on a strong passive adversary model, consisting of an External Global Passive Adversary and an Internal Local Passive Adversary composed of few attackers. A realistic study case of the assumed adversary model can be given as follows. Similarly to a mobile network, a VANET infrastructure is envisioned to be managed by vehicular system operators. It could exist for example a corrupt employee that works at an operator and has a full access to the infrastructure administration system. Since this employee is able to capture each event occurs in the VANET system, he can be considered as an external global passive adversary. Moreover, this employee can collude with some VANET's users (drivers) to help him in the tracking of their targets. These users can then be considered as an internal local passive adversary. In this discussion, we study the location privacy protection provided by the strategies against each part of the adversary model (internal or external) separately.

By synchronizing pseudonym changing processes between vehicles, all strategies provide some level of protection against the syntactic linking of pseudonyms attack. This level of protection depends on the accuracy of the applied synchronization method and the number of vehicles that involved in this process. After analyzing the strategies, we distinguished three used synchronization methods. We could sort them according to their effectiveness against the syntactic linking attack as follows:

1) GPS-based synchronization: In this method, vehicles use GPS clocks to synchronize the change of their pseudonyms.
2) Infrastructure-based synchronization: In this method, protected zones are created with the help of road infrastructures. Vehicles thus change their pseudonyms inside these zones, which makes an impression that the changing of pseudonyms is synchronized.
3) Protocol-based synchronization: In this method, vehicles run a distributed protocol to synchronize pseudonym changes between them. Indeed, vehicles can make an appointment to change their pseudonyms at a given time.

We argue that the strategies based on the GPS synchronization method are the most effective against the syntactic linking attack, because they involve all vehicles. In addition, using the GPS signals is considered among the most accurate time synchronization methods. Indeed, the accuracy of GPS time signals is at the level of a few nanoseconds [87]. However, GPS signals could be affected due to the bad weather and cannot be received in the tunnels, underground passages, or near tall buildings [88]. The infrastructure-based method is the second more effective synchronization method, because it involves a limited number of vehicles, i.e., only vehicles exist inside the zone controlled by the infrastructure. As the external adversary cannot control the zone, it seems that all pseudonyms changes occur simultaneously. The protocol-based synchronization method is less effective than the others because it involves a limited number of vehicles and it is not guaranteed if all the concerned vehicles will change their pseudonyms or not.

Regards the protection against the semantic linking attack, we noticed that just few strategies can provide protection against this attack. These strategies are based on hiding safety messages information from the adversary for some period of time. To achieve this, two techniques have been proposed: the encryption and the radio silence. However, each of these two techniques has drawbacks. On the one hand, the encryption of safety messages is ineffective against the internal passive

TABLE IV
A SUMMARY OF PSEUDONYM CHANGING STRATEGIES

Category	Strategy	Mode	Radio Silence	Encryp	Pseudo Exchang	Evaluation Metric	Evaluation Method
Mix-context-based	CARAVAN/A-MOEBA [51], [74]	Infrastructureless	Yes	No	No	Entropy MTT	Analy-model Simulation
	Mix-Context [66]	Infrastructureless	No	No	No	MTT	Simulation
	SLOW [49]	Infrastructureless	Yes	No	No	ASR	Simulation
	DLP [68], [69]	Infrastructureless	No	No	No	ASR	Analy-model
	Mix-Context-Enhanced [67]	Infrastructureless	No	No	No	Statistics	Simulation
	REP [81]	Infrastructureless	No	Yes	No	ASS	Simulation
	CPN [71]	Infrastructureless	No	No	No	ASS	Analy-model Simulation
	SlotSwap [82], [8]	Infrastructureless	No	No	Yes	Entropy	Simulation
	PCC [73]	Infrastructureless	No	No	No	ASS ASR	Simulation
	SPCP [84]	Infrastructureless	No	No	No	ASS ASR	Simulation
	DMLP [79], [80]	Infrastructure-based	No	Yes	No	Entropy	Simulation
	TAPCS [85]	Infrastructureless	Yes	No	No	Entropy	Analy-model Simulation
	TRIGGER [83]	Infrastructure-based	No	No	Yes	ASS Entropy ASR	Analy-model
Mix-zone-based	UPCS [63], [64]	Infrastructure-based	Yes	No	Yes	Entropy	Analy-model Simulation
	CMIX [56]	Infrastructure-based	No	Yes	No	Entropy ASR	Simulation
	SocialSpots [62], [40]	Infrastructure-based	No	No	No	ASS	Analy-model Simulation
	VLPZ-based PCS [50], [86]	Infrastructure-based	Yes	No	No	ASS DA	Analy-model Simulation

