This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

Pseudonym Schemes in Vehicular Networks: A Survey

Jonathan Petit, Florian Schaub, Michael Feiri, and Frank Kargl

***Abstract*—Safety-critical applications in cooperative vehicular networks require authentication of nodes and messages. Yet, privacy of individual vehicles and drivers must be maintained. Pseudonymity can satisfy both security and privacy requirements. Thus, a large body of work emerged in recent years, proposing pseudonym solutions tailored to vehicular networks. In this survey, we detail the challenges and requirements for such pseudonym mechanisms, propose an abstract pseudonym lifecycle, and give an extensive overview and categorization of the state of the art in this research area. Specifically, this survey covers pseudonym schemes based on public key and identity-based cryptography, group signatures and symmetric authentication. We compare the different approaches, give an overview of the current state of standardization, and identify open research challenges.**

***Index Terms*—Anonymity, authentication, ITS, intelligent transport systems, privacy, pseudonym, unlinkability, untraceability, V2X communications, VANET, vehicular ad-hoc networks**

I. Introduction

The automotive and transportation industry is currently developing smart vehicles that are safer, more efficient, greener, and more comfortable. As part of Intelligent Transportation Systems (ITS), these future vehicles will increasingly rely on Information and Communication Technology (ICT) to achieve such goals. The use of wireless communications has been proposed to increase the line-of-sight of drivers and vehicle's sensors, and thus, will play a vital role for increasing the contextual awareness of vehicles. To enable this cooperative awareness, vehicles involved in Vehicle-to-Vehicle (V2V) communications will broadcast position beacons. This potentially endangers the privacy of drivers, as an eavesdropper could create detailed mobility patterns of individual drivers. Therefore, anonymous vehicular communications is desirable, however, a certain level of linkability between a vehicle's individual broadcast messages is required for system operation. Pseudonym schemes have emerged to address these privacy, security, and system requirements. In recent years, a large body of literature has emerged that investigates the issue of pseudonymity in vehicular networks. Our goal is to provide a consolidated overview of the research in this area, and thus, guide future research, as well as support standardization and future deployment activities with a consistent treatment of the issue.

J. Petit, M. Feiri and F. Kargl are with the Services, Cybersecurity and Safety Research Group, University of Twente, P.O. Box 217, 7500 AE Enschede, the Netherlands. E-mail: {j.petit, m.feiri, f.kargl}@utwente.nl.

F. Schaub conducted parts of this work while at the Institute of Media Informatics, University of Ulm, Albert-Einstein-Allee 11. He is now with the School of Computer Science, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, United States. E-mail: fschaub@cs.cmu.edu.

F. Kargl is with the Institute of Distributed Systems, University of Ulm, Albert-Einstein-Allee 11, 89081 Ulm, Germany. E-mail: frank.kargl@uni-ulm.de.

Manuscript received XXX; revised XXX.

A. Relation to existing surveys

Despite the large body of literature on pseudonym schemes for vehicular networks, there is so far no comprehensive survey on the different research directions for providing pseudonymity to individual vehicles in vehicular ad hoc networks. A number of surveys exists that focus mainly on the communication aspects of vehicular communication. Willke et al. [1] classify V2V applications and describe their communication requirements. Karagiannis et al. [2] complete the previous survey by describing the basic characteristics and requirements of vehicular ad hoc networks (VANET), and the standardization efforts and ITS projects current in 2011. Al-Sultan et al. [3] provide another view on VANET architecture components, wireless access technologies, VANET characteristics, VANET applications, and simulation tools. Despite providing extensive analysis of the whole field of vehicular communications, those surveys only treat security and privacy briefly.

Riley et al. [4] provide a survey of authentication schemes for VANETs, and discuss some privacy-preserving schemes. However, their work lacks an analysis of the privacy provided by those schemes. Moreover, the authors do not investigate the pseudonym lifecycle and do not analyze each authentication scheme from the pseudonym point of view. They also only consider anonymity, which is a subset of privacy requirements, as we will discuss in Section III-C. Biswas et al. [5] provide a brief survey on pseudonymous authentication. Nevertheless, their work only considers Public Key Infrastructure (PKI), one group signature protocol (namely GSIS [6]), and symmetric cryptography schemes, all dated from 2007. Their comparison is not extensive and needs to be completed. Krumm [7], on the other hand, offers an excellent overview of location privacy research in various areas, but without specifically treating V2X communication. In contrast, we focus specifically on the unique privacy challenges of V2X communication and survey proposed pseudonymous authentication solutions specific to this field.

B. Methodology

The main goal of this survey is to provide a comprehensive and structured overview of different research directions and approaches for anonymity and pseudonymity in vehicular networks. This survey aims at (i) providing an overview of the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

state-of-art solutions for pseudonymity in vehicular networks for security and privacy researchers; (ii) educating the broader VANET research community on the issues of security and privacy in vehicular networks; and (iii) serving as a basis for discussion for regulators and standardization bodies.

We first give an introduction to Vehicular Networks to motivate the emergence of security and privacy approaches for those systems in Section II. In Section III, we outline the adversary model underlying pseudonymous authentication in vehicular networks, and detail metrics to evaluate an adversary's effectiveness. In Section III, we provide a consistent set of definitions for pseudonymity and digital pseudonyms, before discussing the different requirements that necessitate pseudonymity in vehicular networks and affect mechanisms for its realization. In Section IV, we derive an abstract pseudonym lifecycle from these requirements, which is applicable to the majority of pseudonym approaches for vehicular networks and facilitates comparison and discussion of different pseudonym approaches.

In Sections V-VIII, we discuss existing pseudonymous authentication schemes for vehicular networks. The presented schemes are grouped according to their general approach towards pseudonymity. We distinguish four major categories that reflect the dominant research directions: pseudonym schemes based on asymmetric cryptography and PKIs (Sec. V), identity-based cryptography schemes (Sec. VI), group signature schemes (Sec. VII), and schemes based on symmetric cryptography (Sec. VIII). However, such categories are not hard-edged as many schemes employ aspects from multiple categories to achieve enhancements over previously proposed schemes. We discuss such schemes in the category that best fits the scheme's underlying rationale, while highlighting how they draw from other categories to obtain certain characteristics.

For each category, we use the abstract pseudonym lifecycle proposed in Section IV to model the basic rationale shared by the schemes of that category and discuss different approaches taken by those schemes. We also highlight specific challenges and research issues of each category. The abstract pseudonym lifecycle allows direct comparison of schemes in one category, but also facilitates comparison between different categories and their schemes. The pseudonym lifecycle also allows us to place narrow contributions addressing only specific aspects of the lifecycle in better relation to other work. Thus, we achieve a coherent overview of the current state of the art research on pseudonyms and pseudonymous authentication in vehicular communications, despite the variety of proposed approaches.

Following the categorization and presentation of different schemes, we compare the different categories in Section IX. To provide an astute survey, Section X gives an overview on the role of pseudonym mechanisms in current standardization and deployment activities. In Section XI, we raise challenges for future research. Section XII concludes the survey with a summary of our findings.

II. Intelligent Transportation Systems and Vehicular Networks

Development of standards for vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communications (globally called V2X) is in progress worldwide. Major activities involve IEEE 802.11p [8], the IEEE 1609 working group,[1] the work of the ETSI Technical Committee on ITS,[2] and the ISO Technical Committee 204.[3]

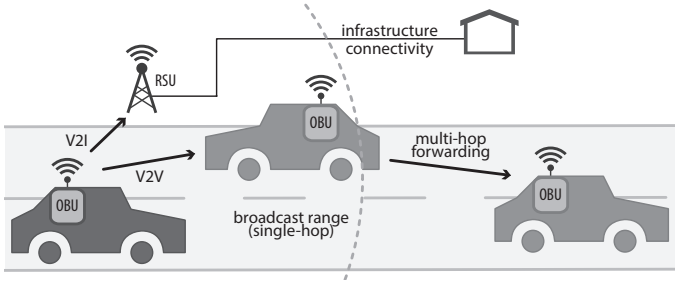

Fig. 1. System model for vehicular communications.

While certain applications may rely on cellular communication, such as LTE, for V2I communication, applications with real-time requirements, such as many efficiency and safety applications, will be based on dedicated short-range communication (DSRC) between vehicles. Examples of safety-related applications include Local Danger Warning (LDW), Electronic Emergency Braking Light (EEBL) and Cooperative Collision Avoidance (CCA) [9]. These applications are all based on direct information exchange between vehicles. In the envisioned ITS architecture [10], a vehicle's On-Board Unit (OBU) will broadcast information like its position, speed, and heading to neighboring vehicles to create mutual awareness between proximate vehicles of the local traffic situation. This communication is typically broadcast periodically at 1–10 Hz in so-called beacon messages (also known as Cooperative Awareness Message in Europe [11] and Basic Safety Message in the US [12]). Specific event-triggered messages may also be re-broadcast by receiving vehicles in order to extend spatial coverage with multi-hop communication. Examples are warning vehicles of accidents or the end of a traffic jam on the road ahead. Roadside units (RSUs), placed alongside the road, can additionally support message dissemination, e.g., at intersections, and enable communication with infrastructure services. Figure 1 summarizes the discussed system model for vehicular communications. Schoch et al. [13] give a complete overview of envisioned communication patterns for vehicular communication.

As many applications of vehicular networks are directly related to driving safety, it is of high importance to properly implement security. Otherwise attackers could send out spoofed or forged information that may result in incorrect warnings to drivers or even wrong automatic reactions of cars in the case of automated driving applications. Accidents, injuries, or even fatalities might be direct results [14]. For example, a fabricated or replayed EEBL message could cause the receiving vehicle to brake suddenly in order to avoid a nonexistent obstacle. Therefore, security mechanisms for ITS are of paramount importance to enable safety applications

[1] http://standards.ieee.org/develop/wg/1609_WG.html
[2] http://www.etsi.org/website/technologies/intelligenttransportsystems.aspx
[3] http://www.iso.org/iso/iso_technical_committee?commid=54706

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

based on V2V communication. Initial proposals by Gollan and Meinel [15] and El Zarki et al. [16] suggested to use digital certificates to identify vehicles and authenticate messages in vehicular communications, which generated an influx of research [17, 18, 19, 20, 21, 22, 23]. Current standardization efforts mainly follow an approach based on asymmetric cryptography. Messages are authenticated with Elliptic Curve Digital Signature Algorithm (ECDSA) signatures [24], and a corresponding public key certificate is attached, which is issued to vehicles by a Certificate Authority (CA).

However, this approach challenges the privacy of drivers. Beacon messages convey exact location information of vehicles. While a certificate's abstract identifier does not necessarily identify a specific driver, a private car is typically only driven by few individuals. For example, a typical German household owns one car that is driven by two to three persons [25]. By knowing the position of a vehicle, one can likely ascertain the whereabouts of the vehicle's drivers. Hoh et al. [26] find that there is a strong correlation between start and end points of vehicle trips and the vehicle owner's home address. Thus, knowing where a vehicle travels can reveal a potential home address, which suffices to identify the driver.

Consequently, beacon information must be treated as personal data and protected accordingly. The European Data Protection Supervisor, Peter Hustinx, takes this position in his opinion on the European Commission's ITS Directive [27] by stating that: *"Some of the information that will be processed through ITS is aggregated—such as on traffic, accidents, and opportunities—and does not relate to any individual, while other information is related to identified or identifiable individuals and therefore qualifies as personal data within the meaning of Article 2(a) of Directive 95/46/EC."*

Therefore, vehicle tracking and attacks revealing vehicle or driver identities must be prevented to preserve privacy. In 2006, Gerlach [28] provides a first basic approach to protect privacy in V2V. Any vehicle or driver identifiers are removed from messages and certificates. Instead, vehicles are assigned an abstract identifier—a pseudonym—which is embedded in certificates. Such a certified pseudonym enables authentication while preserving the anonymity of vehicle and driver. However, a static pseudonym is not sufficient in case of vehicular communication, because a single vehicle could still be identified and tracked based on a time series of eavesdropped messages [29]. Indeed, eavesdropped messages can be correlated with specific vehicles or even drivers based on reoccurring travel patterns, e.g., commuting trips. This problem can be addressed by not only assigning a single pseudonym to a vehicle, but a set of pseudonyms. A vehicle then uses a pseudonym only for a limited amount of time before switching to another pseudonym. However, equipping vehicles with multiple pseudonyms can actually negatively impact security, if their use is not limited. A vehicle could use multiple pseudonyms in parallel to spoof multiple independent vehicles. A selfish driver could use such a *sybil attack* [30] to gain free roads by fabricating a nonexistent traffic jam.

Granting anonymity to vehicles also clashes with potential desires by law enforcement agencies and other stakeholders to ensure accountability and non-repudiation, e.g., to identify a vehicle based on recorded messages at an accident scene.

To address the complex relationship between application requirements, privacy protection, anonymity, authentication, accountability, and non-repudiation requirements, a multitude of pseudonymity mechanisms have been proposed that aim to balance these divergent requirements. Not all of these mechanisms follow the signature-certificate scheme outlined above (detail in Section V); some apply group signatures (see Section VII) or use identity-based cryptography (see Section VI) instead. There is also a large body of literature that investigates when and how to change pseudonyms in order to achieve a sufficient level of privacy.

III. Privacy in Vehicular Networks

Westin [31] defines *privacy* as an individual's right *"to control, edit, manage, and delete information about them[selves] and decide when, how, and to what extent information is communicated to others."* Placed in the context of public roads, the expectation of individual privacy is already limited by license plates. Each vehicle equipped with a license plate is uniquely identifiable, and thus, could be easily stalked. Moreover, the introduction of Automatic License Plate Reader (ALPR) technology [32] is used to take digital pictures of vehicle license plates in order to recognize and record vehicle license plate numbers. It employs optical license plate detection software to seek out and recognize the presence of license plates in view of an ALPR camera. Once an ALPR system recognizes the presence of a license plate, the plate number is automatically extracted, at which point it can be recorded. ALPR systems can also leverage GPS technology to record the date and time, as well as relative location of all recorded images. Therefore, ALPR enables vehicles tracking, and can reveal personal details such as how frequently you visit the doctor, a bar, or whether you go to church [33]. Without V2X communication, potential privacy implications are limited in scale by the visibility of the license plate [34]. Due to their broadcast nature, V2X communications could however enable long-term, remote and large-scale tracking. Hence, we should design V2X communication such as they do not make global and remote surveillance easier.

Placed in the context of vehicular networks, privacy is the claim that the user of the vehicle is able to control which information is sent by the OBU (even in case of forwarding), and the lifetime of such information. Anonymity is a common method to protect privacy of individuals, as well as a goal in itself [35]. Pfitzmann and Köhntropp [36] define *anonymity* as "the state of being not identifiable within a set of subjects", which can be provided in communication systems by *pseudonyms*.

Before discussing the role of pseudonymous authentication in vehicular communications, we take a more general view on pseudonyms and discuss how they protect privacy. We further provide an adversary model and discuss potential attacks on pseudonym schemes. Digital pseudonyms were originally introduced by Chaum in the context of providing anonymity for electronic transactions as "a public key used to verify signatures made by the anonymous holder of the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

corresponding private key" [37]. Pfitzmann and Hansen [38] generalize this notion. They characterize a digital pseudonym as "a bit string which [...] is unique as identifier (at least with very high probability) and suitable to be used to authenticate the holder's items of interest relatively to his/her digital pseudonym, e.g., to authenticate his/her messages sent." From these two definitions, it follows that a pseudonym, or pseudonymous credential, should be useable for authentication, but must not contain any personal identifiable information that could link to the pseudonym holder's real identity. Thus, a pseudonym allows authentication of a specific entity without knowing the holders's real identity. Consequently, all actions authenticated with the same pseudonym are linkable to each other because a pseudonym constitutes a unique identifier. This has the advantage of enabling bidirectional communication, which is not feasible with fully anonymous approaches. However, a holder can use a set of pseudonyms to achieve unlinkability of pseudonymous actions. The holder can either change pseudonyms over time to break linkability of actions in one context, or use different pseudonyms for different contexts [38]. In an extreme case, a different pseudonym could be used for each action. Bohli and Pashalidis [39] show that a system providing pseudonymity does not leak any information about the set of users beyond the linking relation between pseudonym and associated actions. In particular, an adversary does not learn the size of the user set.

If accountability is a desired characteristic, the secret part of the pseudonym must only be known to the pseudonym holder, and sharing of secret credentials between users must be de-incentivized in order to achieve non-repudiation. Accountability denotes that a specific action can be unambiguously assigned to an individual user in a fair protocol [40]. In a pseudonymous authentication scheme, accountability can be supported by enabling traceability. The ability to trace a pseudonym to the pseudonym holder's identity must be restricted to privileged authorities. Pseudonymity is preserved for normal operations; only under specific conditions a specific authority or set of authorities are able to trace, or resolve, a pseudonym to an identity. In systems that support accountability, pseudonymity becomes conditional, i.e., under specific conditions (typically misbehavior) pseudonymity can be revoked. A straightforward approach for conditional pseudonymity is offered by identity escrow schemes in which an escrow authority acts as a mediator for pseudonym generation [41]. After authenticating a node's unique identity, the authority issues pseudonyms to that node (note that in the remainder of this paper the term *node* refers to an entity involved in the network, e.g., a vehicle or RSU) and retains escrow information that enables mapping the issued pseudonyms to the pseudonym holder's identity, if required. The downside of this basic approach is obvious: the escrow authority has full knowledge of pseudonym-identity mappings. Approaches exist to enhance privacy in conditional pseudonymity by requiring multi-tier escrow or multi-party cooperation for pseudonym-identity resolution, as will be discussed later on.

A. Potential Attacks and Adversary Model

Attacks on pseudonymous authentication schemes target the anonymity and unlinkability of a pseudonym's scheme. Wernke et al. [42] classify privacy attacks as *single position attack*, *context linking attack*, *multiple position and context linking attack*, *multiple position attack*, and *compromised TTP*. For example, an adversary can start a *location tracking attack* (named *multiple position attack* in [42]), in which he/she collects location samples and tries to correlate them to determine the path of an individual vehicle [43, 44]. This attack jeopardizes the anonymity of the driver and the unlinkability of pseudonyms. The adversary can also run an *identity revealing attack* (named *context linking attack* in [42]) where he/she correlate information about the environment (stopped vehicle on the road) and messages (warnings, beacons) to identify an individual vehicle. While tracking of vehicles is also already possible with camera systems and license plate recognition, vehicular communication systems would significantly decrease the required effort of tracking vehicles on a large scale.

A vehicular network is a complex distributed system where an adversary can perform different types of attacks based on his/her capabilities. In this survey, we use the adversary model proposed by Raya and Hubaux [20]. Thus, the following types of adversary are considered:

- *Global* vs. *Local*: This dimension defines the range of an adversary. A local adversary has a limited number of eavesdropping stations to deploy in the network. For example, eavesdropping stations deployed at road intersections have a coverage area large enough to detect mobile nodes entering and exiting the intersection [45].
- *Active* vs. *Passive*: A passive adversary cannot inject or modify messages, but can collect pseudonyms at every intersection where he/she has an eavesdropping station.
- *Internal* vs. *External*: The internal adversary is an authenticated member of the network that can communicate with other members. The external adversary is considered by the network members as an intruder and hence is limited in the diversity of attacks. Nevertheless, we assume he/she can eavesdrop the communication.

Based on this model, a Global Passive Adversary (GPA), which can be either internal or external, can locate and track any vehicle in a region-of-interest by eavesdropping its broadcasts [46, 29]. The GPA can leverage the deployed infrastructure (e.g. RSUs) and utilizes the adversarial units (e.g. RSUs) deployed to estimate the locations of all broadcasts in the region-of-interest. A GPA could have incentive in establishing mobility patterns to distribute personalized advertizing or perform data mining techniques [47]. Hence, a GPA can be governments or large organizations (e.g. road operators, certificate authorities). For example, the police could use beacons (e.g. Cooperative Awareness Message [11], Basic Safety Message [12]) to calculate driving behavior and issue speeding tickets.