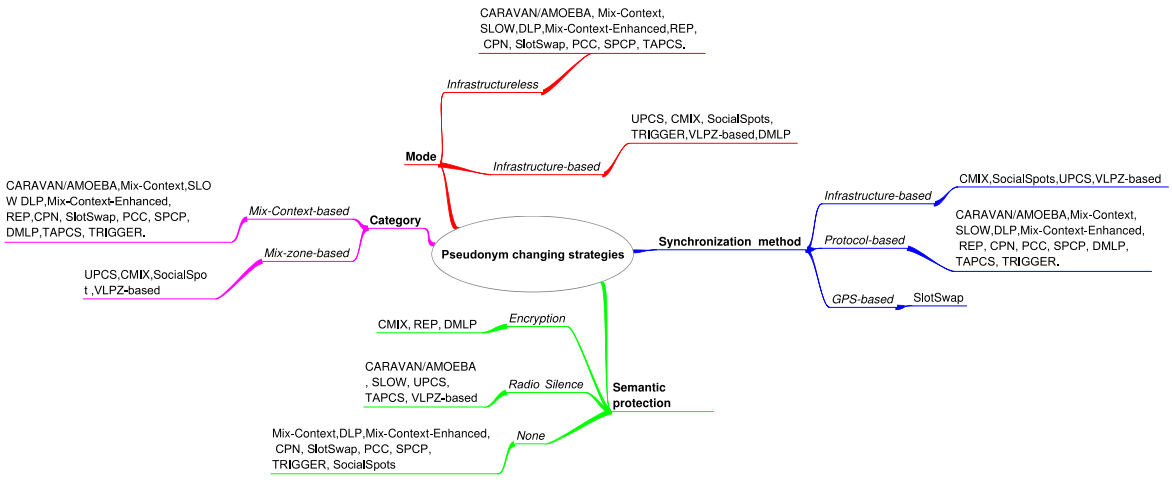

Fig. 14. A graphical summary of existing pseudonym changing strategies for vehicular networks.

adversary. Indeed, as this adversary has the privileges (credentials) to decrypt safety messages, it can then provide a clue to the external adversary to read the contents the safety messages. In addition, encrypting safety messages may not meet with the requirements of VANETs and may introduce a communication overhead due to the messages used to share the encryption keys [56]. On the other hand, because no safety message is broadcasting during the radio silence period, the use of this technique is challenging. Indeed, the radio silence may affect the VANETs' safety-related applications if it is not used properly [89]. However, compared to the encryption technique, the radio silence provides an effective protection against both internal and external passive adversaries, since no safety message is provided to the adversary during the radio silence. Therefore, we argue that the strategies that based on the radio silence are more effective against the semantic linking attack compared to the strategies that based on the encryption.

Besides this, the technique of the exchanging of pseudonyms was used in SlotSwap [8]. This technique is

TABLE V
A REVIEW OF PSEUDONYM CHANGING STRATEGIES

Strategy	**Synchronization Method**	**Semantic Protection Technique**	**Syntactic Protection Against**	**Semantic Protection Against**
CMIX	Infrastructure-based	Encryption	External only	External only
CARAVAN/AMOEBA	Protocol-based	Radio silence	Both	Both
Mix-Context	Protocol-based	None	Both	None
SLOW	Protocol-based	Radio silence	Both	Both
DLP	Protocol-Based	None	Both	None
SocialSpots	Infrastructure-based	None	Both	None
Mix-Context-Enhanced	Protocol-based	None	Both	None
REP	Protocol-based	Encryption	External only	External only
CPN	Protocol-based	None	Both	None
SlotSwap	GPS-based	None	Both	None
DMLP	Protocol-based	Encryption	External only	External only
PCC	Protocol-based	None	Both	None
SPCP	Protocol-based	None	Both	None
UPCS	Infrastructure-based	Radio silence	Both	Both
TAPCS	Protocol-based	Radio silence	Both	Both
VLPZ-based PCS	Infrastructure-based	Radio silence	Both	Both
TRIGGER	Protocol-based	None	Both	None

TABLE VI
A COMPARISON BETWEEN PSEUDONYM CHANGING STRATEGIES

	Privacy Protection		Costs		
Strategy	**Syntactic Linking Protection**	**Semantic Linking Protection**	**Impacts on Safety**	**Overhead**	**Accountability loss**
CMIX	+	+	Yes	Yes	No
CARAVAN/AMOEBA	++	++	Yes	No	No
Mix-Context	++	-	No	No	No
SLOW	++	++	Yes	No	No
DLP	++	-	No	No	No
SocialSpots	+++	-	No	No	No
Mix-Context-Enhanced	++	-	No	No	No
REP	+	+	Yes	Yes	No
CPN	++	-	No	No	No
SlotSwap	++++	-	No	Yes	Yes
DMLP	+	+	Yes	Yes	No
PCC	++	-	No	Yes	No
SPCP	++	-	No	Yes	No
UPCS	+++	++	Yes	No	No
TAPCS	++	++	No	No	No
VLPZ-based PCS	+++	++	No	No	No
TRIGGER	++	-	No	Yes	No

useful, because it limits the number of pseudonyms used by vehicles, which has positive impacts on network performances and vehicles' storage. However, exchanging of pseudonyms without informing the authorities leads to losing the accountability/liability, which is one of the primary security requirements for VANETs. In addition, the overhead

TABLE VII
SYNTACTIC PROTECTION LEVELS

Syntactic Protection Level	Syntactic Protection Against	Synchronization Method
+	External only	*
++	Both	Protocol-Based
+++	Both	Infrastructure-based
++++	Both	GPS-Based

TABLE VIII
SEMANTIC PROTECTION LEVELS

Semantic Protection level	Semantic protection against
+	External only
++	Both

may be introduced, because of the huge number of messages that can be used in the exchange of pseudonyms.

To summarize, Table V reviews pseudonym changing strategies based on the following parameters:

- *Synchronization method:* indicates which method is used to synchronize the pseudonyms changes between vehicles.
- *Semantic protection technique:* indicates which technique is used to temporary hide the safety message's content from the adversary.
- *Syntactic protection against:* indicates against which type of adversary (internal/external), the syntactic protection is provided. "Both" stands for both of the two types.
- *Semantic protection against:* indicates against which type of adversary (internal/external), the semantic protection is provided. "Both" stands for both of the two types.

In Table VI, we compare pseudonym changing strategies. This comparison is based on two axes:

1) *The level of the pseudonyms linking prevention:* this is measured by the ability of the strategy to prevent the syntactic and the semantic linking attacks of pseudonyms. We define four levels for *the syntactic linking protection* based on "Synchronization method" and "Syntactic protection against" parameters (see Table VII). We also define two level for *the semantic linking protection* based on "Semantic protection against" parameter (see Table VIII).
2) *The costs involved in the changing of the pseudonym:* which comprise:
   - *Impacts on road safety:* indicate whether the strategy has negative impacts on road safety or no.
   - *Overhead:* this is expressed in terms of the additional messages that can be used by the strategy to obtain the encryption keys or exchange the pseudonyms for example.
   - *Accountability Loss:* indicates if the strategy leads to the loss of accountability or not.

   A graphical summary of existing pseudonym changing strategies for vehicular networks is also illustrated in Figure 14.

V. LESSONS LEARNED AND RECOMMENDATIONS

An interesting lessons and some recommendations could be concluded from the results and analyses presented in the previous section. First of all, the obtained results strongly depend on the assumed adversary model. The general rule is to assume the strongest possible adversary model in order to propose a powerful protection mechanism. In our analyses, we have considered an adversary model composed of an external global and an internal local passive adversaries with long-term tracking. Analyses show that strategies relying on the radio silence are the most effective to protect against both internal and external passive adversaries. However, the use of radio silence is challenging as discussed in Section VI-A. Fortunately, more options are still available. Indeed, if we assume that the adversary model only consists of an external global passive adversary, the strategies that use the encryption seems suitable to use. Furthermore, if the assumed adversary is external and local with short-term or mid-term tracking, the other strategies could also be applied. Thus, the applied strategy depends on the knowledge of the deployment environment. Specifically, the realistic idea about the power of the adversary model cannot be reached until the deployment of vehicular networks. The requirements and costs of strategies is also important to consider. Indeed: (i) some strategies have requirements such as the availability the roadside infrastructure, and (ii) due to the used protection technique, some strategies have negative costs such as adding an overhead to the communication system and impacting the road safety. The straightforward solution that comes in mind is to allow a dynamic selection strategies. In another words, vehicles dynamically change their strategy according to the context that consists of the adversary model, the availability of requirements and the tolerance of costs. However, since many vehicles are involved in a pseudonym changing strategy, the vehicles' agreement on the strategy to apply could be a major issue. Finally, we believe that the use of the exchange of pseudonyms has a major security issue since the exchange of pseudonyms must be followed by the exchange of the corresponding private keys.

VI. OPEN RESEARCH ISSUES

Several parameters involves to build an effective pseudonym changing strategy. For example, the simultaneous pseudonyms change of a large number of vehicles is required. In addition, the use of the radio silence seems to be inevitable towards an effective strategy. However, although considerable efforts have been made, several open issues are still needing more attention to achieve the aimed strategy. Some of these issues are discussed in the following section.

A. Impact on Road Safety

As discussed in Section IV, the radio silence technique has proved its effectiveness to protect against both external and internal passive adversaries. However, using this technique has negative impacts on safety-related applications [90]. Lefevre *et al.* [89] studied the impact of the radio-silence based pseudonym changing strategies on Intersection Collision Avoidance (ICA) Systems. Their results highlight a positive

correlation between the radio silence duration and the impact on road safety. For example, their simulation results show, in case that the strategy of pseudonym changing proposed by the SAE J2735 standard [91] is used, the radio silence duration should be shorter that two seconds to ensure the well function of the considered ICA application. For this reason, the authors proposed an adaptive pseudonym changing strategy that compromises between privacy and safety. They conclude that the requirements of both safety-related applications and pseudonym changing strategies should be taken into account in the design of each of them.