Compared to the GPA, a Local Passive Adversary (LPA), which can also be either internal or external, is limited in its

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

location tracking capability in a region-of-interest, since it can only leverage the deployed infrastructure for eavesdropping and estimating locations of vehicle broadcasts. Hence, the region over which the LPA can track vehicles is dependent on the vehicle transmission range and the distance between any two successive deployed units (e.g. RSUs). This adversary can be one individual that has incentive in controlling a specific region such as his/her neighbourhood. For example, an employer could overhear communications from vehicles on the company parking lot, and after distinguishing which vehicle-identifier belongs to which employee, he/she could automatically collect exact arrival and departure times.

Thus, the main motivation of GPAs and LPAs is to break the location privacy of users or identify users. Pseudonyms hamper those attacks. Therefore, adversaries want to (i) link multiple pseudonyms to identify pseudonym change and being capable of tracking a vehicle; (ii) link pseudonym to an identity to break user's anonymity.

An *active* adversary is dependent on the implemented pseudonym lifecycle. The goal of an active adversary could be to block pseudonym change, force pseudonym change, or disturb the pseudonym management. For example, an *active internal* adversary could disturb a targeted group by enforcing revocation of the group key (see Section VII for a detailed example of such an attack). Another active attack is the *pseudonym depletion attack*, where an attacker aims at forcing pseudonym change repeatedly until the targeted vehicle's pseudonym set is depleted. In this situation, the victim will attempt to refill its pseudonym set by contacting a trusted third party (see Sec. IV), which is not always accessible.

B. Adversary effectiveness

Re-identification is a well-researched issue that concerns manipulating databases to determine the identity of individuals whose information is recorded as records within a de-identified database through data linkage techniques. Golle and Partridge [48] analyze data from the U.S. Census and show that for the average person, knowing their approximate home and work locations – to a block level – identifies them uniquely. Oh et al. [49] demonstrate vehicle re-identification using data recorded from a simple induction loop sensor. Charbonnier et al. [50] compare the performances of different vehicle re-identification methods using a vehicle's tridimensional magnetic signature recorded with a single three-axis magnetic sensor. These examples show that re-identification of users is an indicator of adversary effectiveness.

However, in vehicular networks, the privacy mainly starts with *location privacy*. Beresford and Stajano [51] define location privacy as "the ability to prevent other parties from learning one's current or past location". This definition captures the idea that the person whose location is being measured should control who can know it. It also recognizes that past location information is important to protect [7]. While real time location could enable an attacker to find you, past data could help him or her discover your identity, your home address, and your activities. Duckham and Kulik [52] refine the concept of location privacy by defining it as "a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others".

In this context, we use the level of location privacy to assess the effectiveness of the aforementioned attacks. Since location can be specified as a single coordinate, one way to measure location privacy is by how much an attacker might know about this coordinate [7]. To characterize the level of location privacy, researchers use different metrics, namely the size of the anonymity set [53, 54, 55], the entropy [44, 56, 57, 58], and the adversary's tracking uncertainty [59, 60, 61, 46] (see Section XI-C for more detail).

For instance, Hoh and Gruteser [62] quantify location privacy as the expected error in distance between a person's true location and an attacker's uncertain estimates of that location. Duckham and Kulik [63] define "level of privacy" as the number of different location coordinates sent by a user with a single location-based query. More points mean more ambiguity, and hence more privacy. The goal of their system is to be as ambiguous as possible while still getting the right answer for a point-of-interest query. In introducing k-anonymity for location privacy, Gruteser and Grunwald [64] use k to represent the level of privacy. Entropy is the privacy quantifier used by Beresford and Stajano [51]. They show how an attacker could use behavioral probabilities (e.g., a u-turn is less likely than going straight ahead) to attach probabilities to the problem of linking changing pseudonyms over time. Hoh et al. [26] quantify location privacy as the duration over which an attacker could track a subject. "Time to confusion" measures how long it will take until an attacker will become confused about a subject's track as the subject seeks to obfuscate his or her location by omitting measured samples.

C. Privacy and Pseudonym Requirements in Vehicular Networks

The potential attacks define the requirements that need to be taken into account by pseudonym schemes. The main privacy requirements are to remain unlinkable and anonymous. However, privacy requirements must be balanced with security requirements and VANET characteristics as we discussed in Section I. Therefore, Schaub et al. [65] identify the following privacy requirements:

- Minimum disclosure: The amount of information that a user reveals in communication should be kept to the minimum, i.e., no more information than required for normal functionality of V2X applications.
- Conditional Anonymity: A sender of a message should be anonymous within a set of potential senders, the anonymity set of the message. As a driver should be identified in case of law enforcement (identity resolution), only conditional anonymity is possible in vehicular networks.
- Unlinkability: Unlinkability requires that the relations between two or more items of interest (e.g. pseudonyms) cannot be linked.
- Distributed resolution authority: The capability of identity resolution should be distributed between authorities so

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

that cooperation of a number of distinct authorities is required to link an anonymous credential to an individual.
- Perfect forward privacy: Resolution of one credential to an identity should not reveal any information that decreases unlinkability of other credentials of the same user.

The main privacy requirements anonymity, unlinkability, and minimum disclosure, all support each other in some way. Distributed resolution authority and perfect forward privacy do not prevent accountability, but they constrain its extent to an appropriate level. Both support minimum disclosure by ensuring that identity resolution reveals no more information than required for accountability. Perfect forward privacy also supports unlinkability by restricting the extent of linking information that can be gained from identity resolution.

After discussing how pseudonyms protect privacy, we now identify requirements that pseudonyms should follow in order to ensure privacy requirements in vehicular networks.

- Time-limited: To prevent location tracking a pseudonym has to be time-limited. This time limit is ensured by the signed certificate that accompanies the pseudonym.
- Uniqueness: To avoid multiple vehicles to use the same (short-term) identifier, each pseudonym has to be unique. This uniqueness is provided by the underlying cryptographic scheme used to generate the pseudonym.
- Availability: A new pseudonym has to be always available for the vehicle in case of pseudonym change. This can be ensured by storing a large set of pseudonyms in the OBU.
- Pseudonym change block: The ability to block pseudonym change is needed to ensure resilience against attacks (see Section IX-f) and safety level (see Section XI-E).
- Link to other identifiers: When a pseudonym is changed, all the other identifiers used by the same vehicle have to be changed as well. For example, in the ETSI Reference Architecture [66], the geonetworking identifier is derived from the pseudonym.

IV. Abstract Pseudonym Lifecycle

As a result of the tension between these requirements, a multitude of pseudonym schemes have been proposed for vehicular networks. The proposed schemes and their underlying cryptographic mechanisms seem highly divergent at first, yet, the requirements imposed by vehicular communications lead to an abstract pseudonym lifecycle, which is similar for most pseudonym approaches for vehicular networks. The main purpose of a pseudonym is to authenticate the sender as a valid vehicle. This can either be achieved by explicitly certifying a sender as a vehicle, or implicitly by ensuring that only valid vehicles are capable of performing a certain action, e.g., a group signature.

In vehicular communications, pseudonyms pass through a common abstract pseudonym lifecycle resulting from the requirements discussed above. Depending on the specific pseudonymous authentication scheme, some of the actual lifecycle phases may diverge from our abstract lifecycle model. However, the phases outlined in the following can be found in almost all pseudonymous authentication schemes surveyed by us. Figure 2 gives an overview of the phases of the abstract pseudonym lifecycle: *issuance*, *use*, *change*, *resolution*, and *revocation*. Pseudonym issuance must already take pseudonym resolution and pseudonym revocation into account. Those phases in turn inherently depend on the measures taken in the pseudonym issuance process to be effective. Pseudonym use and pseudonym change influence each other and also depend on how pseudonyms are issued or obtained by vehicles. Some of the phases are also optional, e.g., not all schemes foresee or support pseudonym resolution or revocation. In the following, we define and discuss each phase and point out their specific challenges.

1) Pseudonym Issuance: Almost all pseudonymous authentication schemes for vehicular communications assume that a vehicle has a unique digital identifier. This vehicle id (VID) can be seen as a signed certificate that allows to unambiguously authenticate a vehicle. Similar to the vehicle identification number (VIN), which is embossed onto the vehicle chassis by the manufacturer, the VID is a long-term identifier assumed to be pre-installed in a vehicle's OBU [67]. The VID could be issued alongside the vehicle registration and license plate by a vehicle registration authority, such as the department of motor vehicles (DMV). Therefore, the VID is also referred to as an electronic license plate (ELP) [17]. Although the VID is required for pseudonym issuance by most pseudonym schemes, the issuance of the VID itself is typically not considered part of the pseudonym scheme or pseudonym lifecycle, because they are separable processes.

In the pseudonym issuance process, the unique VID is used to authenticate the vehicle's OBU as an actual vehicle OBU to ensure that only valid vehicles can obtain pseudonyms and thus participate in vehicular communications. For pseudonym issuance, two major approaches can be distinguished: *third-party issuance* and *self issuance*.

The majority of approaches relies on third-party issuance, whereby pseudonyms are created by a pseudonym issuing authority. Depending on the scheme, this entity may also consist of multiple sub-entities, which are referred to by a variety of names such as *certificate authority (CA)*, *pseudonym provider (PP)*, or just *trusted authority (TA)*. The ETSI TC ITS security architecture [68] refers to them as *enrollment* and *authorization authorities*. The role of pseudonym issuing authority is commonly assigned to infrastructure-based entities (namely CA, PP), RSUs, or split between both. In either case, a pseudonym issuing authority authenticates the vehicle with its VID, verifies the vehicle's eligibility to obtain pseudonyms (i.e., the vehicle's VID is valid and has not been revoked), and then issues some pseudonym credentials (see Section IV-2). Depending on the scheme, either a request-reply pattern is used to issue certified credentials or credentials are jointly computed.

The pseudonym issuing authority may retain escrow information to enable pseudonym-identity resolution later on. In that case, the authoritative entity gains the ability to revoke privacy of individual vehicles by linking pseudonyms back to VIDs. This either requires considerable trust in the pseudonym issuing authority when simple pseudonym-identity mappings

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

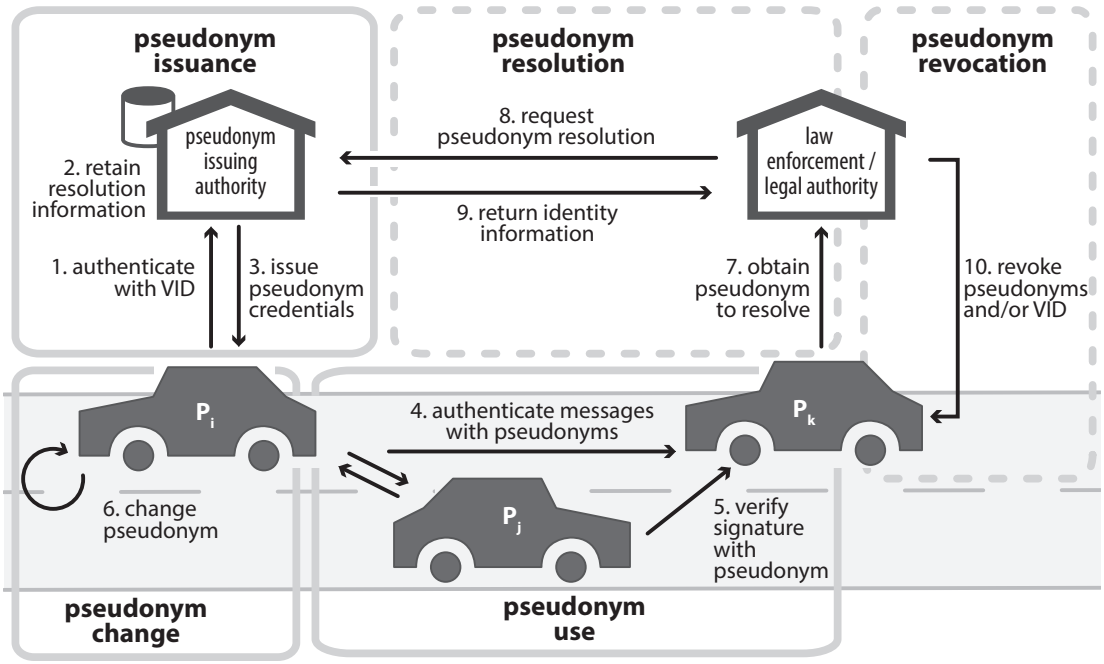

Fig. 2. Abstract pseudonym lifecycle for vehicular networks.

are stored, or requires traceability mechanisms that restrict pseudonym resolution capabilities. Retained resolution information must be well protected to ensure that this information cannot be compromised by attacks against the authority's infrastructure [43]. The resolution and revocation phases are discussed in detail in Sections IV-4 and IV-5.

Pseudonyms are typically assigned an expiry date or validity period. Validity periods or short expiry dates limit the number of pseudonyms available to a vehicle at any given time in order to prevent Sybil attacks. The unlinkability property of pseudonyms prevents receivers from knowing that these messages originated from a single node without performing additional plausibility checks, such as position verification [17]. Thus, the adversary could try to propagate a specific viewpoint in the network to obtain an advantage on the road. For example, a greedy driver could simulate congestion on a stretch of road in order to clear the path ahead [22].

As pseudonyms should not be reused after pseudonym changes, as well as expiry of pseudonyms, an OBU will eventually require fresh pseudonyms. Some approaches favor pre-loading of a large number of pseudonyms sufficient for a couple of years, e.g., between inspection intervals [69]. Other approaches argue for occasional pseudonym refills with respect to intermittent connectivity with pseudonym issuing authorities [70]. The frequency of pseudonym refills depends on pseudonym change rate and pseudonym validity periods.

In contrast to third-party issuance, pseudonym self-issuance has the advantage that a vehicle can perform issuance and generation of pseudonyms autonomously once the vehicle's OBU has been initialized accordingly. However, Sybil attacks are generally harder to prevent in these schemes due to the level of autonomy. Where applicable, self-issuance schemes are discussed alongside schemes based on third-party issuance in subsequent sections.

2) Pseudonym Use: Once a vehicle has obtained pseudonyms it can engage in vehicular communication with other vehicles or infrastructure nodes. Pseudonym use entails two steps: *authentication* (i.e., signing) of outgoing messages and *verification* of received messages.

The authentication of the vehicle's own messages allows other nodes to authenticate the sender as a vehicle with valid credentials. Message integrity must be protected to prevent modification of messages in transit. The message authentication scheme must also provide replay protection. Sender authentication, message integrity, and replay protection essentially corroborate the reliability of received information, which may then be used for safety critical decision making [65]. Note that a valid vehicle would still be able to report false data and thus complementary security mechanisms that verify consistency of data are needed [71].

Typically, pseudonymous authentication schemes employ either asymmetric signatures or message authentication codes. On the receiver side, sender authentication entails verification of the validity of the employed pseudonym. A pseudonym must have been issued by a trusted authority or through verifiable self-issuance and must not be expired or revoked. Online validity verification with the support of backend services is assumed to be unfeasible due to intermittent connectivity with road-side infrastructure, bandwidth constraints, and real-time requirements of cooperative safety applications [72]. Thus, all required verification information must be available locally. For example, schemes based on asymmetric cryptography need to attach pseudonym certificates to messages in order to enable signature verification by receivers (see Section V). At the same time, communication overhead for security functions must be kept as low as possible to facilitate efficient and scalable use of the wireless medium [73].

Another challenge in pseudonym use is the inherent asym-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

metry between creating authenticating information for outgoing messages and verification of received messages. Typically, a vehicle must verify considerably more messages than it sends [74, 75]. For example in periodic beaconing, vehicles may send beacon messages with frequency r Hz. Assuming n neighboring vehicles in reception range a vehicle must verify approximatively $n \times r$ msg/s. Thus, verification of messages and pseudonym credentials must be highly efficient in order to support applications with real-time requirements.

Pseudonyms can only be meaningful credentials if associated key material is securely stored inside vehicle OBUs and cannot easily be extracted or transferred to other nodes. For this reason, the integration of hardware security modules (HSM) or tamper-proof devices (TPD) in OBUs has been proposed for secure key storage and management [76]. Hardware protection of credentials is also seen as an approach to prevent Sybil attacks by making only a limited set of pseudonym credentials available for parallel use via the tamper-resistant HSM.

3) Pseudonym Change: Actions performed under one pseudonym can be linked to each other, due to the mentioned characteristics of pseudonyms. Thus, in order to prevent the linkability of actions, the actions must be performed under different pseudonyms, i.e., a vehicle must change pseudonyms over time. An adversary could then only link a limited number of messages. In order to be effective, pseudonym changes must encompass all network layers [77]. When changing to a new pseudonymous authentication credential, application, protocol, and network identifiers, such as IP or MAC addresses, must all be changed simultaneously to avoid trivial linking between old and new pseudonym. Another important aspect is the necessity of having neighboring vehicles when performing a pseudonym change. As shown in Figure 3, changing the pseudonym when alone is not sufficient for confusing an observer, if that observer is able to monitor locations before and after the area in which the pseudonym change occurred (i.e., the observer will be able to link the new pseudonym Z to vehicle A). Multiple vehicles changing their pseudonyms simultaneously are required to provide an anonymity context to enable an effective pseudonym change.

The frequency of pseudonym changes depends on the desired level of privacy, i.e., what change rate is considered sufficient to prevent adversaries from deriving driving and movement patterns of individuals. The precise nature of this relationship is still being investigated. Topics of active research are also how, where, and in what kind of situations pseudonyms should be changed in order to be effective [78]. Pseudonym changes must not interfere with safety applications [79], but must also be effective to prevent tracking based on vehicle trajectories and coordinates in beacon messages [29] or radio fingerprinting [80]. Proposed schemes vary between the different general categories, with a major focus of research on pseudonym change strategies for public key-based schemes.

4) Pseudonym Resolution (optional): While the previous steps concern all participants of a vehicular network, pseudonym resolution is only relevant for holding misbehaving nodes accountable. Law enforcement representatives might capture messages including pseudonyms from misbehaving nodes and pose a pseudonym resolution request to the issuing authority or pseudonym provider to obtain the pseudonym holder's VID. The authority verifies the eligibility of the request and can divulge the pseudonym holder, if the pseudonymous authentication scheme supports traceability, and respective escrow information has been retained during pseudonym issuance.

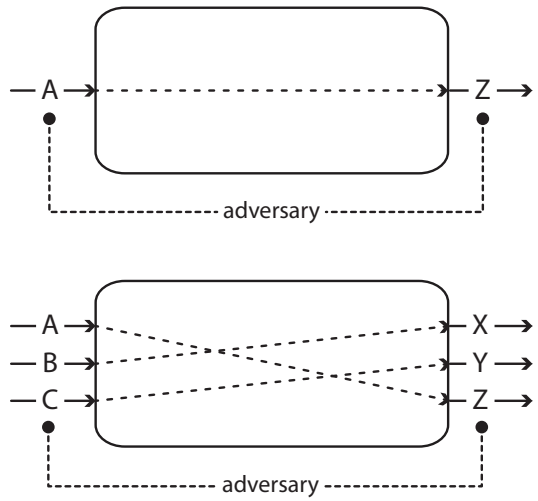

Fig. 3. Necessary context for effective pseudonym change. A single vehicle changing its pseudonym does not prevent linkability of pseudonyms.

While in the simplest case pseudonym resolution could be realized as a database lookup, more advanced resolution schemes have been proposed to enhance privacy by restricting resolution capabilities. Proposals by Fischer et al. [81], Schaub et al. [82], Bißmeyer et al. [83] and others include the separation of pseudonym issuing and pseudonym resolution authorities, providing forward and backward privacy, and the use of threshold cryptography or secret sharing schemes to require cooperation of multiple parties and, thus, enforcing that linking information is only accessible if all parties agree on the necessity of pseudonym resolution in the given case.