In the last few years, several researchers start focusing on this issue. The existing works can be divided into two categories. The works of the first category (e.g., [76], [77], [92], [93], and [85]) suggest that vehicles continuously monitor its neighborhood to find a good opportunity to use the radio silence. In the other hand, the works of the second category suggest executing a radio-silence based strategy in places where the impact on road safety is low or null such as signalized intersections [63], [64] and widespread roadside infrastructures [50], [86] (e.g., gas stations, electric vehicles charging stations, and toll booths).

B. Non Cooperative Behavior

The cooperation between vehicles is a key factor on a successful pseudonym changing strategy. However, due to the costs that involve in changing the pseudonym such as the overhead, and the cost of changing and managing the pseudonym, some vehicles may not want to cooperate with the other vehicles. The non-cooperative behavior in pseudonym changing strategy is first studied by Freudiger *et al.* [94]. The authors proposed a game-theoretic model that takes into account the gained payoff and the cost generated by each vehicle while executing the strategy. They demonstrated the existence of the Nash equilibria in both static and dynamic forms of the game within complete and incomplete information. Based on the results of their analysis and simulations, they proposed PseudoGame protocols for an optimal pseudonym changing. The cooperation behavior is studied in [95] using the auction game model as well. However, when we analyzed strategies we found that just few strategies take into account the non cooperative behavior. Indeed Lu *et al.* [40] relied on a simplified game-theoretic to demonstrate the feasibility of the proposed strategy assuming that all vehicles are rational. Ying *et al.* [78], [80] studied the selfish behavior in the DMLP pseudonym changing strategy. They proposed a reputation mechanism to stimulate selfish vehicles to cooperate by changing their pseudonyms in a DMLP. The reputation value of a vehicle is increased each time it cooperates at other vehicle's DMLP. The increase of reputation is computed based on the number of cooperating vehicles at the i^{th} DMLP. The accumulated reputation strength of a vehicle until the i^{th} DMLP is used as a credit when a vehicle requests to create its own DMLP. Indeed, if the accumulated reputation strength R^i is greater or equal to a certain threshold strength of reputation ε, all vehicle that receive the COMMAND message will change their pseudonyms. Otherwise, the decision of a vehicle to cooperate or not depends on: (i) ts current reputation R^j, (ii) its current location privacy level, and (iii) the remaining lifetime of the current pseudonym (T). Indeed (i) if R^j is less than ε, a vehicle has to cooperate to increase its reputation value, (ii) if the location privacy level is the less then recommended level γ the vehicle has to change its pseudonym as well, and (iii) if the remaining life of the current pseudonym is close to (T), the vehicle will change its pseudonym. Otherwise, the vehicle keeps its pseudonym. Boualouache *et al.* [86] also used a reputation based mechanism to motivate rational vehicles to enter the VLPZ. Indeed, as the level of privacy protection mainly depends on the number of vehicles inside the VLPZ, the VLPZ always tries to increase its occupancy. A vehicle is allowed to execute the strategy only if its reputation value is above or equal to a certain threshold (ω) or it has not already refused an invitation form a VLPZ. Indeed, the VLPZ occasionally sends invitations to vehicles to motivate them to enter to it. If a vehicle accepts to enter, its reputation value will be increased. However, if a vehicle refuses, its reputation value will be decreased. The following formulas gives the reputation value $\mathbb{R}_i^j$ of a given vehicle (v_i) after the j^{th} invitation.

$$\mathbb{R}_i^j = \begin{cases} \mathbb{R}_i^{j-1} + |AS|_{t_j} & \text{if v cooperates} \\ \mathbb{R}_i^{j-1} - |AS|_{t_j} & \text{if v defeats and } \mathbb{R}_i^{j-1} \geqslant |AS|_{t_j} \\ 0 & \text{if v defeats and } \mathbb{R}_i^{j-1} < |AS|_{t_j} \end{cases}$$

where $\mathbb{R}_i^{j-1}$ is the old reputation value of v_i. The reputation value of the vehicle increases as much as it cooperates. The increase or the decrease of the reputation value depends on the VLPZ occupancy at t_j, where the time t_j is depended on the decision of v_i.

C. Evaluation Metrics and Techniques

Due to the abstract nature of privacy concept, quantifying the privacy protection level is difficult task to perform. A variety of metrics (e.g., [25], [92], and [96]–[98]) and techniques (e.g., [99]–[103]) have been proposed to evaluate the achieved level of location privacy protection in VANETs. However, finding an unified framework and a comprehensible metric to evaluate and compare pseudonym changing strategies is not yet achieved.