While many pseudonym schemes foresee resolution capabilities on a technical level, the legal and societal implications of such capabilities can still not be determined. Especially in Europe, the legality and requirement for conditional pseudonymity in future vehicular networks has been highly debated in recent years [27]. Thus, at this point it remains unclear if future vehicular networks will be mandated to support pseudonym resolution or be prohibited from doing so.

5) Pseudonym Revocation (optional): Misbehaving or faulty nodes may need to be revoked from the vehicular network to ensure proper performance and operation of the network. Commonly, node revocation entails revocation of the node's authentication credentials, i.e., its pseudonyms, VID, or both. If only specific pseudonyms are revoked, one must accept the possibility that the corresponding vehicle may possess further pseudonyms to continue communication with. If all pseudonyms should be revoked, they must be somehow linkable through additional revocation information to determine that they all belong to the same pseudonym holder. This can considerably weaken the privacy provided by pseudonyms.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

The decentralized nature and large scale of vehicular networks makes distribution of up-to-date revocation information a major challenge for effective pseudonym and node revocation [84]. Thus, instead of distributing revocation information, e.g. via certificate revocation lists (CRLs), some schemes rely on passive revocation. Pseudonyms are issued with very short lifetimes requiring frequent pseudonym refills with pseudonym providers. If a node is to be revoked, the node's long-term identity (e.g., the VID) is revoked and further pseudonym refill requests are denied. In this case, a revoked vehicle may still participate in the network until it runs out of valid pseudonyms. Typical approaches for pseudonym and node revocation will be discussed in each section. Note that Figure 2 shows an abstraction of the revocation process. Indeed, like in the pseudonym resolution phase, the revocation might involve multiple entities.

A. Discussion

The outlined pseudonym lifecycle summarizes the general operation of pseudonym systems in vehicular networks. Each lifecycle phase introduces specific research challenges. All these aspects need to be taken into account in order to provide viable pseudonymous authentication mechanisms. However, due to the number of challenges and the involved complexity, many contributions focus either only on a subset of the pseudonym lifecycle and very specific problems, or propose architectures that acknowledge but do not fully address all named challenges.

B. Categorization of Pseudonym Schemes

Looking at the means of achieving pseudonymity, the schemes differ in what cryptographic mechanisms they employ. Four major categories can be distinguished for pseudonymity in vehicular networks. Schemes based on *asymmetric cryptography* (see Section V) aim for PKI-oriented privacy solutions. Pseudonyms are typically represented by public key certificates without identifying information. To facilitate verification by receiving vehicles, pseudonym certificates must be sent along with messages. Schemes based on *identity-based cryptography* (see Section VI) extend this idea but remove the need of explicit public key certificates by deriving public keys from identifiers. This reduces communication overhead for pseudonym use but introduces new challenges for pseudonym issuance. Pseudonym schemes based on *group signatures* (see Section VII) introduce one public key for a group of vehicles, which enables an entity of a group to produce a signature on behalf of the group, i.e., the signature can be verified with a group-wide public key. The group-based signature scheme provides privacy as signers are anonymous within the group. Group-based schemes reduce the need for pseudonym changes but pose new challenges for pseudonym resolution and revocation. Schemes based on *symmetric cryptography* (see Section VIII) are attractive because of their computational efficiency, but must be cast into protocols that can enable reliable authentication. A receiver should know the secret key (shared between the sender and the receiver) to be able to authenticate the sender. Due to the different challenges posed by each cryptographic paradigm, many solutions combine different mechanisms to achieve more effective schemes.

We discuss and compare each category in Section IX. The pseudonym lifecycle serves as a common structure in the discussion and aids comparison. This two-tiered structure of general cryptographic categories and pseudonym lifecycle allows intuitive categorization and characterization of all currently proposed pseudonym mechanisms for vehicular communications.

V. Asymmetric Cryptography Schemes

Pseudonymous communication can be achieved with traditional public key cryptography schemes by equipping vehicles with a set of public key certificates and corresponding key pairs. The public key certificates are stripped of any identifying information and used as unlinkable pseudonyms. Vehicles sign messages with the secret key of the currently active pseudonym and attach the resulting signature, as well as the corresponding pseudonym certificate, to the message. Receivers can verify a message signature based on the pseudonym certificate, but are unable to determine the sender's VID.

The first propositions to ensure privacy in vehicular networks were based on asymmetric cryptography [15, 16, 17]. Afterwards, this approach has been followed by major initiatives such as the SeVeCom project [85, 86], the IEEE 1609.2v2 standard [67], and the Car-to-Car Communication Consortium [87].

Figure 4 shows the adapted pseudonym lifecycle for asymmetric pseudonym schemes. The corresponding phases of the basic scheme are outlined in the following.

Pseudonym issuance: In asymmetric schemes, the pseudonym issuance process is similar to certificate issuance in a Public Key Infrastructure (PKI). As depicted in Figure 4, Certificate Authorities (CAs) are organized hierarchically. It is typically proposed that CAs manage and issue long-term identity certificates to vehicles while pseudonyms are issued by separate Pseudonym Providers (PP) [85]. Pseudonyms are only valid for a short period of time [88]. As a result, vehicles must request new pseudonyms in certain intervals, which introduces scalability issues. Self issuance approaches have been proposed to remove the recurring need for communication with CAs (see Section V-A). When issuing pseudonyms, a PP authenticates a vehicle by its long-term certificate and may keep the pseudonyms-to-identity mapping as escrow information in case of liability investigation. Privacy enhancements for conditional pseudonymity are discussed in Section V-B.

Pseudonym use: Pseudonyms are used to sign every outgoing packet. Public/private keys of previously obtained pseudonyms may be stored and managed by a Hardware Security Module (HSM), which is tamper-resistant to restrict the parallel usage of pseudonyms [85]. The pseudonym restriction scheme (lifetime, amount of pseudonyms in parallel, etc.) depends on the assurance level of the HSM [89]. For example, the available secure storage space impacts the number of pseudonyms that can be stored in parallel inside the HSM. For signing or encryption tasks only the currently valid pseudonym certificates can be used or those that are exposed for use by the HSM.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

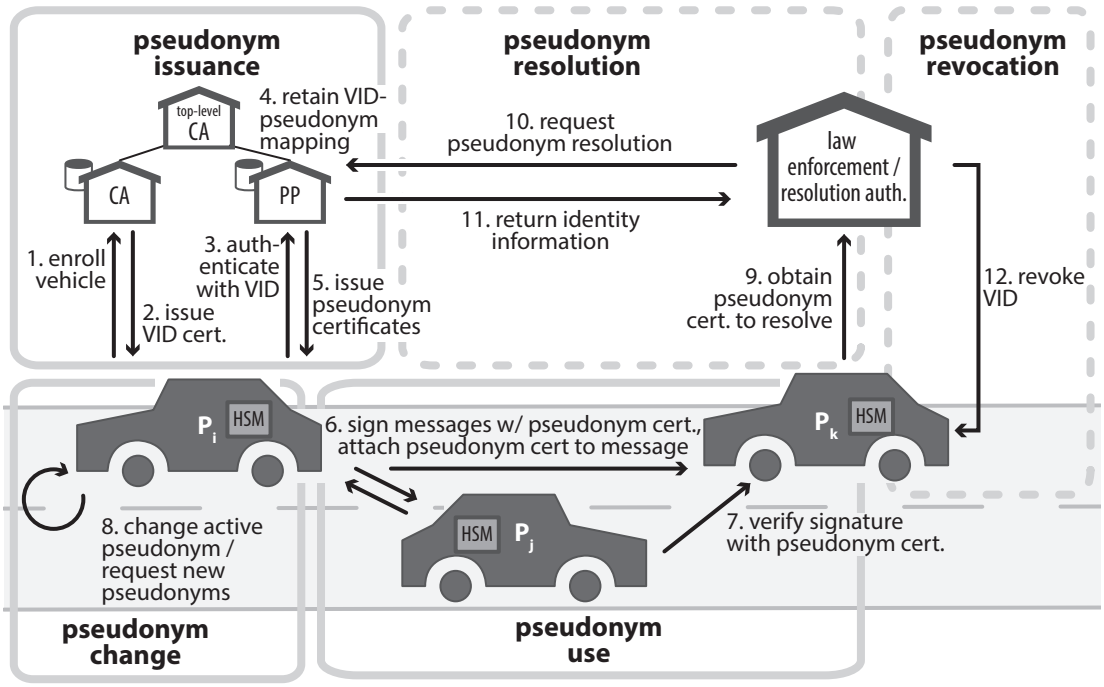

Fig. 4. Pseudonym lifecycle for asymmetric pseudonym schemes.

Pseudonym change: A pseudonym has a lifetime to hamper tracking based on long-term pseudonyms. When a pseudonym expires, the OBU loads a new pseudonym from its store or requests new pseudonyms from the pseudonym provider, which corresponds to pseudonym issuance. In the first case, pseudonyms are changed according to the current context by the vehicle while driving. The employed pseudonym change strategy is crucial to prevent linking of pseudonyms when changing. Numerous pseudonym change strategies have been proposed, which we detail in Section V-C.

Pseudonym resolution: Pseudonym-identity resolution is performed by pseudonym resolution authorities (RAs), which either keep mappings between pseudonyms and VID or have access to such mappings kept by pseudonym providers or CAs [85].

Pseudonym revocation: Revocation of pseudonym certificates is commonly limited to revocation of the VID due to scalability reasons. If the long-term identity is revoked, no new pseudonyms can be obtained. Thus, Certificate Revocation Lists (CRL) must only be distributed to pseudonym providers and not to all individual vehicles. Also, letting OBUs verify pseudonyms of other vehicles against CRLs would not be practical due to high message frequency and potential large CRLs, especially in dense traffic scenarios [90, 91, 92]. On the other hand, by revoking only the VID, a revoked vehicle can continue participating in the network pseudonymously until all its pseudonyms are expired. A solution to this issue is to effectively reduce the lifetime of pseudonyms to very short intervals [93], which in turn increases the frequency of pseudonym refills.

This general approach raises some challenges such as pseudonym change, pseudonym refill, and privacy protection against rogue pseudonym providers. Each issue has been scrutinized by the research community resulting in specialized schemes that address these issues.

A. Self-issued pseudonym certificates

An issue with traditional PKI is that vehicles have to acquire new certified pseudonyms periodically. Zeng [94] proposes the PKI+ approach that enables users to generate CA-certified pseudonyms themselves, thus reducing the communication overhead. Armknecht et al. [95] apply this approach to V2X communication, resulting in a scheme that differs from the general approach in the pseudonym issuance and revocation phases. Concerning the pseudonym issuance, PKI+ does not distribute pseudonyms to vehicles. Instead, vehicles generate their own pseudonyms from their individual master keys, which are chosen by themselves and certified by the CA. PKI+ employs bilinear pairing and zero-knowledge proofs to generate pseudonym and message authentication without originator verification [94]. Since PKI+ enables vehicles to issue their own pseudonyms, no PP is required. If a vehicle's identity has to be resolved, the CA can reconstruct the owner of a pseudonym certificate. Whenever a key has to be revoked, the CA publishes updated system parameters. All nodes must update their keys accordingly in order to continue participation in the vehicular network. The parameters are chosen such that they are unusable for the excluded vehicle, thus impeding it from updating its master key.

In a different approach, Calandriello et al. [96] combine traditional PKI with a group signature scheme to obviate the need for pseudonym refill. Each vehicle holds an individual private key in a group signature scheme with one common group public key. A vehicle uses its group private key to self-sign public key pairs to be used as pseudonyms for message authentication. The resulting message signature can be verified

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

with the publicly known group public key in two steps. First, a receiver verifies the group signature to determine that the message public key has been signed by a legitimate group member without learning the sender's identity. Afterwards, the message signature is verified to check message integrity. The proposed scheme obviates pseudonym refills while maintaining compatibility with common signature generation and verification procedures during pseudonym use. A number of other schemes that completely rely on group signatures are discussed in Section VII.

B. Privacy enhanced pseudonym issuance and resolution

Multiple approaches propose to enhance vehicle privacy against authorities and unwarranted pseudonym resolution based on role separation between Certificate Authorities (CA), Pseudonym Providers (PP), and Registration Authorities (RA). For example, the Crash Avoidance Metrics Partnership (CAMP) and US DOT propose to restrict the CA's ability to link pseudonyms to VIDs by splitting security roles between RA, CA, and Linkage Authorities (LA) [97]. The minimum instantiation requires one RA, one CA, and two LAs. The objective of the design is that no single authority is able to track a vehicle by linking multiple of its certificates. The LAs issue the linkage values (that are used as revocation values) and certificate IDs. As shown in Figure 5, LA1 and LA2 generate a set of CertIDs that are later combined by the CA. The RA acts as an anonymizing mix node which collects and processes OBU requests, shuffles the requests, and forwards individual certificate requests to the CA. The RA also adds another layer of encryption. Batches of certificates are encrypted and RA provides the decryption key upon request by OBU. Finally, CA issues certificates without knowing which certificate belongs to which OBU. In this system, all authorities have to collaborate to link certificates, therefore, enhancing the privacy in pseudonym resolution. But as all authorities are involved in pseudonym issuance, it also increases the communication overhead.

Other approaches employ cryptographic primitives to mandate cooperation between authorities. Fischer et al. [81] propose SRAAC, a pseudonym issuance protocol that uses blind signatures and secret sharing to ensure that multiple authorities are required to cooperate in pseudonym resolution. For pseudonym issuance, a vehicle blinds the public key to be signed and presents shares of it to a number of CAs. Each authority holds a partial secret of a secret key, which is shared between all authorities in a secret sharing scheme. Each authority performs a signature with its partial secret key on the presented blinded key share, returns it to the vehicle, and stores a corresponding partial resolution tag. The vehicle can unblind and combine the received results if at least k of n authorities participate in the issuance process, yielding a certificate which can be verified with a public key common to all authorities. For pseudonym resolution, all generated partial resolution tags are combined. Thus, at least t authorities have to cooperate in order to link a pseudonym to its resolution tag. They compute a joint tag for the presented pseudonym, which then has to be compared to all tags in the database. Although the approach effectively prevents misuse of resolution authority, it also incurs considerable overhead by requiring a number of servers to take part in the certification of a single pseudonym. Furthermore, pseudonym resolution requires comparisons with all tags stored in the revocation database, and therefore, does not scale well with the number of vehicles.

The V-token approach [82] improves scalability by embedding encrypted resolution information inside the pseudonym certificate. A V-token contains a vehicle's VID and a randomization factor encrypted with the common public key of all RAs. The CA signs a vehicle's V-token credentials in a blind signature scheme. A cut-and-choose commitment scheme ensures validity of V-tokens presented for signing. Signed V-tokens are anonymously presented to a PP to obtain a pseudonym. The PP verifies the CA signature before embedding the V-token in the pseudonym certificate. The resulting pseudonym can be used normally for message signing and verification. If pseudonym resolution is required, the V-token is extracted from the pseudonym in question. Multiple RAs must cooperate in a threshold decryption scheme to decrypt the V-token and obtain the VID. While the V-token approach requires less interaction with authorities in the issuance phase, embedding V-tokens increases pseudonym size which incurs communication overhead in pseudonym use.

The TACKs approach [98] uses a group signature scheme to enable anonymous authentication in the pseudonym issuance phase. At initial registration, a vehicle is issued a private key of a group scheme as a long-term identifier. When obtaining new pseudonyms, the vehicle signs the request with that private key. The PP can verify the signature with the group public key (the same for all group members), thus verifying the vehicle's legitimacy without learning its identity. In case of offense, the PP and the group manager can perform pseudonym resolution and the group manager can issue and distribute a revocation token to all PPs that prevents issuance of new pseudonyms to the vehicle. Sha et al. [99] propose to use group-based anonymous authentication for communication with infrastructure servers and services.

All the privacy-preserving schemes presented in this section modify the pseudonym issuance and resolution without altering the message authentication itself.

C. Pseudonym change strategies

A crucial parameter of pseudonym changes is the change rate [88]. Indeed, it impacts the communication, computation, storage overhead, and the level of privacy. Moreover, a simple pseudonym change is not sufficient to evade tracking [29]. Burmester et al. [100] show that a global observer can use Bayesian traffic analysis to re-identify vehicles. Because pseudonym changes must be consistent across layers [77], i.e., a vehicle has to change its MAC and IP address as well, pseudonym changes also affect other protocols and communication patterns [101]. A number of different pseudonym change strategies have been proposed, which we discuss in the following.

1) Fixed time change (periodic): In this strategy, a vehicle changes its pseudonym according to a fixed, periodic schedule.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

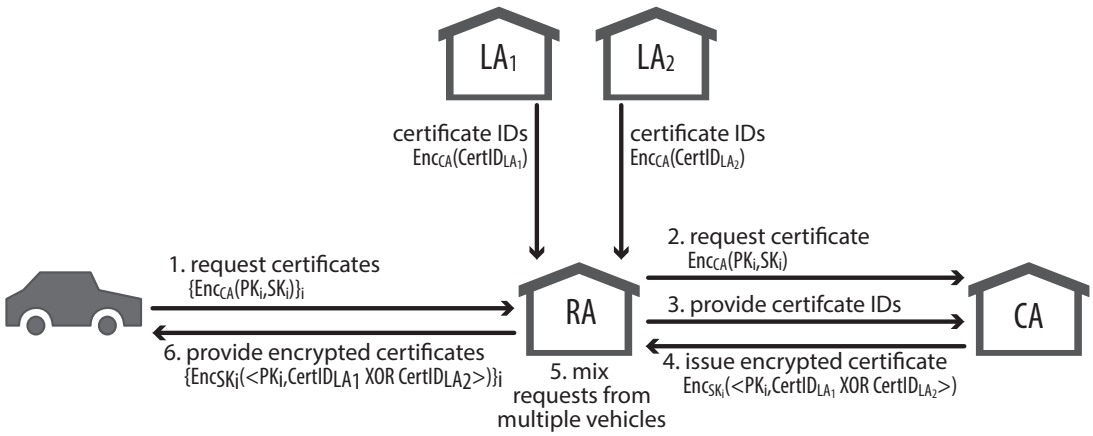

Fig. 5. Security server design overview of CAMP

Eckhoff et al. [102] extend the fixed time change strategy with a *time-slotted pseudonym pool*. Instead of storing a very large amount of pseudonyms, every vehicle maintains a set of pseudonyms (called *pseudonym pool*) which are used at specific time slots. The time slot length determines how often a vehicle changes its pseudonym. A benefit of this strategy is that a vehicle always has a valid pseudonym even if the PP is not reachable. It also introduces an upper bound for pseudonym storage. However, as soon as the attacker knows the period of pseudonym change—which is easy to assess—tracking becomes trivial [103].

2) Random change: In order to solve the issue of fixed periods, vehicles can change their pseudonym randomly [54]. As a result, an adversary cannot predict the next pseudonym change. However, tracking is still possible if only one or few vehicles change pseudonyms at a specific time, because all other neighbors would keep the same identity. Thus, linking of new and old pseudonym of the vehicle that performed the change is still trivial.

3) Silent period between change: In AMOEBA [46] and its predecessor CARAVAN [104] a vehicle remains silent after changing its pseudonym. The silent period makes tracking attacks more complex. Indeed, if a vehicle changes at an intersection and then waits for a short silent period the computation of movement prediction is difficult. The silent period strategy is a good example for a tradeoff between privacy and safety. In [26], the authors proposed a similar concept, named the uncertainty-aware path cloaking algorithm, that can guarantee a specified maximum time-to-confusion and protect against home identification risks. On one hand, vehicle tracking may be hampered, but on the other hand safety applications are jeopardized (see Section XI-E).

4) Vehicle-centric: In a distributed, vehicle-centric approach, vehicles independently determine where and when to change their pseudonyms. Li et al. [105] propose two protocols *Swing* and *Swap*. In *Swing*, vehicles change pseudonyms when changing velocity, i.e. direction and speed. Thus, an adversary cannot utilize the predictability of node movement to correlate node locations before and after an update. Following the same strategy, Eichler [88] adjusts the silent period (called *quiet-time* in his paper) based on a function of the vehicle's mobility. In *Swap*, vehicles exchange their pseudonyms with each other during update with probability 0.5 and then enter a random silent period. However, each cooperating node is only indistinguishable from the node initiating exchange, and not from other cooperating nodes. A silent period is also used in the SLOW protocol [106], but the vehicle only stops beaconing if its speed drops below 30 km/h and changes its pseudonym during such silent periods.