Three initiatives have recently been emerged to propose a simulation framework for evaluating the privacy level in VANETs. Tomandl *et al.* [101] proposed VANETsim an event-driven simulation framework that allows implementing a set of pseudonym changing strategies in an abstract way, i.e., without considering the wireless medium characteristics and communication protocols used in VANETs. Eckhoff *et al.* [100] described a generic design of Veins simulation framework extension devoted to evaluate the pseudonym changing strategies. This extension consists of three main blocks (i) the attacker model block, (ii) the metrics block, and (iii) the scenarios block. This extension is concertized by Emara [104]. Indeed, the authors proposed PREXT (Privacy Extension for Veins VANET Simulator). PREXT adopts the attacker model

proposed in [92], uses most popular privacy metrics and implements seven pseudonym changing strategies.

From a macroscopic view, these efforts seem encouraging. However, with more focus, we believe that more efforts should to be done to evaluate the proposed privacy mechanisms. In particular, the used privacy metrics are general and do not take the context of VANETs into account. We think that the difficulty of the problem is mainly related to the definition of privacy in the context of VANETs.

VII. Conclusion

The pseudonym changing strategy is an important building block of the pseudonym changing approach. All efforts should be made in order to achieve the aimed strategy before the real-word deployment of the pseudonym changing mechanism. In this paper, we surveyed relevant pseudonym changing strategies for VANETs and classified them into two categories. We also identified the strengths and costs generated by the presented strategies. Finally, we highlighted some challenges on the pseudonym changing strategy issue.

References

[1] C. Sommer and F. Dressler, *Vehicular Networking*. Cambridge, U.K.: Cambridge Univ. Press, Nov. 2014.

[2] G. Karagiannis *et al.*, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584–616, 4th Quart., 2011.

[3] C. Sommer, D. Eckhoff, and F. Dressler, "IVC in cities: Signal attenuation by buildings and how parked cars can improve the situation," *IEEE Trans. Mobile Comput.*, vol. 13, no. 8, pp. 1733–1745, Aug. 2014.

[4] Z. Doukha and S. Moussaoui, "An SDMA-based mechanism for accurate and efficient neighborhood-discovery link-layer service," *IEEE Trans. Veh. Technol.*, vol. 65, no. 2, pp. 603–613, Feb. 2016.

[5] R. Kroh, A. Kung, and F. Kargl, "VANETs security requirements final version," Eur. 6th RTD Framework Programme, Paris, France, Tech. Rep. IST-027795, 2010.

[6] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication," *J. Commun. Netw.*, vol. 11, no. 6, pp. 574–588, Dec. 2009.

[7] K. Emara, W. Woerndl, and J. H. Schlichter, "Vehicle tracking using vehicular network beacons," in *Proc. IEEE 14th Int. Symp. World Wireless Mobile Multimedia Netw. (WoWMoM)*, Madrid, Spain, 2013, pp. 1–6.

[8] D. Eckhoff, R. German, C. Sommer, F. Dressler, and T. Gansen, "SlotSwap: Strong and affordable location privacy in intelligent transportation systems," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 126–133, Nov. 2011.

[9] D. Eckhoff, "Privacy and surveillance: Concerns about a future transportation system," in *Proc. 1st GI/ITG KuVS Fachgespräch Inter Veh. Commun. (FG IVC)*, Innsbruck, Austria, Feb. 2013, pp. 15–18.

[10] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[11] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

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

[13] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proc. 4th ACM Int. Workshop Veh. Ad Hoc Netw.*, 2007, pp. 19–28.

[14] F. Dressler, F. Kargl, J. Ott, O. K. Tonguz, and L. Wischhof, "Research challenges in intervehicular communication: Lessons of the 2010 Dagstuhl seminar," *IEEE Commun. Mag.*, vol. 49, no. 5, pp. 158–164, May 2011.

[15] *IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages*, IEEE Standard 1609.2-2013, pp. 1–289, Apr. 2013.

[16] *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*, ETSI Standard 102 941 v1.1.1, 2012.

[17] P. Papadimitratos *et al.*, "Architecture for secure and private vehicular communications," in *Proc. IEEE 7th Int. Conf. ITS Telecommun. (ITST)*, 2007, pp. 1–6.

[18] E. Schoch, F. Kargl, T. Leinmüller, S. Schlott, and P. Papadimitratos, "Impact of pseudonym changes on geographic routing in VANETs," in *Proc. 3rd Eur. Conf. Security Privacy Ad Hoc Sensor Netw. (ESAS)*, 2006, pp. 43–57.

[19] D. Eckhoff and C. Sommer, "Driving for big data? Privacy concerns in vehicular networking," *IEEE Security Privacy*, vol. 12, no. 1, pp. 77–79, Jan./Feb. 2014.

[20] E. B. Hamida, H. Noura, and W. Znaidi, "Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures," *Electronics*, vol. 4, no. 3, pp. 380–423, 2015.

[21] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.

[22] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, 2014.

[23] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, 1st Quart., 2014.

[24] I. Wagner and D. Eckhoff, "Technical privacy metrics: A systematic survey," *arXiv preprint arXiv:1512.00327*, 2015.

[25] I. Wagner and D. Eckhoff, "Privacy assessment in vehicular networks using simulation," in *Proc. Win. Simulat. Conf. (WSC)*, Savannah, GA, USA, Dec. 2014, pp. 3155–3166.

[26] *An Example of VANETs*. Accessed: Jul. 20, 2017. [Online]. Available: http://www.brunel.ac.uk/cedps/electronic-computer-engineering/research-activities/wncc/student-profiles/shariq-mahmood-khan

[27] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the united states," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.

[28] ETSI. (2012). *302 663 (v1. 2.0): Intelligent Transport Systems (ITS); Access Layer Specification for Intelligent Transport Systems Operating in the 5 GHz Frequency Band*. [Online]. Available: http://www.etsi.org/deliver/etsi_en/302600_302699/302663/01.2.00_20/en_302663v010200a.pdf

[29] *Information Technology Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments*, IEEE standard 802 11p, 2010.

[30] R. A. Uzcategui, A. J. De Sucre, and G. Acosta-Marum, "Wave: A tutorial," *IEEE Commun. Mag.*, vol. 47, no. 5, pp. 126–133, May 2009.

[31] U. Nations. (1948). *The Universal Declaration of Human Rights(Article 12)*. [Online]. Available: http://www.claiminghumanrights.org/udhr_article_12.html

[32] J. van den Hoven, M. Blaauw, W. Pieters, and M. Warnier, "Privacy and information technology," in *The Stanford Encyclopedia of Philosophy*, E. N. Zalta, Ed. 2016. [Online]. Available: https://plato.stanford.edu/entries/it-privacy/

[33] H. Dok, R. Echevarria, and H. Fu, "Privacy issues for vehicular ad-hoc network," in *Communication and Networking* (Communications in Computer and Information Science), vol. 56. Berlin, Germany: Springer, 2009, pp. 370–383.

[34] H. Lim and T. Chung, "Privacy treat factors for VANET in network layer," in *Soft Computing in Information Communication Technology* (Advances in Intelligent and Soft Computing), vol. 158. Berlin, Germany: Springer, 2012, pp. 93–98.

[35] F. Schaub, Z. Ma, and F. Kargl, "Privacy requirements in vehicular communication systems," in *Proc. Int. Conf. Comput. Sci. Eng. (CSE)*, vol. 3. Vancouver, BC, Canada, 2009, pp. 139–145.

[36] B. K. Chaurasia and S. Verma, "Conditional privacy through ring signature in vehicular ad-hoc networks," *Trans. Comput. Sci. XIII*, vol. 6750, pp. 147–156, 2011.

[37] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

[38] A. Pfitzmann and M. Hansen. (Aug. 2010). *A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management v0.34*. [Online]. Available: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

[39] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[40] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, Jan. 2012.

[41] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE 27th Conf. Comput. Commun. (INFOCOM)*, Apr. 2008, p. 9.

[42] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, "Certificate revocation list distribution in vehicular communication systems," in *Proc. ACM MobiCom VANET*, San Francisco, CA, USA, Sep. 2008, pp. 86–87.

[43] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," in *Proc. 4th Eur. Conf. Security Privacy Ad Hoc Sensor Netw. (ESAS)*, 2007, pp. 129–141.

[44] D. B. Reid, "An algorithm for tracking multiple targets," *IEEE Trans. Autom. Control*, vol. 24, no. 6, pp. 843–854, Dec. 1979.

[45] J. Petit, D. Broekhuis, M. Feiri, and F. Kargl, "Connected vehicles: Surveillance threat and mitigation," in *Proc. Black Hat Europe*, Nov. 2015, pp. 1–12.

[46] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *Proc. 7th Int. Conf. Wireless Demand Netw. Syst. Services (WONS)*, 2010, pp. 176–183.

[47] R. E. Kalman, "A new approach to linear filtering and prediction problems," *J. Basic Eng.*, vol. 82, no. 1, pp. 35–45, 1960.

[48] R. J. Fitzgerald, "Development of practical PDA logic for multitarget tracking by microprocessor," in *Proc. IEEE Amer. Control Conf.*, Seattle, WA, USA, 1986, pp. 889–898.

[49] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in VANETs," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Tokyo, Japan, 2009, pp. 1–8.

[50] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "VLPZ: The vehicular location privacy zone," in *Proc. 7th Int. Conf. Ambient Syst. Netw. Technol. (ANT)*, 2016, pp. 369–376.

[51] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1569–1589, Oct. 2007.

[52] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *Proc. 2nd Int. Conf. Privacy Enhancing Technol. (PET)*, 2003, pp. 41–53.

[53] C. Díaz, "Anonymity metrics revisited," in *Proc. Dagstuhl Seminar Anonymous Commun. Appl.*, vol. 05411. 2005.

[54] M. Feiri, J. Petit, and F. Kargl, "The case for announcing pseudonym changes," in *Proc. 3rd GI/ITG KuVS Fachgespräch Inter Veh. Commun. (FG IVC)*, 2015, pp. 31–33.