5) Density-based: In this strategy, the vehicle changes its pseudonym based on a function of the current neighbor density. Therefore, it avoids ineffective pseudonym changes when the vehicle is alone. This strategy is called *crowd* by Chaurasia et al. [107, 108, 109]. They propose that a vehicle must update its pseudonym when the crowd size is larger than a threshold.

6) Collaborative (synchronous) change: When changing pseudonyms when no other vehicles are in the vicinity, a vehicle falls easily victim to tracking attacks. A better strategy is for a vehicle to change its pseudonym at the same time as its neighbors. To do so, the vehicle broadcasts a message with a flag set to *change ready* [102]. This strategy creates a context-based *mix-zone* where vehicles in the same area change their pseudonym synchronously. The basic idea of a mix-zone is a spatial area where no location-aware applications are available and where the mobile entities change their pseudonyms. Buttyán et al. [78] use the mix-zone approach to avoid tracking across pseudonym changes. Lu et al. [58, 110, 111] suggest to place mix-zones at social spots (e.g. intersection, traffic light, parking) to increase the number of simultaneous changes. As all vehicles change simultaneously, higher density increases the difficulty for tracking attacks. But this strategy suffers from low privacy protection in low density scenarios [112].

Buttyán et al. [78] analyze the effectiveness of mix-zones and conclude that the optimal frequency of pseudonym change depends on the characteristics of the mix-zone (size, location, number of entry points), which are difficult to determine in practice. They show that changing pseudonyms in mix-zones between RSUs does not suffice to obtain location privacy when an attacker monitors more than 50% of the intersections of the road network. Freudiger et al. [113] propose cryptographic mix zones (CMIX) as a practical implementation of the mix-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

zone notion. The CMIX protocol uses traditional asymmetric cryptography to distribute symmetric keys to establish the cryptographic mix zone within the broadcast distance of a RSU. Inside this zone, vehicles encrypt all broadcast messages with the same symmetric key distributed by the RSU. Intuitively, an adversary cannot link the identities of vehicles since all vehicles use the same key.

Also based on encryption, Wasef and Shen [114] present a scheme for changing pseudonyms that combines the proposals of encrypting messages and user-initiated periods (here called *random encryption periods*). A vehicle that needs to change its pseudonym contacts nearby vehicles and arranges a period of time in which all messages are encrypted and pseudonyms are changed. Once again, an attacker may easily participate in the encryption of messages and therefore can observe the pseudonym change [115]. Gerlach and Guttler [28, 80] propose a *mix-context* approach where vehicles change their pseudonyms when detecting a favorable context. A mix-context is determined by the best opportunity to change pseudonyms (such as favorable number of neighbors, their speed and direction). To identify the best opportunity to change, a threshold for the minimum entropy has to be defined either by the user or by an application.

Freudiger et al. [116] introduced a user-centric model of location privacy to measure the evolution of location privacy over time and evaluated the strategic behavior of mobile nodes with a game-theoretic model, the *pseudonym change game*. They analyzed the *n*-player scenario with complete and incomplete information and derived the equilibrium strategies for each node. The obtained equilibria allow to predict the strategy of rational mobile nodes seeking to achieve location privacy in a non-cooperative environment. This analysis results in the design of the PseudoGame protocols that coordinate pseudonym changes. In order to be independent of a defined area, Weerasinghe et al. [117] propose a synchronized pseudonym change inside a *group* (see Section VII for a definition of *group*).

Despite the different strategies proposed for pseudonym change, it remains unclear which strategy is the most effective in practice. Nevertheless, one could use envision the following dimensions to compare these pseudonym change strategies: privacy level (time to confusion, see Section XI-C), the overhead created (storage, computation, or instability in the communication stack, see Section XI-A), impact on the awareness quality of neighboring vehicles [118]. Accountability in pseudonym exchange environments remains also an open problem. If there is no mapping from a vehicle's long-term identity to all its pseudonyms, or if pseudonyms are used by multiple vehicles, revocation of the entire pseudonym pool is a non-trivial task. We discuss these and other remaining challenges in Section XI.

VI. Identity-based Cryptography Schemes

Identity-based cryptography (IBC) [119] is related to asymmetric cryptography with the significant difference that a node's identifier functions as that node's public key. A corresponding private key is derived from the identifier to sign messages. To verify the signature, knowledge of the sender's identifier is sufficient. An explicit public key or additional certificate are not required. However, to prevent that any node can derive a corresponding private key from a given identifier, only a centralized trusted authority with full knowledge of system parameters is able to generate private keys and assign them to nodes. Thus, a node's authenticity is implicitly guaranteed rather than explicitly stated through a certificate, because only authorized nodes would receive a private key corresponding to a specific identifier.

Compared to conventional PKIs, IBC avoids the use of certificates for public key verification and the exchange of public keys and associated certificates, while providing similar authentication characteristics. The resulting communication and storage efficiency make IBC attractive for authentication in vehicular communications. A drawback is the requirement that a trusted authority must contribute to generate private keys from vehicle identifiers rather than having vehicles generate their own key pairs. The IBC scheme can be extended for pseudonyms by extracting identifiers from arbitrary strings instead of identity information. Most IBC schemes are based on bilinear maps also known as pairings [120] due to computational efficiency. Zhao et al. [121] provide detailed background discussion on IBC and give an overview of IBC applications in mobile ad-hoc networks. In this chapter, we focus on approaches directly pertaining to vehicular networks.

The pseudonym lifecycle for IBC-based pseudonym schemes is very similar to the pseudonym lifecycle for PKI-based schemes (Fig. 6). Notable differences are how pseudonyms are issued and the enhanced role of the PP. The PP, often referred to as trusted authority (TA) in IBC schemes, holds the master secret of the IBC scheme required for private key extraction from identifiers, and also publishes system parameters required for signature verification.

Pseudonym issuance: When a vehicle requests pseudonyms, the TA first authenticates the vehicle to verify that it has not been evicted from the network. For this purpose, some schemes propose to use an asymmetric public key certificate issued for the vehicle's VID [122]. The TA then extracts a private key PSK_i from the vehicle's pseudonym identifier PID_i and sends it to the vehicle. Pseudonymous identifiers could be provided by the vehicle but are usually generated by the TA to encode resolution information. The role of the TA typically corresponds to the PP [123] but can also be decentralized to prevent a single authority from learning all issued private keys [122]. For example, SPECS [124] uses an IBC approach to ensure identity privacy from RSUs as only the TA knows the identity.

Pseudonym use: A pseudonym key pair is represented by the pseudonym identifier PID_i and the private key PSK_i. The vehicle uses PID_i as sender address and signs messages with PSK_i. Receivers verify the signature based on PID_i and the published system parameters. Because the sender identity serves as public key no additional public key certificates need to be attached to messages.

Pseudonym change: Vehicles have to request new pseudonyms periodically, similar to public key schemes discussed in Section V, but less storage space is required because only

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

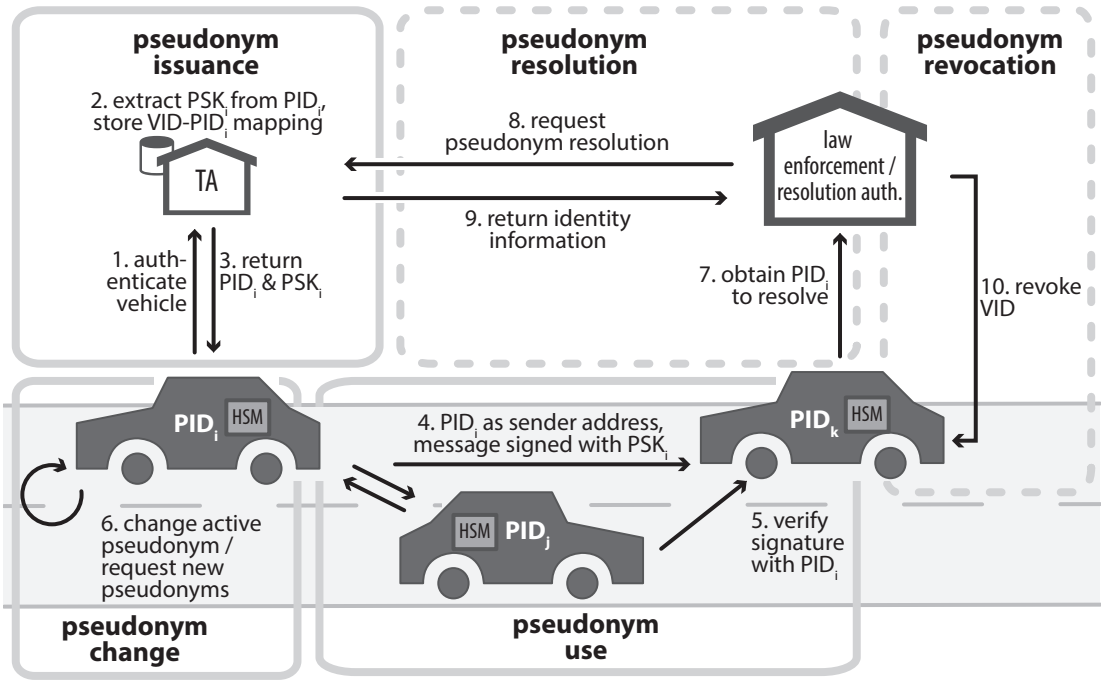

Fig. 6. Pseudonym lifecycle for identity-based cryptography pseudonym schemes.

the pseudonym identifier and the corresponding private key have to be stored. When changing pseudonyms on the road, the same considerations apply as for changing certificate-based pseudonyms. Thus, pseudonym change strategies discussed in Section V-C apply also to IBC schemes. However, Kim et al. [123] (and the fully secure version [125]) propose AnonySign as a signature verification scheme that leverages properties of bilinear maps to obviate the need for disclosure of the sender's pseudonym identifier for signature verification. More specifically, the TA assigns unique identifiers ID_i to vehicles and extracts corresponding private keys (D_i, S_i). A vehicle A computes a signature on a message m with D_A and S_A. A receiver B only needs its own identity ID_B, as well as secret keys D_B and S_B to construct two expressions from the signature components which are equal if, and only if, A's and B's private keys have been extracted with the same secret system parameter t. Thus, the receiver can verify that the signature originated from a legitimate vehicle without learning the vehicle's identifier. Therefore, the scheme does not require periodic changes of pseudonym identifiers. However, the effectiveness of this approach is limited because MAC addresses would still need to be changed according to some strategy in order to prevent tracking.

Pseudonym resolution: Pseudonym-to-identity resolution is trivial if a centralized TA generates all private keys [126]. Similar to asymmetric schemes, the TA could keep identity to pseudonym identifier mappings in the pseudonym issuance step and could link a pseudonym to a VID by searching in this database. AnonySign [123] has also repercussions for pseudonym resolution, because the TA is required to compute signatures for comparison with the secret keys of each registered vehicle to match a signature to a VID—a computationally expensive process. In either case, vehicles must place high trust in the TA that such mappings are stored securely and are not abused. Some schemes have been proposed to mitigate the key escrow problem and enhance privacy (see Section VI-A).

Pseudonym revocation: Revocation is a general issue in IBC schemes [127], because revoking a public key is equivalent with revoking an identity, which is not always feasible. In the vehicular communications context, revoking individual pseudonym identifiers poses similar scalability issues as for PKI certificates. Thus, revocation of a vehicle's VID is more efficient and can be combined with short-lived pseudonym identifiers. Time-dependent identities can be created by adding timing information to identity strings before private key extraction. Receivers can locally verify the validity of the used pseudonym identifier based on the encoded lifetime.

Overall, IBC schemes are efficient in the pseudonym use phase because only the sender identity is required for signature verification. A disadvantage of IBC schemes is the reliance on a centralized trusted authority for private key generation. Furthermore, the authority of identity resolution is also concentrated in the same entity. Due to this centralization of capabilities, the TA poses an attractive target for adversaries with devastating effects in case of successful attacks—a compromised authority could impersonate any OBU and also resolve arbitrary pseudonymous messages to sender identities.

A. The Key Extraction and Escrow Problem

The unconditional trust in the TA is an unrealistic requirement. Most enhancements of the basic IBC pseudonym lifecycle address, both, the key extraction and key escrow problems, usually by decentralizing both capabilities.

Kamat et al. [122] propose to decentralize pseudonym issuance. A central TA (or CA) computes the master secret

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

of the IBC scheme, publishes system parameters, and issues unique VIDs to vehicles. RSUs act as decentralized TAs and issue short-lived pseudonyms. Each RSU receives the system parameters, the master secret, and an individual symmetric key SK_i. After authenticating the vehicle with an asymmetric public key certificate, the RSU creates a pseudonym identifier PID_i by encrypting the VID and a timestamp with its symmetric key SK_i. The result is concatenated with the RSU's identifier ID_{RSU}, a timestamp TS, and a string denoting the pseudonym holder as a vehicle:

$$PID_i = (\text{vehicle} \parallel E_{SK_i}(VID, TS) \parallel ID_{RSU} \parallel TS)$$

The private key PSK_i is subsequently extracted from the pseudonym identifier and the pseudonym key pair (PID_i, PSK_i) is sent to the vehicle. Pseudonym resolution is performed by the central TA which obtains SK_i of the RSU specified in the PID_i and decrypts the unique VID of the pseudonym holder. This proposal reduces the potential for abuse if pseudonym-identity mappings would be leaked. Yet, the risk of impersonation is increased because each RSU holds the master secret for key extraction. In addition, the dependence on RSUs for pseudonym issuance increases overhead.

Sun et al. [128, 129] follow a similar approach by introducing regional TAs for pseudonym issuance. Each regional TA publishes specific system parameters and retains VID-pseudonym mappings. Vehicles registered with the same regional TA can verify each others signatures. In a different region, vehicles use their current pseudonym to request new pseudonyms from the regional TA. The TA retains pseudonym-pseudonym mappings in that case. Thus, resolution requires cooperation of multiple TAs in most cases. A resolution request must also be supported by multiple authorities (e.g., law enforcement) in a threshold signature scheme. Only if enough authorities cooperate, a resolution request obtains a valid signature. While this prevents unjustified identity resolution requests, it does not protect against compromise of regional TAs.

Huang et al. [130] enhance key escrow in a two-step process called PACP. First, vehicles obtain a *ticket* from the central TA. This ticket can be seen as a long-term pseudonym, and is used to obtain *tokens* from RSUs. Those tokens are used by the vehicle to generate pseudonyms for anonymous broadcast communication with other vehicles. Therefore, the RSU only provides the credential and restrictions for the vehicle to generate its pseudonyms, but does not learn any information about the vehicle. An RSU only maps a ticket to a token and the generated pseudonym. To increase vehicle anonymity, the RSU can deliver multiple tokens linked to the same ticket. During the revocation phase, the TA contacts the RSU and obtains the vehicle's ticket. Then, the TA can extract the identity of the vehicle.

Gamage et al. [131] adopt an identity-based ring signature scheme to achieve signer ambiguity. Vehicles obtain a private key for their VID from the TA and use the VID as their public key. To sign a message in the ring signature scheme, a vehicle gathers VIDs of surrounding vehicles resulting in a set L, which is used for signature generation. Utilizing bilinear mappings, signature verification proves that a signature has been generated by one identity in L, but does not reveal which one. Thus, the vehicle's anonymity set is defined by L. For pseudonym resolution, all vehicles identified in L are contacted by the TA and have to compute a proof that only holds if they did not perform the signature in question.

Another approach to address the key escrow problem is to use blind signatures. SECSPP [132] is a non interactive ID-based scheme for V2V that uses member IDs to establish a secure trust relationship and a blind signature scheme for V2I that allows authorized vehicles to anonymously interact with the services from RSUs, without disclosing any contextual information such as precise location or user identity.

To conclude, the core difference between an IBC and a traditional asymmetric algorithm lies in the means of generating the keys. Because the TA is directly responsible for the generation of the private key in an IBC mechanism, there is an inherent escrow facility in the system. Above, we presented techniques that address the key extraction and escrow problem. Although the idea of using a client's identity as the base for key pair is very appealing, it does not come without consequences. Two main issues are revocation and computational overhead (the computation of pairing is time-consuming). We further discuss the issue of computational overhead in Section XI-B.

VII. Group Signature Schemes

The downside of using a changing set of anonymous keys as pseudonyms is the necessity for generation, delivery, storage, and verification of numerous certificates for all pseudonym public keys (or private keys in case of IBC). To mitigate this overhead, Calandriello et al. [96] propose to use group signatures to enable vehicle OBUs to generate and certify their own pseudonyms without interacting with the CA (or Pseudonym Provider). Basically, they use group signatures to support issuance of traditional public key certificates. In contrast, the schemes discussed in this section directly employ group signatures also for message authentication.

Group-oriented signature schemes [133] enable an entity of a group to produce a signature on behalf of the group, i.e., the signature can be verified with a group-wide public key. The group-based signature scheme provides privacy as signers are anonymous within the group. Additionally, two messages signed by the same vehicle are not linkable as one cannot determine if two messages came from the same or different members of the group. Each group has a shared public key, while each group member has its own private key provided by the group manager. There are two major paradigms in anonymous group-oriented signature schemes: group signatures and ring signatures. In a group signature scheme, the group is predefined and there is a group manager that can revoke anonymity for a given signature. Ring signature schemes, on the other hand, do not directly support anonymity revocation, but also do not require a setup stage to produce and distribute group secrets [134]. Hence, any individual can spontaneously cooperate with $n-1$ arbitrary entities and generate a publicly verifiable 1-out-of-n signature on behalf of the whole group. The actual signer remains

unconditionally anonymous in the process. A threshold ring signature scheme is the corresponding t-out-of-n threshold version where t or more entities are required to jointly generate a valid signature [135, 136].

The pseudonym lifecycle for vehicular pseudonym schemes based on group signatures differs slightly from previous categories. The group manager (GM) is a new entity that sets group parameters, changes group public keys, and may revoke anonymity, if supported by the scheme. In contrast to PP or CA, the GM role can be filled by a vehicle and not necessarily a trusted third party. Figure 7 depicts the pseudonym lifecycle for group-based pseudonym schemes, as presented in the following. We use the AMOEBA scheme [46], which uses vehicle groups to mitigate location tracking of target vehicles, as a representative candidate for the lifecycle discussion.

Pseudonym issuance: During the group enrollment phase, the group manager derives an individual private key from the group key and provides it to the new group member. The group key is the public key and can be seen as the pseudonym. This phase highly depends on a scheme's group manager election, as discussed in Section VII-A.

Pseudonym use: A group member uses its individual private key to sign messages and appends the group key. Signatures are verified with the group key. Thus, verifiers learn the sender's group membership but not the sender's identity—all group member share the same pseudonym.

Pseudonym change: In general, there is no need for frequent pseudonym changes in group signature schemes. Pseudonym change is only required in order to manage group dynamics, e.g., to revoke certain vehicles from the group, and is triggered by the GM. Then, the GM generates a new group public key and has to issue new private keys to all group members. AMOEBA uses random silent periods when changing pseudonyms. When a new vehicle joins the group with a pseudonym, it waits for a random time interval before changing its pseudonym, then the new and old pseudonyms cannot be linked.

Pseudonym resolution: To provide accountability, a signature may be traced to the individual signer by the GM using its group manager secret key [137].

Pseudonym revocation: After detecting a misbehaving vehicle, the GM can revoke this vehicle by generating a new group key and deriving new private keys for each group member. When an OBU requests a private key certificate, the group manager checks whether the OBU is in the newly updated revocation list. If so, the OBU is excluded from the group by not providing it with an up-to-date private key.

Lin et al. [6] propose GSIS which extends the above scheme by employing an additional identity-based signature scheme for messages sent by nodes without privacy requirements, such as RSUs or emergency vehicles, to save bandwidth.

In most group signature-based pseudonym schemes, signer privacy is conditional on the GM. As a result, all group signature-based schemes also have the problem of *identity escrow*, as a GM who possesses the group master key can arbitrarily reveal the identity of any group member. In addition, due to potential limitations of group formation in VANETs (e.g., too few cars in the vicinity to establish the group), the group-based schemes may not be applied properly. The *election* of the group leader could encounter some difficulties since the trusted entity cannot be found amongst peer vehicles [128]. Another drawback is *revocation*, as revoking an individual vehicle impacts the whole group by requiring group members to obtain new private keys from the GM.

A. Group Manager Election and Identity Escrow

The issue of defining the GM in a group of peers is not trivial. This challenge has been intensively investigated in Wireless Sensor Networks literature [138, 139]. For vehicular networks, Zhang et al. [140] propose that groups are maintained by RSUs. Vehicles request a new private member key when they pass by an RSU for the first time or when their existing private member keys expire. To manage the group key, Park et al. [141] propose RSU-based Distributed Key Management (RDKM), where a part of the group key management is delegated to RSUs. Instead of having one management entity (Key Distribution Center), the KDC delegates a part of key management functions to each RSU in a distributed manner. An RSU manages a key tree for its associated vehicles and handles pseudonym revocation. The KDC only manages the public group key and is responsible for membership changes such as join or leave, thus, reducing the communication overhead of the KDC.

However, when RSUs are used as group managers, a compromised RSU can break the group members' privacy or prevent authorities from identifying malicious vehicles. So, Hao et al. [142] propose to certify RSUs, i.e., a CA delivers credentials to the RSU. To cope with the increase of communication overhead due to this additional certification layer, this protocol adopts short group signatures [143]. But it does not deal with the computational overhead, and adding a certificate layer just shifts the identity escrow issue to the CA level.

Although the group signature approach does not require each vehicle to store a large number of anonymous keys, the unrevoked vehicles have to update their private keys and group public keys with the group manager when the number of revoked vehicles surpasses some predefined threshold [144].

B. Revocation

Based on the assumption of using an HSM, Rabadi and Mahmud [145] propose an over-the-air rekeying protocol that enables the CA to access OBU memory and delete the group key. Thus, this protocol obviates the need for all other group members to update their private key. Likewise, Zhang et al. [146] propose that a trusted authority acts as GM and generates a group public key, private keys, and revocation tokens for all group members. The revocation token is valid for a period of time and provides backward unlinkability, i.e., signatures produced by a revoked member before the revocation remain anonymous [147]. When the token expires, it is added to a revocation list, which is used by a receiver to check the revocation status of the sender. To cope with the revocation issue, Qin et al. [148] use an identity-based group signature scheme in the enrollment phase to properly identify vehicles,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

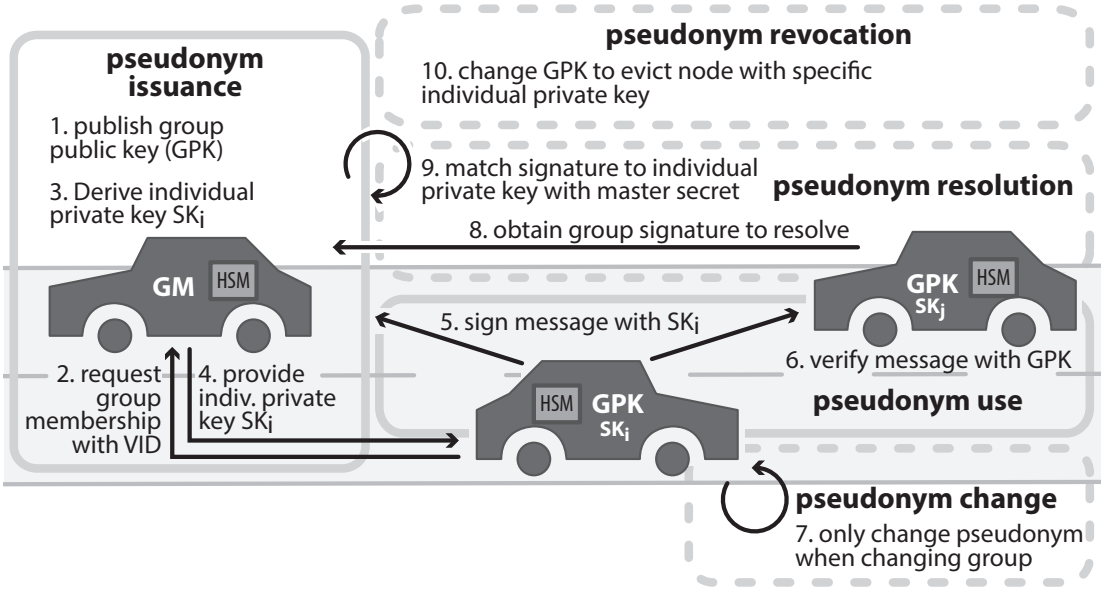

Fig. 7. Pseudonym lifecycle for group-signature based pseudonym schemes.

before issuing a group private key. Their proposal benefits from simplified group management and the liability property provided by the identity-based scheme. Xiong et al. [149] employ a revocable ring signature scheme, proposed by Liu et al. [150], to achieve conditional privacy. The revocable ring signature scheme allows a set of authorities to revoke the anonymity of the real signer. In other words, it provides non-repudiation. Due to the indistinguishability of the Bilinear Decisional Diffie-Hellman assumption, it is difficult for any participant in the system to identify the actual signer except for the CA. Revocation information must be distributed via revocation lists to all OBUs.

The Efficient Conditional Privacy Preservation (ECPP) protocol [151] deals with the issue of growing revocation lists, while achieving conditional traceability by the authorities based on bilinear maps. In ECPP, PPs generate pseudonyms and pseudonym credentials for vehicles, after verifying the vehicle's VID as in asymmetric approaches. Despite the provided anonymity features, the ECPP scheme suffers from multiple drawbacks. First, ECPP is not efficient because it has fairly high latency for generation of pseudonym keys by RSUs [130], and requires ubiquitous presence of RSUs to assist vehicles to derive their pseudonyms at any given road location. Second, ECPP requires that the issued pseudonyms are known to the issuing authorities (i.e. RSUs) beforehand. Since RSUs are distributed in open areas along roads, they are potentially vulnerable to physical attacks. Thus, they should not be fully trusted, unless equipped with tamper-resistant hardware. Third, there is no clear revocation mechanism for ECPP. Since vehicles can derive their pseudonyms from every RSU, even a compromised one, malicious vehicles cannot be revoked. ECPP does not provide unlinkability and untraceability when multiple RSUs are compromised. Indeed, in this case, an adversary is able to track the movement trace of a vehicle by using the information stored in the compromised RSUs, because each RSU stores unchanged pseudonyms for OBUs in ECPP. Jung et al. [152] propose an improvement of ECPP based on a universal re-encryption scheme and identity-based group signatures. However, Tan [153] find that their proposal cannot overcome the weaknesses of ECPP. In fact, if an adversary can corrupt the RSU that issued the short-time anonymous certificates, the adversary can derive all pseudonyms of the OBU. Thus, the adversary can trace vehicles that use those pseudonyms. Moreover, their protocol does not address bidirectional communication between vehicles or between vehicles and RSU.

To solve the issue of revocation overhead, a promising approach is to divide the whole domain of VANET into several sub-regions while providing distributed key management service to vehicles by each regional group manager (RM). The group key issued by an RM is valid just in the corresponding sub-region and a limited validity period. In this way, a revoked membership is just notified in a sub-region instead of the whole domain, and then the average size of the revocation list in each sub-region decreases. Similar to [142], Sun et al. [154] proposed an efficient distributed key management scheme (DKM) for group signature in VANET, which restricts the vehicles enjoying authorisations only to a particular region and duration. Despite DKM could decrease the revocation cost, a malicious user might still use the excellent anonymity property of group signature to send out forged message to other vehicles.

Nevertheless, the current solutions have practical drawbacks like using an expensive tamper-proof hardware, the computation bottlenecks of the verification and revocation phases, complicated certificate distribution/revocation or omitting important properties like short-term linkability, which is demanded in several applications, e.g. change lanes of vehicles in VANETs [155]. Malina et al. [155] propose a solution that employs the short group signature with short-term linkability and categorized batch verification. Moreover, the solution allows secure and practical registration

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

and revocation of users. Their proposal uses the revocation process with the expiration of timestamp in certified pseudonym which revokes members by self. Thus, vehicles do not work with a Revocation List (RL) anymore. The proposal uses only a Group Temporary Revocation List (GTRL) broadcasted between group managers to deny malicious members accessing the group of VANET members. This solution seems promising and future work should be done on the scalability of the solution and the definition of the main parameter k (as it affects the short-term linkability).

To conclude, group-signature schemes are similar to asymmetric cryptography schemes with one major difference in pseudonym issuance. We presented group manager election and revocation issues with their current set of techniques to cope with it. However, no holistic solution has been proposed so far. In Section XI, we discuss a number of future challenges that apply to group signature schemes.

VIII. Symmetric Cryptography Schemes

Symmetric cryptography is less flexible than asymmetric cryptography when it comes to the realization of authentication capabilities, but is highly efficient in terms of computational and communication overhead. In symmetric schemes, a (Hashed) Message Authentication Code ((H)MAC) is used for message authentication. The signer hashes the message and a secret key. Any verifier must know the same secret key to verify the MAC by performing the same operation on the message. As a consequence, any node with knowledge of the secret key can generate valid MACs. Thus, a node's anonymity set extends to all nodes using the same secret key. However, sender accountability is not provided as non-repudiation cannot be achieved.

For inter-vehicle communication, utilization of symmetric authentication schemes offers the benefits of short generation and verification time as well as less security overhead [156]. At the same time, deployment and maintenance of certification infrastructure and associated costs, as required by asymmetric schemes, could be replaced by potentially simpler key distribution. In a naïve scheme, each OBU could have the same secret key preinstalled, or even a set of shared secret keys [157]. Due to the potential benefits, symmetric schemes have been considered for VANET authentication. However, reliable authentication requires that exposure of single secret keys should not compromise authentication of all OBUs. This requirement, paired with the desire for accountability, makes actual symmetric authentication schemes more complex.

Choi et al. [156] first showed the feasibility of symmetric authentication in vehicular networks with balanced privacy and accountability. Their solution is based on key escrow to enforce anonymity and allow optional resolution. Short-term pseudonyms are introduced to achieve privacy against peers. We explain the pseudonym lifecycle for symmetric schemes based on their approach as depicted in Figure 8, which is representative for this category.

Pseudonym issuance: A vehicle registers with an authority, sometimes called ombudsman OM [156]. OM generates a unique identifier (VID) and a seed value for each vehicle. Vehicle and OM can compute a set of pseudonymous handles by hashing the VID with the seed and a counter value. OM retains an identity-pseudonym mapping. Short-term pseudonyms are generated in cooperation with regional infrastructure, i.e., RSUs. The vehicle sends one of its handles to a RSU. The RSU computes multiple short-term pseudonyms by hashing the vehicle's handle with time values and assigning pseudonym IDs to them. The RSU retains a mapping between handle and short-term pseudonym. Zhang et al. introduce RAISE [158, 159] to extend the approach by proposing that the RSU assigns the same group identifier to vehicles in range, thus achieving k-anonymity for the vehicles, while maintaining the ability of pseudonym resolution based on the individual secret key shared between RSU and each vehicle.

Pseudonym use: Vehicles use the short-term pseudonym keys to create MACs for outgoing messages and annotate messages with the pseudonym ID. In Choi et al.'s scheme [156] only RSUs can verify MACs, as only they know the secret keys associated with pseudonym IDs in their region. Thus, receivers must forward messages to RSUs for authentication, which introduces additional delay. In order to mitigate this issue, Zhang et al. [159] propose that RSUs periodically broadcast an aggregate of verified HMACs. Still, vehicles have to delay message utilization until they receive the verification notification from the RSU.

Pseudonym change: Short-term pseudonyms are restricted in their validity by the included time value. At the end of each time interval, all vehicles in the region change their pseudonyms. Laurendeau and Barbeau [160] propose a similar approach.

Pseudonym resolution: Pseudonyms can be resolved in a two step escrow process requiring cooperation of RSUs and OM. RSUs reveal the pseudonymous handle of the vehicle and OM can reveal the vehicle's unique identifier. In [160], vehicles are required to include their identity encrypted with a key shared between OM and vehicle in broadcast messages. OM can decrypt such tokens to obtain the sender's identity.

Pseudonym revocation: Revocation can be achieved by OM marking a vehicle ID as revoked and publishing the corresponding seed value to RSUs. Laurendeau and Barbeau [160] propose that RSUs verify a vehicle's revocation state with the OM before issuing new local pseudonyms. In a more simplistic approach, Xi et al. [157] propose that vehicles hold a set of shared secret keys randomly drawn from a global key pool. As each vehicle holds a random set of keys, the sets of misbehaving vehicles could be revoked while the remaining vehicles are still likely to be successfully authenticated, as the probability that non misbehaving vehicles still possess sufficient valid keys is high.

Symmetric schemes offer highly efficient message authentication, but lack the asymmetric properties of public key schemes, which need to be emulated to provide non-repudiation. The main challenges of utilizing symmetric schemes for vehicular networks are the reliance on road-side infrastructure for message verification and the resulting time delay. Only few proposals, discussed below, aim to reduce infrastructure reliance.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

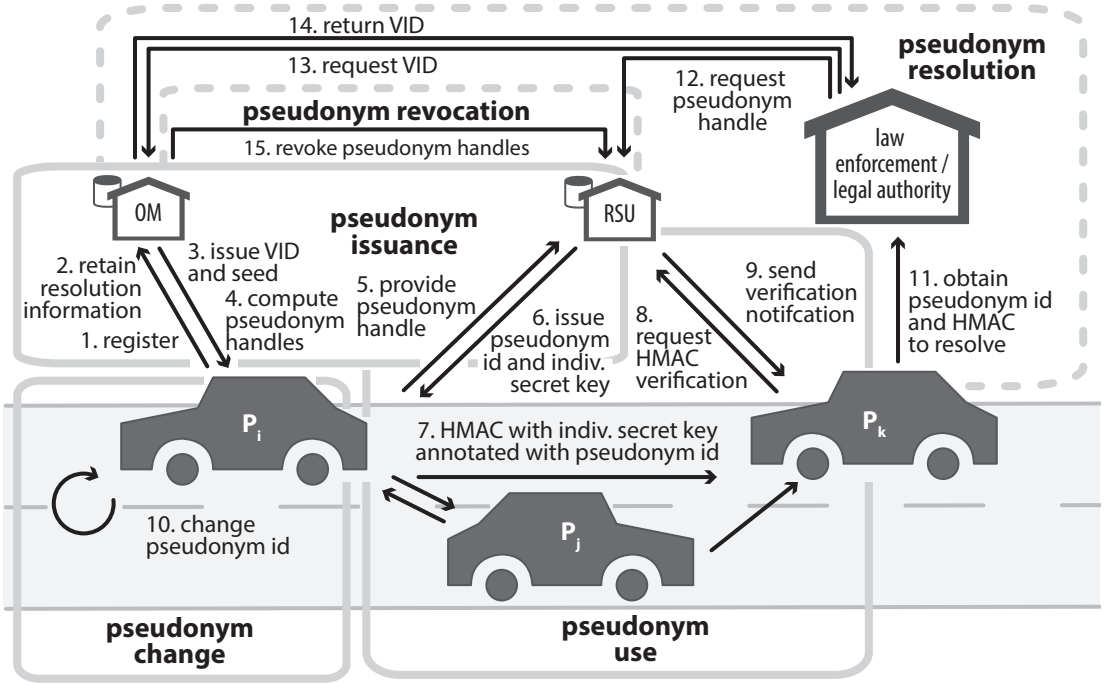

Fig. 8. Pseudonym lifecycle for schemes based on symmetric cryptography.

A. Infrastructure Reliance and Verification Delay

In order to overcome authentication issues when vehicles move between regions of different RSUs, Choi et al. [156] suggest cooperation between neighboring RSUs to ensure message authentication across RSU regions. Wu et al. [161] also propose a handover protocol to enable message authentication in intra and inter RSU range.

Riley et al. [162] obviate the need for RSUs by utilizing mobility characteristics to form vehicle groups. In these dynamic groups, vehicles establish a symmetric key between group members rather than for a specific region. The group formation and symmetric key establishment is based an a standard solution with asymmetric cryptography and a PKI.

Hu and Laberteaux [163] apply the TESLA symmetric authentication protocol to vehicular networks, which does not require RSU support. In TESLA [164], signers use symmetric keys derived from hash chains for message authentication and release keys after a certain period of time (see Figure 9). A message is authenticated with a key that has not been released yet, thus, receivers have to buffer messages until the corresponding or a higher key has been released and the message can be verified. In Hu and Laberteaux's proposal, key release periods are determined according to message frequency and permissible latency. Vehicles also have CA-issued asymmetric pseudonym certificates which are only used to sign their own key chain anchor. When two vehicles encounter each other for the first time, they exchange their signed key chain anchors once. Subsequently, TESLA keys used for message verification can be traced back to a specific anchor. Thus, if pseudonym resolution is required, the asymmetric pseudonym can be resolved (see Section V) and the TESLA-authenticated message can be linked to it. Keys are released for verification by integrating them in periodic beacon messages, without incurring much overhead due to the small key size. However, the delayed key release inadvertently introduces a delay for message verification.

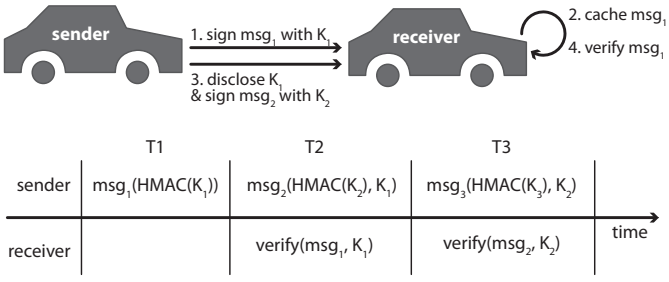

Fig. 9. Delayed key release in the TESLA protocol.

IX. Comparison and discussion

After providing a comprehensive overview of different pseudonym approaches, we now compare them with the help of the pseudonym lifecycle. Table I summarizes the key characteristics of each category.