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

[56] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-zones for location privacy in vehicular networks," in *Proc. 1st Int. Workshop Wireless Netw. Intell. Transp. Syst. (Win ITS)*, 2007, pp. 1–7.

[57] M. Humbert, M. H. Manshaei, J. Freudiger, and J.-P. Hubaux, "On the optimal placement of mix zones: A game-theoretic approach," in *Proc. 16th ACM Conf. Comput. Commun. Security*, 2009, pp. 324–337.

[58] B. Palanisamy and L. Liu, "MobiMix: Protecting location privacy with mix-zones over road networks," in *Proc. IEEE 27th Int. Conf. Data Eng. (ICDE)*, Hanover, Germany, 2011, pp. 494–505.

[59] X. Liu *et al.*, "Traffic-aware multiple mix zone placement for protecting location privacy," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, 2012, pp. 972–980.

[60] X. Liu and X. Li, "Privacy preservation using multiple mix zones," in *Location Privacy Protection in Mobile Networks*. New York, NY, USA: Springer, 2013, pp. 5–30.

[61] Y. Sun, B. Zhang, B. Zhao, X. Su, and J. Su, "Mix-zones optimal deployment for protecting location privacy in VANET," *Peer Peer Netw. Appl.*, vol. 8, no. 6, pp. 1108–1121, 2015.

[62] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. S. Shen, "Anonymity analysis on social spot based pseudonym changing for location privacy in VANETs," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2011, pp. 1–5.

[63] A. Boualouache and S. Moussaoui, "S2SI: A practical pseudonym changing strategy for location privacy in VANETs," in *Proc. Int. Conf. Adv. Netw. Distrib. Syst. Appl. (INDS)*, 2014, pp. 70–75.

[64] A. Boualouache and S. Moussaoui, "Urban pseudonym changing strategy for location privacy in VANETs," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 24, nos. 1–2, pp. 49–64, 2017.

[65] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & swap: User-centric approaches towards maximizing location privacy," in *Proc. 5th ACM Workshop Privacy Electron. Soc. (WPES)*, Alexandria, VA, USA, 2006, pp. 19–28.

[66] M. Gerlach and F. Güttler, "Privacy in VANETs using changing pseudonyms—Ideal and real," in *Proc. IEEE 65th Veh. Technol. Conf. (VTC Spring)*, Apr. 2007, pp. 2521–2525.

[67] J. Liao and J. Li, "Effectively changing pseudonyms for privacy protection in VANETs," in *Proc. 10th IEEE Int. Symp. Pervasive Syst. Algorithms Netw. (ISPAN)*, 2009, pp. 648–652.

[68] J.-H. Song, V. W. S. Wong, and V. C. M. Leung, "Wireless location privacy protection in vehicular ad-hoc networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2009, pp. 1–6.

[69] 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.

[70] Y. Pan and J. Li, "An analysis of anonymity for cooperative pseudonym change scheme in one-dimensional VANETs," in *Proc. IEEE 16th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, 2012, pp. 251–257.

[71] Y. Pan and J. Li, "Cooperative pseudonym change scheme based on the number of neighbors in VANETs," *J. Netw. Comput. Appl.*, vol. 36, no. 6, pp. 1599–1609, 2013.

[72] Y. Pan, Y. Shi, and J. Li, "A novel and practical pseudonym change scheme in VANETs," in *Proc. Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput.*, 2017, pp. 413–422.

[73] B. Ying and D. Makrakis, "Pseudonym changes scheme based on candidate-location-list in vehicular networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2015, pp. 7292–7297.

[74] K. Sampigethaya *et al.*, "Caravan: Providing location privacy for VANET," in *Proc. Embedded Security Cars (ESCAR)*, 2005, pp. 1–15.

[75] 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.

[76] K. Emara, W. Woerndl, and J. Schlichter, "CAPS: Context-aware privacy scheme for VANET safety applications," in *Proc. 8th ACM Conf. Security Privacy Wireless Mobile Netw. (WiSec)*, 2015, pp. 1–12. [Online]. Available: http://doi.acm.org/10.1145/2766498.2766500

[77] K. Emara, W. Woerndl, and J. Schlichter, "POSTER: Context-adaptive user-centric privacy scheme for VANET," in *Proc. 11th Int. Conf. Security Privacy Commun. Netw. (SecureComm)*, Dallas, TX, USA, Oct. 2015, pp. 590–593, doi: 10.1007/978-3-319-28865-9_37.

[78] B. Ying and D. Makrakis, "Reputation-based pseudonym change for location privacy in vehicular networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2015, pp. 7041–7046.

[79] B. Ying, D. Makrakis, and H. T. Mouftah, "Dynamic mix-zone for location privacy in vehicular networks," *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1524–1527, Aug. 2013.

[80] 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.

[81] A. Wasef and X. Shen, "REP: Location privacy for VANETs using random encryption periods," *Mobile Netw. Appl.*, vol. 15, no. 1, pp. 172–185, 2010.

[82] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, 2010, pp. 174–181.