The four presented categories all use pseudonyms, but the employed type of pseudonym differs. In asymmetric cryptographic schemes, a pseudonym is composed by a signature and a certificate. Therefore, the sender must have a valid public key certificate to be authenticated properly by receivers. The pseudonym used in IBC is shorter as no certificate is attached. Without certificate, the sender is then authenticated based on its identity. The group signature schemes use the same type of pseudonym as the asymmetric schemes, but the pseudonym's scope is broader as it affects every members of the group. The group certificate

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

TABLE I
OVERVIEW OF EACH APPROACH

	Asymmetric	**Identity-based**	**Group sign.**	**Symmetric**
Pseudonym type	Asymmetric key pair, anonymous PKI certificate.	Pseudonymous node identifier as public key.	Group-wide public key.	Short-term symmetric keys
Authentication type	Sender has valid public key certificate	Sender can perform signature for pseudonym identity	Sender can perform signature for group public key	Symmetric key known to RSU.
Pseudonym issuance	Relies on PKI. Vehicles are registered to CAs to obtain long-term identity. Pseudonyms are issued by PP. Frequent communication with PP required for pseudonym refill.	Pseudonym identifiers and corresponding private keys issued by TA (PP). TA can be authority or RSU. Frequent communication with TA required for pseudonym refill.	Group public key and individual private keys generated by GM. GM can be a vehicle, RSU or authority.	Vehicle registered with OM. RSU issues individual short-term symmetric keys in its region.
Pseudonym use	Sender generates asymmetric message signature and appends pseudonym certificate. Receiver verifies signature with pseudonym certificate.	Sender generates asymmetric message signature. Receiver verifies signature with sender's pseudonym identifier.	Sender generates asymmetric message signature. Receiver verifies signature with known group public key. Batch verification possible.	Sender generates MAC with individual symmetric key. Receiver waits for RSU verification or computes MAC after delayed key release.
Pseudonym change	Pseudonym change required to avoid tracking based on public key certificate. Different change strategies exist.	Pseudonym change required to avoid tracking based on identifier. Different change strategies exist.	No obvious need of pseudonym change as group signature ensures anonymity.	Symmetric key change needed to restrict key validity in space and time.
Pseudonym resolution	PP stores identity pseudonym mapping. Resolution can require cooperation of multiple RAs.	TA stores identity pseudonym mapping. No cooperation required.	GM can determine individual signer key. No cooperation required.	RSU and OM cooperate in identity escrow.
Pseudonym revocation	Revocation of VID to prevent pseudonym refill. Possibly CRL to revoke individual pseudonyms	Revocation of VID to prevent pseudonym refill.	Change of group parameters by GM to evict node from group. Requires update of group public key.	Revocation of VID to prevent pseudonym refill.

authenticates the group and that the sender is a valid member of the group. The symmetric cryptographic schemes use an even shorter pseudonym than IBC schemes since only a MAC is used. We now compare how the pseudonym is used in the four approaches.

a) Pseudonym issuance: The asymmetric and identity-based approaches require backend connectivity for pseudonym issuance. Indeed, they require contact to PP or TA for pseudonym issuance. To overcome the issue of permanent infrastructure connectivity, pseudonym pre-loading or self-generation have been proposed. Nevertheless, preloading and self-generation have to be controlled to prevent Sybil attacks. On the opposite, group signature and symmetric approaches rely on vehicle collaboration or RSU contact for pseudonym issuance. At first glance, group signature and symmetric approaches appear as a cost-effective solution as they do not need infrastructure. However, vehicle collaboration raises new issues, such as group manager election (see Section VII-A). Moreover, the reliance on backend connectivity of the first two approaches is shifted to the reliance and stability of the group manager. So the core of the problem remains unchanged.

b) Pseudonym use: Regarding the pseudonym use phase, the asymmetric approach requires a public key certificate to be attached to messages for sender authentication. Therefore, the communication overhead is higher than for identity-based or group signature approaches, which only require a small identifier and a signature. Symmetric approaches require only a MAC. To cope with the overhead issues of asymmetric schemes, certificate omission [96, 75, 165] and adaptive beaconing rates [166] have been proposed. By omitting the certificate, the packet size is reduced and scalability is improved. The adaptive beaconing rate is even more drastic as some messages may be skipped completely. The group signature approach also aims for scalability as the pseudonym management is limited to the group size. Unfortunately, vehicular networks are highly dynamic

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

and group management creates a significant computational overhead. Another issue of group signature schemes is the lack of linkability. As group members are sharing the public key, a receiver cannot distinguish the exact number of neighboring vehicles. This can jeopardize safety applications such as collision avoidance warnings or all applications that rely on knowledge of exact vehicle density. Regarding the symmetric cryptography schemes, protocols like TESLA delay key disclosure to enable use of symmetric keys, but require two successful packet receptions instead of one, which is problematic in delay-sensitive applications.

c) Pseudonym change: Pseudonym change is mainly relevant for privacy in asymmetric and identity-based approaches to prevent vehicle tracking based on constant identifiers. Symmetric approaches also require change of symmetric keys but rather to limit the validity of keys and prevent impersonation attacks once a symmetric key has been released. Group signature approaches do not require a pseudonym change on the authentication level. Yet, static network identifiers could also allow tracking. Therefore, all approaches must change not only pseudonyms but also the vehicle's MAC address and other identifiers. In order to avoid tracking due to radio fingerprinting, switching between different radio modules has also been proposed, but given the state of fingerprinting in real outdoor scenarios, this seems currently a rather academic proposal of low practical relevancy [103]. Thus, one advantage of group signature schemes is removed by the requirement to prevent tracking attacks on lower layers. Section V-C presents an exhaustive list of pseudonym change strategies in the context of asymmetric schemes, however, such strategies could also be applied to the other categories as well as change of network identifiers. Unfortunately those strategies can not fully prevent tracking. For example, eavesdroppers can analyze where users spend most of their time to discover their home address [167]. Selfish vehicles can also refuse participation in a cooperative pseudonym change and brake the mix-zone strategy [57]. But even if an OBU changes the entire communication stack identifiers (MAC address, IP address, etc.) in addition to the pseudonym, there might still be non-volatile data, such as tire pressure sensor IDs, that can serve as an attack surface [103]. An open challenge is to investigate which pseudonym change strategy is the most appropriate. A major step forward would be to reach consensus on the metric used to assess those strategies. We discuss this challenge in Section XI.

d) Pseudonym resolution: The resolution phase either involves a single authority or multiple authorities that need to cooperate. By default, pseudonym resolution could be realized in all categories with simple identity escrow with only one authority. In order to protect against rogue authorities, new architectures are proposed to split responsibility. Regardless of the category, these mechanisms usually involve multiple authorities in secret sharing and threshold cryptography schemes. Besides the technical aspect of resolution, there are potential legal issues. Indeed, pseudonym resolution strategies have to be in line with legal regulations. For example in Europe, data in vehicular communication falls under the European data protection directive 95/46/EC [168], which restricts pseudonym resolution procedures by law enforcement accordingly.

e) Pseudonym revocation: Revoking vehicles in the asymmetric approach implies management of a certificate revocation list. However, including all individual pseudonyms in such CRLs would significantly increase the CRL size. Therefore, revocation is typically limited to the VID, which is verified when obtaining new pseudonyms. Identity-based and symmetric schemes follow similar approaches of rather revoking the vehicle identifier than individual pseudonyms. In group signature approaches, revoking a vehicle provokes changes in the whole group as the group public key has to be updated. Another approach followed by the V-token [82] and CAMP [97] approaches is to insert a linkage value into each certificate. The linkage value is basically an encrypted identifier that remains secret until the revocation of the certificate. Hence, if the encryption key is included in the CRL, all future certificates used by the revoked vehicle can be recognized. This technique permits the revocation of all future messages while preserving privacy of past messages.

f) Resilience against attacks: After comparing the approaches with respect to the pseudonym lifecycle, we compare their resilience against attacks. As a Global Passive Attacker (GPA) can eavesdrop everything, and thus performs location tracking, this is an issue for the four approaches. A local attacker is a more realistic type of attacker, therefore we compare the four main approaches regarding the resilience against a local passive attacker (LPA) and a local active attacker (LAA).

Especially, we consider a LAA that aims at breaking the pseudonymity of vehicles by performing a *pseudonym depletion attack*, because his attack is valid for the four approaches. Indeed, even if statistically improbable, a pseudonym might not be unique, i.e. two distinct vehicles might claim the same identifier (remember that the network identifier is derived from the currently used pseudonym–see Section 9.2.1.5 of [169]). This conflicting identifier would trigger a pseudonym change. An attacker can thus always claim to use the same identifier as the targeted vehicle. Hence, in function of the pseudonym refill strategy, the vehicle will either deplete its pseudonym pool, or will request for refill when a threshold is reached. However, a refill strategy might require connection to a trusted third party (e.g., pseudonym provider) which might not be continuously available. As a consequence, the vehicle might be forced to use the same pseudonym (the last one) or to stop participating in the network. A high threshold would ensure that a vehicle will only be depleted after a sufficient long period of time (and thus tracking), but would require more secure storage to cope with the larger pseudonym pool.

The group-signature approach does no suffer from this depletion attack per se. However, an attacker could wait for the likely moment where the targeted vehicle is not member of a group to break is location privacy. Moreover, within the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

group, an attacker could force re-keying, e.g., by joining and leaving the group repeatedly.

As symmetric approaches typically uses asymmetric cryptography to bootstrap, depletion attacks are also possible.

We discuss the research challenge of pseudonym refill and the impact on the communication stack in Section XI-A. Note that the resilience against attacks is tightly linked to the pseudonym change strategy used.

To conclude the discussion, symmetric schemes have substantial drawbacks and are not practical. One could notice that the establishment of shared secret keys for safety messages would add a non negligible delay. Group signature schemes provide interesting properties, but the computation overhead is problematic. Asymmetric and IBC schemes are similar and according to our analysis the most viable approaches for realizing pseudonymity in vehicular networks.

X. Standardization

While specific privacy requirements and data protection legislation differ significantly between countries, the need to protect privacy in ITS is generally acknowledged. In Standards Development Organizations (SDOs), such as ETSI, ISO, or IEEE, approaches to protect privacy in vehicular networks are actively being discussed. However, privacy approaches are currently considered more at a preliminary stage rather than as part of drafts or final standards already. Yet, there is a clear trend to standardize privacy protection mechanisms for ITS based on pseudonyms.

In Europe, the ETSI Technical Committee on ITS Working Group 5 is responsible for designing a privacy solution. Technical Specification 102 941 [170] specifies a functional split between an enrollment authority and an authorization authority. This corresponds to a simple pseudonym scheme with a CA and PP where the enrollment authority manages vehicle identities and issues long-term certificates, while the authorization authority is responsible for verifying the long-term enrollment of vehicles and issuing short-term pseudonymous certificates that vehicles then use for message authentication. So far, this specification misses important aspects of the pseudonym lifecycle discussed throughout this paper like pseudonym resolution, protection from misuse by authorities, and even pseudonym change. These issues need to be refined and worked out in future specifications. To support this refinement and extensions, the security working group of the C2C-CC[4] has created a "Public Key Infrastructure Memo" [87, 70] that discusses details about PKI operation and how to separate concerns between the CA (here long-term CA) and the pseudonym provider (here pseudonym CA) in order to prevent the pseudonym provider from learning the identities of vehicles it issues pseudonyms for, and the CA from learning the pseudonyms issued for those vehicles. It is expected that this solution will strongly influence the final approach of the ETSI standards.

In Japan, the standardization of vehicular communications is led by the ITS Forum. The standard ARIB STD-T109 specifies 700 MHz band ITS [171]. Unfortunately, the current version (December 2012) does not consider privacy.

In the U.S., vehicular networking security is defined in the standard IEEE 1609.2-2013: Section E.9.5 [67], which does not include privacy mechanisms as the authors argue that privacy requirements are not clear yet. Nevertheless, the 1609 working group considers anonymity—the ability of private drivers to maintain a certain amount of privacy—as one goal of the system, but notes that "revocation and privacy are in conflict with each other, and the exact tradeoff between these goals is a policy matter, with the policy to be decided by stakeholders such as (in the U.S.) the vehicle OEMs and federal and state governments. These stakeholders have not yet communicated the specific requirements to the 1609 Working Group. The 1609 Working Group therefore decided not to include an anonymous certificate specification that might fail to meet the eventual set of requirements. An anonymous certificate specification will be addressed in a future version of or amendment to this standard." [67]

Similar to the C2C-CC efforts in Europe, the Crash Avoidance Metric Partnership (CAMP) consortium has provided a detailed specification of V2X trust management that also foresees pseudonym-based privacy protection (see Section V-B). Their design specifies a detailed solution that separates concerns between Certification Authority (CA), Registration Authority (RA), and two Linkage Authorities (LA). It is to be expected that this proposal will significantly influence work on privacy protection in future versions of IEEE 1609.2.

In 2012, a joint harmonization task force has been set up by the US Department of Transportation and the European Commission[5]. As part of this endeavor, a dedicated working group investigates how to harmonize the EU and US security solutions for vehicular networks. Privacy protection using a pseudonym scheme has been identified as one of the major areas requiring harmonization.

XI. Research challenges

The previous sections show that protecting privacy in vehicular networks with pseudonyms still poses significant research challenges. Many challenges arise for specific categories, because they are shaped by the characteristics of the employed pseudonym type and underlying cryptographic primitives. However, a number of general open research and deployment challenges can be identified that require attention.

A. Considering pseudonym impact on communication stack and services

The purpose of pseudonym change is to (1) mask the change even from nearby vehicles (to prevent tracking) and to (2) prevent long-term tracking. The first goal creates issues for neighborhood-based mechanisms, like cooperative collision warning. Indeed, changing pseudonyms requires to flush the communication stack to change identifiers on all layers, and to avoid sending messages with inconsistent sets of identifiers [172]. Therefore, messages may get lost and routing

[4]Car-2-Car Communications Consortium, www.car-2-car.org

[5]http://www.its.dot.gov/connected_vehicle/international_research.htm

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

tables will have inconsistent entries as a result of pseudonym changes [101]. Hence, pseudonym change strategies impact the communication stack and applications, and thus, require a tradeoff between application quality and privacy level, which should be adequately reflected in respective privacy metrics. In the simTD project[6], this tradeoff is addressed by hiding pseudonym changes from the application layer. A translation table between lower layers and the application layer makes pseudonym changes transparent for applications [173]. Another option is to block pseudonym change for Decentralized Environmental Notification Messages (DENM). Indeed, if a vehicle has stopped at the roadside and sends DENMs to warn approaching vehicles and then changes its pseudonym, receivers will conclude that there are two broken-down vehicles. Plausibility checks could help to prevent such situations and need to be investigated, because blocking pseudonym change decreases the privacy level. So, an open challenge is to investigate how often and for how long vehicles can afford to block pseudonym change without too negative effects on their privacy protection [93]. A privacy metric that captures this tradeoff could help answering this question.

B. Enhancing scalability and reducing computation and communication overhead

As discussed in Section III-C, pseudonym approaches for vehicular networks have to balance seemingly contradicting sets of requirements while considering constraints of the communication system and without compromising the functionality of the vehicular network. Specifically, pseudonym mechanisms must adhere to real-time or near real-time constraints of safety applications, support VANET-specific communication patterns, such as beaconing, multi-hop communication and geocast [13], and provide robustness and scalability [65].

Indeed, when dealing with thousands of vehicles, scalability becomes an issue. The real-world performance of security mechanisms for vehicular networks have been analyzed by Iyer et al. [174], Haas et al. [175], Petit [176], and Petit and Mammeri [177]. The results of these performance studies have been summarized in Deliverable D1.1 [178] of the PRESERVE project.[7] A main result is the identification of an upper bound of about 1,000 verifications per second for an asymmetric cryptography scheme. Therefore, vehicles have to be capable of supporting such load to ensure a secured service. To help solving the scalability issue, a strategy is to reduce computation and communication overhead of security and privacy mechanisms, which is directly related to the use of pseudonym schemes. For instance, Nowatkowski et al. [179] analyze the effects of short-term pseudonyms on certificate revocation list size to highlight the relationship between privacy and security mechanisms. Indeed, depending on the policies for the number of pseudonyms carried by vehicles and the triggers for revoking certificates, the size of the CRL may grow very quickly. For example, when a CA issues pseudonyms for two hours of daily driving with a one year lifetime an hourly CRL would reach a size of over 2.2 GB. When a "valid after" field is added to the pseudonym to limit the lifetime of pseudonyms, a reduction down to 42 MB is achievable. Li et al. [180] propose to use the concept of fountain code for CRL dissemination, which shows significant improvement in reduction of the communication overhead. The frequency of pseudonym refill is also directly linked to the communication and computation overhead caused by CRLs. Indeed, a high frequency refill will increase the size of the CRL.

Another approach taken by the Car-to-Car Communication Consortium is to revoke certificates of long-term identifiers rather than revoking pseudonym certificates [70]. Given a fixed pseudonym lifetime, pseudonym schemes do not need to consider pseudonym revocation as pseudonyms will expire automatically. Hence, a key parameter is the pseudonym lifetime. Without revocation, an adversary has a vulnerability window to perform attacks. The pseudonym lifetime will affect the probability of an attack succeeding. Further research is required to investigate the potential consequences of such vulnerability windows.

Therefore, a cost model that assesses the impact of a pseudonym scheme on computation and communication overhead would be a key metric. Similarly, Chaurasia et al. [181] verify the effectiveness and overhead of group signature schemes and conclude that the delay is significant and that mitigation techniques have to be studied.

According to the current set of standards (see Section X), one can wonder what is actually revoked and what are the consequences of this revocation. If one pseudonym is revoked, then the vehicle can still change its pseudonym to perform privacy-preserving communication. If all pseudonyms a vehicle owns are revoked, then either this vehicle stops communicating, or this vehicle would have to use its long-term identifier to communicate, which would remove any privacy protection. These questions show that the process of revocation should be controlled by regulated authorities and with the awareness of all potential consequences of revoking a vehicle's identifiers.

C. Privacy metrics

Pseudonym change needs to be considered holistically in order to effectively provide privacy. To guide the selection of appropriate pseudonym change strategies, privacy metrics have been proposed to assess the effectiveness of different strategies [44, 182]. For example, entropy [107], anonymity set size [183], or degree of location privacy [114] are privacy metrics used in the context of vehicular networks. Entropy assesses the level of usefulness of information and is often used to measure privacy. However, entropy is not an intuitive metric as it uses a logarithmic scale and is unbounded. Thus drawing conclusions from entropy values is difficult, because it can be difficult to relate them to practical privacy implications. The anonymity set size (k-anonymity) is more intuitive as it represents the number of entities that are indistinguishable from each other, e.g., due to using the same group key. A larger anonymity set (larger k) signifies better privacy. We refer the reader to Fung et al. [184] for details on k-anonymity, and its optimizations l-diversity and t-closeness.

[6]http://www.simtd.org

[7]http://www.preserve-project.eu

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2014.2345420, IEEE Communications Surveys & Tutorials

The degree of location privacy indicates how long an attacker could successfully track a vehicle.

In the context of information retrieval, differential privacy has emerged as a major privacy preservation technique [185]. Laplacian noise is added to a database in order to perturb information. A sensitivity parameter adjusts the level of added noise, e.g., depending on the number of entries in the database and the number of possible queries. While highly effective, the application to vehicular communications is not clear as differential privacy produces noisy data while vehicular communication requires accurate information [186]. Moreover, there is no database or centralized query processor in distributed vehicular networks.

Vehicles can also evaluate the distance over which they are potentially tracked by an adversary (i.e., the *distance-to-confusion* [187]) and can act upon it by deciding whether and when to change its pseudonym. The *distance-to-confusion* is defined as the travel distance until tracking uncertainty rises above a defined threshold.

As the pseudonym change is an important step in the pseudonym lifecycle, Freudiger et al. [116] propose to take into account the various costs involved in changing pseudonym and express it as: $\gamma = \gamma_{acq} + \gamma_{rte} + \gamma_{sil}$, where γ_{acq} is the cost of acquiring new pseudonyms, γ_{rte} is the cost of updating routing tables, and γ_{sil} is the cost of remaining silent (if applicable). The cost can be seen as the minimum privacy gain that compensates for the effort of a pseudonym change.

In general, there is a lack of consensus on suitable privacy metrics for vehicular networks, fostered by the fact that most metrics have only been validated in limited simulations and rarely in the wild. In particular, a comprehensive assessment of proposed pseudonym change strategies with consistent metrics is missing. Ultimately, standard metrics and evaluation methods need to be identified and agreed upon, which can then be used to effectively evaluate pseudonym proposals in a comparable manner. Recent work by Rebollo-Monedero et al. [188] provides a survey of privacy metrics that sheds new light on the understanding of those metrics and their suitability when it comes to applying them to specific scenarios.

D. Fundamental relationship between pseudonym change strategies and privacy level

Pseudonym change is a critical phase of the lifecycle as it directly impacts the privacy level. If not properly set, the frequency of pseudonym changes can increase the linkability of a vehicle. Moreover, a pseudonym change strategy is defined by the rate of change and the context of the vehicle (location, density of neighbors, infrastructure availability and deployment). All these parameters are linked and their interdependencies have to be formalized. Troncoso et al. [189] analyze PKI approaches and their results indicate that privacy-preserving solutions should be based on one-time pseudonyms (i.e. one pseudonym per message sent), as the reuse of certificates is the key feature that enables their tracking attacks. Furthermore, one-time pseudonyms would provide forward (and backward) security properties: even if a vehicle is tracked in a trip (e.g., because it is traveling alone in the road and does not cross any other vehicles), one-time pseudonyms would not provide any useful information for tracking the past or future trips of that vehicle. Anonymous credentials are one way of implementing one-time pseudonyms with optional anonymity revocation. Nevertheless, one-time pseudonym will create "ghost vehicles" [190] inside the Local Dynamic Map (LDM) [191], which jeopardizes safety applications like cooperative collision warning. The fundamental relationship between pseudonym change strategies and the privacy level needs to be formalized to identify all the parameters involved, and enable a cost-benefit analysis. A set of standardized but diverse simulation/experiment parameters would help the comparison of pseudonym change strategies and facilitate the exposure of strengths and weaknesses in proposed strategies.

E. Impact of privacy strategies on safety level

The discussion of the previous challenges highlights that privacy protection schemes are not without consequences for safety applications. Such applications make decisions (e.g. warning drivers of an upcoming danger) based on their current estimation of the state of the real world, and this representation is created from the information contained in beacons received from other vehicles. Therefore, interruptions in the transmission of information will impact the decision-making process. If a silent period is scheduled to start at a safety-critical moment, it could result in safety systems not intervening when they should have, namely a "missed intervention." From a user and safety perspective, this is not acceptable. Lefèvre et al. [79] address this issue and evaluated the impact of pseudonym change strategies on V2X-based intersection collision avoidance systems. The authors also encouraged similar studies for other safety applications in order to establish privacy policies that provide the optimal compromise between privacy and safety of drivers.

XII. CONCLUSIONS

Safety-critical applications in cooperative vehicular networks require authentication of nodes and messages. Yet, privacy of individual vehicles and drivers must be maintained. Pseudonymity can combine security and privacy requirements. Thus, a large body of work emerged in recent years, proposing pseudonym solutions tailored to vehicular networks. In this paper, we provided a comprehensive survey on the complex topic of pseudonymity in vehicular networks. The proposed abstract pseudonym lifecycle is applicable to the majority of pseudonym approaches for vehicular networks and facilitates comparison and discussion of those approaches. We identified four major categories of pseudonym approaches that overlap with the dominant research directions: pseudonym schemes based on asymmetric cryptography and PKIs, identity-based cryptography schemes, group signature schemes, and schemes based on symmetric cryptography. We discussed each category by introducing its general concepts in relation to the pseudonym lifecycle, followed by a more detailed discussion of issues and optimizations for this category. The categorization and integrative discussion of contributions provides the opportunity to establish deeper insights into the pseudonym approaches in

vehicular networks, their requirements, and challenges. Our discussion and the provided comparison table in Section IX contrast the four categories of pseudonym approaches and highlight their advantages and disadvantages. To foster further research in this area, we identified a number of challenges for future research, such as pseudonym change strategies, and reduction of computation and communication overhead. To the best of our knowledge, this survey provides the most comprehensive overview of the existing body of work on pseudonym approaches for vehicular networks to date.

This survey also highlights the fact that current standardization efforts lack behind the research results regarding pseudonym solutions. Most notably, approaches beyond public key based schemes are hardly considered standardization efforts at the moment. We hope that this survey is also recognized and considered helpful in standardization bodies and contributes to their work, eventually leading to secure and privacy preserving V2X systems. Therefore, an additional challenge to the research community is to demonstrate the feasibility of proposed pseudonym mechanisms in realistic settings to convincingly communicate advantages of specific contributions. Hence, suitable metrics need to be developed that capture the required utility-privacy tradeoff and can be used to compare the suitability of different proposals.

RECOMMENDED READING

The number of references in this research area can be taunting. In the following, we provide further reading recommendations for newcomers to the field. Schoch et al. [13] summarize dominant communication patterns in vehicular networks, Raya and Hubaux [20] provide a good overview of security and privacy issues in such networks, and Krumm [7] summarizes location privacy issues and solutions. Schaub et al. [65] more specifically assess the interplay of privacy, security, and system requirements in vehicular networks. Wiedersheim et al. [29] and Freudiger et al. [113] provide good introductions to the relevance and issues of changing pseudonyms dynamically. Rebollo-Monedero et al. [188] and Freudiger et al. [116] provide the state of the art for measuring privacy in dynamic networks, such as vehicular networks.

ACKNOWLEDGMENTS

The authors would like to thank Geert Heijenk, Marco Gruteser, and the anonymous reviewers for their insightful comments and suggestions.

J. Petit, M. Feiri, and F. Kargl received funding from the European Union's Seventh Framework Programme project PRESERVE under grant agreement no. 269994. F. Schaub conducted parts of this research as a research associate at the Institute of Media Informatics, Ulm University. F. Schaub also received funding from the German Academic Exchange Service (DAAD) for a research stay at the University of Twente. Icons in the figures have been adopted from picol.org.

REFERENCES

[1] T. Willke, P. Tientrakool, and N. Maxemchuk, "A survey of inter-vehicle communication protocols and their applications," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 2, pp. 3–20, 2009.

[2] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 99, pp. 1–33, 2011.

[3] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *Journal of Network and Computer Applications*, 2013.

[4] M. Riley, K. Akkaya, and K. Fong, "A survey of authentication schemes for vehicular ad hoc networks," *Security and Communication Networks*, vol. 4, no. 10, pp. 1137–1152, 2011.

[5] S. Biswas, M. M. Haque, and J. V. Misic, "Privacy and anonymity in vanets: A contemporary study," *Ad Hoc & Sensor Wireless Networks*, vol. 10, no. 2-3, pp. 177–192, 2010.

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

[7] J. Krumm, "A survey of computational location privacy," *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 391–399, 2009.

[8] IEEE, "IEEE 802.11p-2010: Wireless access in vehicular environments," Standard, 2010. [Online]. Available: http://standards.ieee.org/getieee802/download/802.11p-2010.pdf

[9] ETSI, "ETSI EN 302 637-1-3: Intelligent transport systems (ITS); vehicular communications; basic set of applications; part 1 to 3," Standard, 2010.

[10] ETSI TC ITS, "EN 302 665 - intelligent transport systems (ITS); communications architecture," Standard, ETSI TC ITS, 2010. [Online]. Available: http://pda.etsi.org/pda/home.asp?wki_id=EtIZjWUpxNikqnnmkuk9z

[11] ——, "ETSI TS 103 097 v1.1.1 - intelligent transport systems (ITS); security; security header and certificate formats," Standard, TC ITS, 2013. [Online]. Available: http://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.01.01_60/ts_103097v010101p.pdf

[12] SAE International, "SAE j2735 v1.1.1 - dedicated short range communications (dsrc) message set dictionary," Standard, 2009. [Online]. Available: http://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.01.01_60/ts_103097v010101p.pdf

[13] E. Schoch, F. Kargl, and M. Weber, "Communication patterns in VANETs," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 119–125, 2008.

[14] A. Studer, M. Luk, and A. Perrig, "Efficient mechanisms to provide convoy member and vehicle sequence authentication in vanets," in *3rd Int. Conf. Security and Privacy in Comm. Networks (SecureComm '07)*, Sept. 2007.

[15] L. Gollan and C. Meinel, "Digital signatures for automobiles," in *6th World Multiconference on of Systemics,*

Cybernetics and Informatics (SCI '02), July 2002.

[16] M. El Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," in *European Wireless (EW'02)*, Feb. 2002.

[17] J. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy Magazine*, vol. 2, no. 3, pp. 49–55, 2004.

[18] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "Securing vehicular communications - assumptions, requirements, and principles," in *4th Workshop on Embedded Security in Cars (ESCAR '06)*, Nov. 2006.

[19] F. Dötzer, "Privacy issues in vehicular ad hoc networks," in *Privacy Enhancing Technologies Symposium (PETS '06)*. Springer, June 2006.

[20] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security (JCS)*, vol. 15, no. 1, pp. 39–68, 2007.

[21] P. Papadimitratos, A. Kung, J.-P. Hubaux, and F. Kargl, "Privacy and identity management for vehicular communication systems: A position paper," in *Workshop on Standards for Privacy in User-Centric Identity Management*, July 2006.

[22] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Workshop on Hot Topics in Networks (HotNets-IV)*, Nov. 2005.

[23] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing Vehicular Communications," *IEEE Wireless Communications Magazine*, vol. 13, no. 5, pp. 8–15, 2006.

[24] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.

[25] Statistisches Bundesamt, "Laufende Wirtschaftsrechnungen - Ausstattung privater Haushalte mit ausgewählten Gebrauchsgütern 2010," Statistisches Bundesamt, Wiesbaden, Fachserie 15 Reihe 2, August 2011.

[26] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Achieving guaranteed anonymity in GPS traces via uncertainty-aware path cloaking," *IEEE Trans. Mob. Comput*, vol. 9, no. 8, pp. 1089–1107, 2010.

[27] P. Hustinx, "Opinion of the european data protection supervisor on the communication from the commission on an action plan for the deployment of intelligent transport systems in europe and the accompanying proposal for a directive of the european parliament and of the council laying down the framework for the deployment of intelligent transport systems in the field of road transport and for interfaces with other transport modes," *Official Journal of the European Union*, vol. 47, no. 2, pp. 6–15, 2010.

[28] M. Gerlach, "Assessing and improving privacy in VANETs," in *4th Workshop on Embedded Security in Cars (ESCAR '06)*, Nov. 2006.

[29] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *7th Int. Conf. Wireless On-demand Network Systems and Services (WONS '10)*, Feb. 2010.

[30] J. Douceur, "The sybil attack," in *1st Int. Workshop on Peer-to-Peer Systems (IPTPS '02)*. Springer, Mar. 2002.

[31] A. F. Westin, "Privacy and freedom," *Washington and Lee Law Review*, vol. 25, no. 1, p. 166, 1968.

[32] S. Du, M. Ibrahim, M. Shehata, and W. Badawy, "Automatic License Plate Recognition (ALPR): A State-of-the-Art Review," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 23, no. 2, pp. 311–325, 2013.

[33] A. Cavoukian, "Surveillance, then and now: Securing privacy in public spaces," Tech. Rep., 2013.

[34] D. J. Glancy, "Privacy on the Open Road," *Ohio NUL Rev.*, vol. 30, p. 295, 2004.

[35] B. Thomas, K. Antonio, K. Martin, K. Frank, M. Zhendong, T. Guido, and F. Johann-Christoph, "PRECIOSA D1 v2x privacy issues analysis," PRECIOSA consortium, Deliverable, 2009.

[36] A. Pfitzmann and M. Köhntropp, "Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology," *Designing Privacy Enhancing Technologies*, vol. 2009, pp. 1–9, 2001.

[37] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[38] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management," TU Dresden, Tech. Rep. v.034, August 2010. [Online]. Available: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

[39] J.-M. Bohli and A. Pashalidis, "Relations among privacy notions," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1–24, May 2011.

[40] R. Küsters, T. Truderung, and A. Vogt, "Accountability: definition and relationship to verifiability," in *17th ACM Conf. Computer and Communications Security (CCS '10)*, Oct. 2010.

[41] J. Kilian and E. Petrank, "Identity escrow," in *18th Int. Cryptology Conf. (CRYPTO '98)*. Springer, Aug. 1998.

[42] M. Wernke, P. Skvortsov, F. DÃŒrr, and K. Rothermel, "A classification of location privacy attacks and approaches," *Personal and Ubiquitous Computing*, pp. 1–13, 2012.

[43] A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmüller, "Attacks on inter-vehicle communication systems - an analysis," in *3rd Int. Workshop on Intelligent Transportation (WIT '06)*, Mar. 2006.

[44] Z. Ma, F. Kargl, and M. Weber, "Measuring location privacy in V2X communication systems with accumulated information," in *6th IEEE Int. Conf. Mobile Ad-hoc and Sensor Systems (MASS '09)*, Oct. 2009.

[45] M. Humbert, M. H. Manshaei, J. Freudiger, and J.-P. Hubaux, "Tracking games in mobile networks," in *1st Int. Conf. Decision and game theory for security (GameSec '10)*. Springer, Nov. 2010.

[46] K. Sampigethaya, M. Li, L. Huang, and R. Pooven-

dran, "AMOEBA: Robust location privacy scheme for VANET," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1569–1589, 2007.

[47] Y. Al-Khassawneh and N. Salim, "On the use of data mining techniques in vehicular ad hoc network," in *Advanced Machine Learning Technologies and Applications*. Springer, 2012, pp. 449–462.

[48] P. Golle and K. Partridge, "On the Anonymity of Home/Work Location Pairs," in *Pervasive*, ser. Lecture Notes in Computer Science, H. Tokuda, M. Beigl, A. Friday, A. J. B. Brush, and Y. Tobe, Eds., vol. 5538. Springer, 2009, pp. 390–397.

[49] C. Oh, S. Ritchie, and S.-T. Jeng, "Anonymous vehicle reidentification using heterogeneous detection systems," *IEEE Trans. on Intelligent Transportation Systems*, vol. 8, no. 3, pp. 460–469, 2007.

[50] S. Charbonnier, A. Pitton, and A. Vassilev, "Vehicle reidentification with a single magnetic sensor," in *IEEE Int. Instrumentation and Measurement Technology Conference (I2MTC '12)*, May 2012.

[51] A. Beresford and F. Stajano, "Location privacy in pervasive computing," *Pervasive Computing, IEEE*, vol. 2, no. 1, pp. 46–55, 2003.

[52] M. Duckham and L. Kulik, "Location privacy and location-aware computing," *Dynamic & mobile GIS: investigating change in space and time*, 2006.

[53] Y. Pan and J. Li, "An analysis of anonymity for cooperative pseudonym change scheme in one-dimensional VANETs," in *IEEE 16th Int. Conf. Computer Supported Cooperative Work in Design (CSCWD '12)*, May 2012.

[54] Y. Pan, J. Li, L. Feng, and B. Xu, "An analytical model for random changing pseudonyms scheme in VANETs," in *Int. Conf. Network Computing and Information Security (NCIS '11)*, May 2011.

[55] L. Huang, H. Yamane, K. Matsuura, and K. Sezaki, "Towards modeling wireless location privacy," in *5th Int. Privacy Enhancing Technologies Symposium (PETS '06)*. Springer, June 2006.

[56] Z. Ma, F. Kargl, and M. Weber, "A location privacy metric for v2x communication systems," in *IEEE Sarnoff Symposium*, Mar. 2009.

[57] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "On non-cooperative location privacy: a game-theoretic analysis," in *16th ACM Conf. Computer and communications security (CCS '09)*, Nov. 2009.

[58] R. Lu, X. Lin, T. Luan, X. Liang, and X. Shen, "Anonymity analysis on social spot based pseudonym changing for location privacy in VANETs," in *IEEE Int. Conf. Communications (ICC '11)*, June 2011.

[59] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *IEEE Symposium on Security and Privacy*, May 2011.

[60] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec, "Protecting location privacy: optimal strategy against localization attacks," in *ACM Conf. Computer and communications security (CCS '12)*, Oct. 2012.

[61] J.-H. Song, V. W. S. Wong, and V. C. M. Leung, "Wireless location privacy protection in vehicular ad-hoc networks," in *IEEE Int. Conf. Communications (ICC '09)*, June 2009.

[62] B. Hoh and M. Gruteser, "Protecting location privacy through path confusion," in *1st Int. Conf. Security and Privacy for Emerging Areas in Communications Networks (SecureComm '05)*, Sept. 2005.

[63] M. Duckham and L. Kulik, "Simulation of obfuscation and negotiation for location privacy," in *Spatial Information Theory*. Springer, 2005.

[64] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *1st Int. Conf. Mobile systems, applications and services (MobiSys '03)*, May 2003.

[65] F. Schaub, Z. Ma, and F. Kargl, "Privacy Requirements in Vehicular Communication Systems," in *Symposium on Secure Computing, IEEE Int. Conf. on Privacy, Security, Risk, and Trust (PASSAT '09)*, Aug. 2009.

[66] ETSI - European Telecommunications Standards Institute, "Intelligent transport systems (ITS); communications architecture," ETSI, European Norm EN 302 665, September 2010.

[67] IEEE, "IEEE 1609.2: Standard for wireless access in vehicular environments (wave) - security services for applications and management messages," Standard, 2013.

[68] ETSI TC ITS, "ETSI TS 102 731 v1.1.1 - intelligent transport systems (ITS); security; security services and architecture," Standard, TC ITS, 2010. [Online]. Available: http://www.etsi.org/deliver/etsi_ts/102700_102799/102731/01.01.01_60/ts_102731v010101p.pdf

[69] W. Fehr, "Security credential management system design - security system design for cooperative vehicle-to-vehicle crash avoidance applications using 5.9 GHz dedicated short range communications (DSRC) wireless communications," RITA Intelligent Transportation Systems Joint Program Office, Draft report FHWA-JPO-, 2012.

[70] N. Bissmeyer, H. Stübing, E. Schoch, S. Götz, and B. Lonc, "A generic public key infrastructure for securing car-to-x communication," in *18th World Congress on Intelligent Transport Systems*, Oct. 2011.

[71] T. Leinmüller, E. Schoch, and F. Kargl, "Position Verification Approaches for Vehicular Ad Hoc Networks," *IEEE Wireless Communication Magazine*, vol. 13, no. 5, pp. 16–21, 2006.

[72] J. Song, Y. Zhuang, J. Pan, and L. Cai, "Certificateless secure upload for drive-thru internet," in *IEEE Int. Conf. Communications (ICC '11)*, June 2011.

[73] J. Petit and Z. Mammeri, "Authentication and consensus overhead in vehicular ad hoc networks," *Telecommunication Systems*, pp. 1–14, 2011.

[74] F. Kargl, E. Schoch, B. Wiedersheim, and T. Leinmüller, "Secure and efficient beaconing for vehicular networks," in *5th ACM Int. workshop on VehiculAr Inter-NETworking (VANET '08)*, Sept. 2008.

[75] E. Schoch and F. Kargl, "On the efficiency of secure beaconing in VANETs," in *3rd ACM Conf. Wireless*

network security (WiSec '10), Mar. 2010.

[76] M. Wolf and T. Gendrullis, "Design, implementation, and evaluation of a vehicular hardware security module," in *Int. Conf. Information Security and Cryptology (ICISC '12)*. Springer, Nov. 2012.

[77] E. Fonseca, A. Festag, R. Baldessari, and R. Aguiar, "Support of anonymity in VANETs - putting pseudonymity into practice," in *IEEE Wireless Comm. and Networking Conf. (WCNC '07)*, Mar. 2007.

[78] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," in *4th European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS '07)*, July 2007.

[79] S. Lefèvre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of v2x privacy strategies on intersection collision avoidance systems," in *5th IEEE Vehicular Networking Conference (VNC '13)*, Dec. 2013.

[80] M. Gerlach and F. Guttler, "Privacy in VANETs using changing pseudonyms - ideal and real," in *IEEE 65th Vehicular Technology Conference (VTC '07-Spring)*, Apr. 2007.

[81] L. Fischer, A. Aiijaz, C. Eckert, and D. Vogt, "Secure revocable anonymous authenticated inter-vehicle communication (SRAAC)," in *4th Workshop on Embedded Security in Cars (ESCAR '06)*, Nov. 2006.

[82] F. Schaub, F. Kargl, Z. Ma, and M. Weber, "V-tokens for Conditional Pseudonymity in VANETs," in *IEEE Wireless Comm. & Networking Conf. (WCNC '10)*, Apr. 2010.

[83] N. Bißmeyer, J. Petit, and K. M. Bayarou, "CoPRA: Conditional Pseudonym Resolution Algorithm in VANETs," in *10th IFIP/IEEE Annual Conference on Wireless On-Demand Network Systems and Services (WONS '13)*, Mar. 2013.

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

[85] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: Design and architecture," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, 2008.

[86] F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: implementation, performance, and research challenges," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 110–118, 2008.

[87] C2C-CC, "Public key infrastructure memo," Car 2 Car Communication Consortium, Tech. Rep., 2010.