[83] S. Wang, N. Yao, N. Gong, and Z. Gao, "A trigger-based pseudonym exchange scheme for location privacy preserving in VANETs," *Peer Peer Netw. Appl.*, vol. 10, no. 2, pp. 1–13, Mar. 2017.

[84] H. Weerasinghe, H. Fu, S. Leng, and Y. Zhu, "Enhancing unlinkability in vehicular ad hoc networks," in *Proc. IEEE Int. Conf. Intell. Security Informat. (ISI)*, 2011, pp. 161–166.

[85] A. Boualouache and S. Moussaoui, "TAPCS: Traffic-aware pseudonym changing strategy for VANETs," *Peer Peer Netw. Appl.*, vol. 10, no. 4, pp. 1008–1020, 2017.

[86] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "Towards an efficient pseudonym management and changing scheme for vehicular ad-hoc networks," in *Proc. IEEE Glob. Commun. Conf. USA (GLOBECOM)*, 2016, pp. 1–7.

[87] W. Lewandowski, G. Petit, and C. Thomas, "Precision and accuracy of GPS time transfer," *IEEE Trans. Instrum. Meas.*, vol. 42, no. 2, pp. 474–479, Apr. 1993.

[88] H. Zarza, S. Yousefi, and A. Benslimane, "RIALS: RSU/INS-aided localization system for GPS-challenged road segments," *Wireless Commun. Mobile Comput.*, vol. 16, no. 10, pp. 1290–1305, 2016.
[89] S. Lefevre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of V2X privacy strategies on intersection collision avoidance systems," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2013, pp. 71–78.
[90] G. P. Corser, A. Arenas, and H. Fu, "Effect on vehicle safety of nonexistent or silenced basic safety messages," in *Proc. Int. Conf. Comput. Netw. Commun. (ICNC)*, 2016, pp. 1–5.
[91] *Dedicated Short Range Communications (DSRC) Message Set Dictionary*, SAE Standard j2735 v1.1.1, 2009.
[92] K. Emara, W. Woerndl, and J. Schlichter, "On evaluation of location privacy preserving schemes for VANET safety applications," *Comput. Commun.*, vol. 63, pp. 11–23, Jun. 2015.
[93] K. Emara, W. Woerndl, and J. Schlichter, "Context-based pseudonym changing scheme for vehicular adhoc networks," *arXiv preprint arXiv:1607.07656*, 2016.
[94] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "Non-cooperative location privacy," *IEEE Trans. Depend. Secure Comput.*, vol. 10, no. 2, pp. 84–98, Mar./Apr. 2013.
[95] 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.
[96] G. P. Corser, H. Fu, and A. Banihani, "Evaluating location privacy in vehicular communications and applications," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 9, pp. 2658–2667, Sep. 2016.
[97] Z. Ma, F. Kargl, and M. Weber, "A location privacy metric for V2X communication systems," in *Proc. IEEE Sarnoff Symp. (SARNOFF)*, Mar./Apr. 2009, pp. 1–6.
[98] Z. Ma, "Location privacy in vehicular communication systems: A measurement approach," Ph.D. dissertation, Faculty Eng. Comput. Sci., Univ. at Ulm, Ulm, Germany, 2011.
[99] D. Eckhoff, "Simulation of privacy-enhancing technologies in vehicular ad-hoc networks," Ph.D. dissertation, Dept. Comput. Sci., Erlangen-Nurnberg Univ., Erlangen, Germany, 2016.
[100] D. Eckhoff, M. Protsenko, and R. German, "Toward an open source location privacy evaluation framework for vehicular networks," in *Proc. IEEE 80th Veh. Technol. Conf. (VTC Fall)*, Sep. 2014, pp. 1–2.
[101] A. Tomandl, D. Herrmann, K.-P. Fuchs, H. Federrath, and F. Scheuer, "VANETsim: An open source simulator for security and privacy concepts in VANETs," in *Proc. Int. Conf. High Perform. Comput. Simulat. (HPCS)*, Jul. 2014, pp. 543–550.
[102] A. Tomandl, F. Scheuer, and H. Federrath, "Simulation-based evaluation of techniques for privacy protection in VANETs," in *Proc. IEEE 8th Int. Conf. Wireless Mobile Comput. Netw. Commun. (WiMob)*, Oct. 2012, pp. 165–172.
[103] D. Förster, F. Kargl, and H. Löhr, "A framework for evaluating pseudonym strategies in vehicular ad-hoc networks," in *Proc. 8th ACM Conf. Security Privacy Wireless Mobile Netw. (WiSec)*, New York, NY, USA, 2015, pp. 1–6.
[104] K. Emara, "Poster: PREXT: Privacy extension for veins VANET simulator," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2016, pp. 1–2.

Abdelwahab Boualouache, photograph and biography not available at the time of publication.

Sidi-Mohammed Senouci, photograph and biography not available at the time of publication.

Samira Moussaoui, photograph and biography not available at the time of publication.