[88] S. Eichler, "Strategies for pseudonym changes in vehicular ad hoc networks depending on node mobility," in *IEEE Intelligent Vehicles Symposium (IV '07)*, June 2007.

[89] H. Schweppe, Y. Roudier, B. Weyl, L. Apvrille, and D. Scheuermann, "Car2x communication: Securing the last meter - a cost-effective approach for ensuring trust in car2x applications using in-vehicle symmetric cryptography," in *IEEE Vehicular Technology Conference (VTC '11 Fall)*, Sept. 2011.

[90] M. Nowatkowski and H. Owen, "Scalable certificate revocation list distribution in vehicular ad hoc networks," in *IEEE Global Telecomm. Conf. (GLOBECOM '10)*, Dec. 2010.

[91] Y. Kondareddy, G. Di Crescenzo, and P. Agrawal, "Analysis of certificate revocation list distribution protocols for vehicular networks," in *IEEE Global Telecomm. Conf. (GLOBECOM '10)*, Dec. 2010.

[92] P. P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, "Certificate revocation list distribution in vehicular communication systems," in *5th ACM Int. workshop on VehiculAr InterNETworking (VANET '08)*, Sept. 2008.

[93] Z. Ma, F. Kargl, and M. Weber, "Pseudonym-on-demand: a new pseudonym refill strategy for vehicular communication," in *2nd IEEE Int. Symp. Wireless Vehicular Communications (WiVec '08)*, Sept. 2008.

[94] K. Zeng, "Pseudonymous PKI for ubiquitous computing," in *3rd European Conference on Public Key Infrastructure: Theory and Practice (EuroPKI '06)*. Springer, June 2006.

[95] F. Armknecht, A. Festag, D. Westhoff, and K. Zeng, "Cross-layer privacy enhancement and non-repudiation in vehicular communication," in *4th Workshop on Mobile Ad-Hoc Networks (WMAN '07)*, Feb. 2007.

[96] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *4th ACM Int. workshop on Vehicular ad hoc networks (VANET '07)*, Sept. 2007.

[97] US DOT, "Security Credential Management System Design: Security system design for cooperative vehicle-to-vehicle crash avoidance applications using 5.9 GHz Dedicated Short Range Communications (DSRC) wireless communications," US Department of Transportation, Draft, 2012.

[98] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," in *6th IEEE Conf. Sensor, Mesh and Ad Hoc Communications and Networks (SECON '09)*, June 2009.

[99] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang, "Adaptive privacy-preserving authentication in vehicular networks," in *1st Int. Conf. Comm. and Networking in China (ChinaCom '06)*, Oct. 2006.

[100] M. Burmester, E. Magkos, and V. Chrissikopoulos, "Strengthening privacy protection in vanets," in *IEEE Int. Conf. Wireless and Mobile Computing, Networking and Communications (WiMob '08)*, Oct. 2008.

[101] E. Schoch, F. Kargl, T. Leinmüller, S. Schlott, and P. Papadimitratos, "Impact of pseudonym changes on geographic routing in vanets," in *3rd European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS '06)*, Sept. 2006.

[102] 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 *2nd IEEE Vehicular Networking Conf. (VNC '10)*, Dec. 2010.

[103] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study," in *19th USENIX Conf. Security (USENIX Sec '10)*, Aug. 2010.

[104] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," in *3rd. Workshop on Embedded Security in Cars (ESCAR '05)*, Nov. 2005.

[105] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & swap: user-centric approaches towards maximizing location privacy," in *5th ACM workshop on Privacy in electronic society (WPES '06)*, Oct. 2006.

[106] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "SLOW: A Practical Pseudonym Changing Scheme for Location Privacy in VANETs," in *1st IEEE Vehicular Networking Conf. (VNC '09)*, Oct. 2009.

[107] B. Chaurasia and S. Verma, "Optimizing pseudonym updation for anonymity in VANETs," in *IEEE Asia-Pacific Services Computing Conf. (APSCC '08)*, Dec. 2008.

[108] B. Chaurasia, S. Verma, G. Tomar, and A. Abraham, "Optimizing pseudonym updation in vehicular ad-hoc networks," in *Trans. Computational Science IV*. Springer, 2009.

[109] B. Chaurasia, S. Verma, G. Tomar, and S. Bhaskar, "Pseudonym based mechanism for sustaining privacy in VANETs," in *1st Int. Conf. Computational Intelligence, Communication Systems and Networks (CICSYN '09)*, July 2009.

[110] R. Lu, X. Lin, T. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Trans. on Vehicular Technology*, vol. 61, no. 1, pp. 86–96, 2011.

[111] R. Lu, X. Lin, and X. Shen, "SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *29th IEEE Conf. on Comp. Comm. (INFOCOM '10)*, Mar. 2010.

[112] J. Liao and J. Li, "Effectively changing pseudonyms for privacy protection in VANETs," in *10th Int. Symp. Pervasive Systems, Algorithms, and Networks (ISPAN '09)*, Dec. 2009.

[113] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-Zones for Location Privacy in Vehicular Networks," in *ACM Workshop on Wireless Networking for ITS (WiN-ITS '07)*, Aug. 2007.

[114] A. Wasef and X. S. Shen, "REP: Location Privacy for VANETs Using Random Encryption Periods," *Mob. Netw. Appl.*, vol. 15, pp. 172–185, 2010.

[115] F. Scheuer, K.-P. Fuchs, and H. Federrath, "A safety-preserving mix zone for vanets," in *8th Int. Conf. Trust, privacy and security in digital business (TrustBus '11)*, Aug. 2011.

[116] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "Non-cooperative location privacy," *IEEE Trans. Dependable and Secure Comp.*, vol. 10, no. 2, pp. 84–98, 2013.

[117] H. Weerasinghe, H. Fu, S. Leng, and Y. Zhu, "Enhancing unlinkability in vehicular ad hoc networks," in *IEEE Int. Conf. Intelligence and Security Informatics (ISI '11)*, July 2011.

[118] R. K. Schmidt and T. Leinmüller, "A spatio-temporal metric for the evaluation of cooperative awareness," in *18th World Congress on Intelligent Transport Systems*, Oct. 2011.

[119] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology (CRYPTO '84)*. Springer, Aug. 1985.

[120] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology (CRYPTO '01)*. Springer, Aug. 2001.

[121] S. Zhao, A. Aggarwal, R. Frost, and X. Bai, "A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 380–400, 2011.

[122] P. Kamat, A. Baliga, and W. Trappe, "An identity-based security framework for VANETs," in *3rd ACM Int. workshop on Vehicular ad hoc networks (VANET '06)*, Sept. 2006.

[123] B. H. Kim, K. Y. Choi, J. H. Lee, and D. H. Lee, "Anonymous and traceable communication using tamper-proof device for vehicular ad hoc networks," in *Int. Conf. Convergence Information Technology (ICCIT '07)*, Nov. 2007.

[124] T. Chim, S. Yiu, L. C. Hui, and V. O. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," *Ad Hoc Networks*, vol. 9, no. 2, pp. 189–203, 2011.

[125] J. Zhang and Y. Xu, "Breaking and repairing of an anonymous and traceable communication protocol for vehicular ad hoc networks," in *12th Int. Conf. on Computer and Information Technology (CIT '12)*, Oct. 2012.

[126] C. Lai, H. Chang, and C. C. Lu, "A secure anonymous key mechanism for privacy protection in VANET," in *9th Int. Conf. on Intelligent Transport Systems Telecomm. (ITST '09)*, Oct. 2009.

[127] K. G. Paterson and G. Price, "A comparison between traditional public key infrastructures and identity-based cryptography," *Information Security Technical Report*, vol. 8, no. 3, pp. 57–72, 2003.

[128] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Trans. Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1227–1239, 2010.

[129] X. Sun, X. Lin, and P.-H. Ho, "Secure vehicular communications based on group signature and id-based signature scheme," in *IEEE Int. Conf. Comm. (ICC '07)*, June 2007.

[130] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: An efficient pseudonymous authentication-based conditional privacy protocol for vanets," *IEEE Trans. ITS*, vol. 12, no. 3, pp. 736–746, 2011.

[131] C. Gamage, B. Gras, B. Crispo, and A. S. Tanenbaum, "An identity-based ring signature scheme with enhanced privacy," in *2nd Int. Conf. Security and Privacy in Communication Networks (SecureComm '06)*, Aug. 2006.

[132] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Computer Communications*, vol. 31, no. 12, pp. 2803–2814, 2008.

[133] D. Chaum and E. Van Heyst, "Group signatures," in *10th Int. Conf. Theory and application of cryptographic techniques (EUROCRYPT '91)*, Aug. 1991.

[134] R. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Advances in Cryptology (ASIACRYPT '01)*, Dec. 2001.

[135] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups," in *Advances in Cryptology (CRYPTO '02)*. Springer, Aug. 2002.

[136] S. S. M. Chow, L. C. K. Hui, and S.-M. Yiu, "Identity based threshold ring signature," in *Int. Conf. Information Security and Cryptology (ICISC '04)*, Dec. 2004.

[137] J. Guo, J. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *IEEE INFOCOM Workshop on Mobile Networking for Vehicular Environments (MOVE '07)*, May 2007.

[138] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Computer Communications*, vol. 30, no. 14–15, pp. 2826–2841, 2007.

[139] B. Deosarkar, N. Yadav, and R. Yadav, "Clusterhead selection in clustering algorithms for wireless sensor networks: A survey," in *Int. Conf. Computing, Communication and Networking (ICCCN '08)*, Aug. 2008.

[140] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Trans. Vehicular Technology*, vol. 59, no. 4, pp. 1606–1617, 2010.

[141] M.-H. Park, G.-P. Gwon, S.-W. Seo, and H.-Y. Jeong, "RSU-Based Distributed Key Management (RDKM) For Secure Vehicular Multicast Communications," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 644–658, 2011.

[142] Y. Hao, Y. Chengcheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 616–629, 2011.

[143] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *CRYPTO '04*. Springer, Aug. 2004.

[144] Q. Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," *IEEE Trans. Vehicular Technology*, vol. 59, no. 2, pp. 559–573, 2010.

[145] N. M. Rabadi and S. M. Mahmud, "Privacy protection among drivers in vehicle-to-vehicle communication networks," in *4th IEEE Consumer Comm. and Networking Conf. (CCNC '07)*, Jan. 2007.

[146] J. Zhang, L. Ma, W. Su, and Y. Wang, "Privacy-preserving authentication based on short group signature in vehicular networks," in *1st Int. Symp. Data, Privacy, and E-Commerce (ISDPE '07)*, Nov. 2007.

[147] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *11th ACM Conf. Computer and comm. security (CCS '04)*, Oct. 2004.

[148] B. Qin, Q. Wu, J. Domingo-Ferrer, and L. Zhang, "Preserving security and privacy in large-scale VANETs," in *13th Int. Conf. Information and comm. security (ICICS '11)*, Nov. 2011.

[149] H. Xiong, K. Beznosov, Z. Qin, and M. Ripeanu, "Efficient and spontaneous privacy-preserving protocol for secure vehicular communication," in *IEEE Int. Conf. Communications (ICC '10)*, May 2010.

[150] D. Liu, J. Liu, Y. Mu, W. Susilo, and D. Wong, "Revocable ring signature," *Journal of Computer Science and Technology*, vol. 22, pp. 785–794, 2007.

[151] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *27th Conf. Comp. Comm. (INFOCOM '08)*, Apr. 2008.

[152] C. D. Jung, C. Sur, Y. Park, and K.-H. Rhee, "A robust conditional privacy-preserving authentication protocol in VANET," in *Security and Privacy in Mobile Information and Communication Systems*. Springer, 2009.

[153] Z. Tan, "A privacy-preserving mutual authentication protocol for vehicle ad hoc networks," *Journal of Convergence Information Technology*, vol. 5, no. 7, pp. 180–186, 2010.

[154] Y. Sun, Z. Feng, Q. Hu, and J. Su, "An efficient distributed key management scheme for group-signature based anonymous authentication in vanet," *Security and Communication Networks*, vol. 5, no. 1, pp. 79–86, 2012.

[155] L. Malina, J. Castella-Roca, A. Vives-Guasch, and J. Hajny, "Short-term linkable group signatures with categorized batch verification," in *Foundations and Practice of Security*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2013, vol. 7743, pp. 244–260.

[156] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing auditability and privacy in vehicular networks," in *1st ACM Int. workshop on Quality of service & security in wireless and mobile networks (Q2SWinet '05)*, Oct. 2005.

[157] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, "Enforcing privacy using symmetric random key-set in vehicular networks," in *8th Int. Symp. Autonomous Decentralized Systems (ISADS '07)*, Mar. 2007.

[158] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in *IEEE Int. Conf. Comm. (ICC '08)*, May 2008.

[159] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Trans. Vehicular Technology*,

vol. 57, no. 6, pp. 3357–3368, 2008.

[160] C. Laurendeau and M. Barbeau, "Secure anonymous broadcasting in vehicular networks," in *32nd IEEE Conf. Local Computer Networks (LCN '07)*, Oct. 2007.

[161] H.-T. Wu, W.-S. Li, T.-S. Su, and W.-S. Hsieh, "A novel RSU-based message authentication scheme for VANET," in *1st Int. Conf. Systems and Networks Comm. (ICSNC '10)*, Aug. 2010.

[162] M. Riley, K. Akkaya, and K. Fong, "Group-based hybrid authentication scheme for cooperative collision warnings in VANETs," *Security and Comm. Networks*, vol. 4, no. 12, pp. 1469–1482, 2011.

[163] Y.-C. Hu and K. P. Laberteaux, "Strong VANET security on a budget," in *4th Workshop on Embedded Security in Cars (ESCAR '06)*, Nov. 2006.

[164] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *RSA CryptoBytes*, vol. 5, no. 2, pp. 2–13, 2002.

[165] M. Feiri, J. Petit, and F. Kargl, "Congestion-based certificate omission in VANETs," in *9th ACM Int. workshop on Vehicular inter-networking, systems, and applications (VANET '12)*, June 2012.

[166] R. Schmidt, T. Leinmuller, E. Schoch, F. Kargl, and G. Schafer, "Exploration of adaptive beaconing for efficient intervehicle safety communication," *IEEE Network*, vol. 24, no. 1, pp. 14–19, 2010.

[167] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Enhancing security and privacy in traffic-monitoring systems," *IEEE Pervasive Computing*, vol. 5, no. 4, pp. 38–46, 2006.

[168] European Commission, "Directive 95/46/EC of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," *Official Journal of the European Union*, vol. L 281, pp. 31–50, October 1995.

[169] ETSI TC ITS, "ETSI TS 102 636-4-1: "Intelligent Transport Systems (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality " V1.2.0 (2013-10)," Standard, 2013. [Online]. Available: http://www.etsi.org/deliver/etsi_en/302600_302699/3026360401/01.02.00_20/en_3026360401v010200a.pdf

[170] ——, "ETSI TS 102 941 v1.1.1 - intelligent transport systems (ITS); security; trust and privacy management," Standard, TC ITS, 2012. [Online]. Available: http://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.01.01_60/ts_102941v010101p.pdf

[171] ARIB, "T109: 700 mhz band intelligent transport systems; v1.1," Standard, ARIB, 2012. [Online]. Available: http://www.arib.or.jp/english/html/overview/doc/5-STD-T109v1_1-E1.pdf

[172] H.-J. Lim and T.-M. Chung, "A survey on privacy problems and solutions for vanet based on network model," in *11th Int. Conf. on Algorithms and architectures for parallel processing (ICA3PP '11)*. Springer, Oct. 2011.

[173] A. Jaeger, N. Bißmeyer, H. Stübing, and S. A. Huss, "A novel framework for efficient mobility data verification in vehicular ad-hoc networks," *Int. J. Intelligent Transportation Systems Research*, vol. 10, pp. 11–21, 2012.

[174] A. Iyer, A. Kherani, A. Rao, and A. Karnik, "Secure V2V communications: Performance impact of computational overheads," in *IEEE INFOCOM Workshops*, Apr. 2008.

[175] J. Haas, Y.-C. Hu, and K. Laberteaux, "Real-world VANET security protocol performance," in *IEEE Global Telecomm. Conf. (GLOBECOM '09)*, Nov. 2009.

[176] J. Petit, "Analysis of ECDSA Authentication Processing in VANETs," in *3rd IFIP Int. Conf. New Technologies, Mobility and Security (NTMS '09)*, Dec. 2009.

[177] J. Petit and Z. Mammeri, "Analysis of Authentication Overhead in Vehicular Networks," in *3rd IFIP Wireless and Mobile Networking Conf. (WMNC '10)*, Oct. 2010.

[178] J. P. Stotz, N. Bißmeyer, F. Kargl, S. Dietzel, P. Papadimitratos, and C. Schleiffer, "PRESERVE D1.1 security requirements of vehicle security architecture," PRESERVE consortium, Deliverable, 2011.

[179] M. Nowatkowski, J. Wolfgang, C. McManus, and H. Owen, "The effects of limited lifetime pseudonyms on certificate revocation list size in VANETs," in *IEEE SoutheastCon*, Mar. 2010.

[180] C. Li, J. Jose, and X. Wu, "Distributed-fountain network code (dfnc) for content delivery in vehicular networks," in *10th ACM Int. workshop on Vehicular inter-networking (VANET '13)*, June 2013.

[181] B. Chaurasia, S. Verma, and S. Bhasker, "Message broadcast in VANETs using group signatures," in *4th Int. Conf. Wireless Communication and Sensor Networks (WCSN '08)*, Dec. 2008.

[182] Z. Ma, F. Kargl, and M. Weber, "Measuring long-term location privacy in vehicular communication systems," *Computer Communications*, vol. 33, no. 12, pp. 1414–1427, 2010.

[183] D. Chaum, "The dining cryptographers problem: unconditional sender and recipient untraceability," *J. Cryptol.*, vol. 1, no. 1, pp. 65–75, 1988.

[184] B. C. M. Fung, K. Wang, R. Chen, and P. S. Yu, "Privacy-preserving data publishing: A survey of recent developments," *ACM Comput. Surv.*, vol. 42, no. 4, pp. 1–53, 2010.

[185] C. Dwork, "Differential privacy," in *Int Conf. Automata, Languages and Programming (ICALP '06)*, July 2006.

[186] F. Kargl, A. Friedman, and R. Boreli, "Differential privacy in intelligent transportation systems," in *6th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '13)*, Apr. 2013.

[187] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J.-C. Herrera, A. M. Bayen, M. Annavaram, and Q. Jacobson, "Virtual trip lines for distributed privacy-preserving traffic monitoring," in *6th Int. Conf. Mobile systems, applications, and services (MobiSys '08)*, June 2008.

[188] D. Rebollo-Monedero, J. Parra-Arnau, C. Diaz, and J. Forne, "On the measurement of privacy as an at-

tacker's estimation error," *Conf. Journal of Information Security*, vol. 12, no. 2, pp. 129–149, 2013.

[189] C. Troncoso, E. Costa-Montenegro, C. Diaz, and S. Schiffner, "On the difficulty of achieving anonymity for vehicle-2-x communication," *Comput. Netw.*, vol. 55, pp. 3199–3210, Oct. 2011.

[190] N. Bissmeyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for vanets based on mobility data plausibility," in *9th ACM Int. workshop on Vehicular inter-networking, systems, and applications (VANET '12)*, June 2012.

[191] K. Wevers, A. Yuen, C. Brown, C. Zott, A. Hiller, F. Ahlers, S. Dreher, T. Schendzielorz, C. Bartels, Z. Papp, and B. Netten, "SAFESPOT D3.3.3 local dynamic maps specifications," SAFESPOT consortium, Deliverable, 2008.

Jonathan Petit is a postdoctoral fellow in the Services, Cybersecurity and Safety group at the University of Twente, Netherlands. He received his PhD degree in Networks, Systems and Architecture from the University of Toulouse, France, in 2011. He is technical coordinator of the European FP7 PRESERVE project. His research interests include security and privacy, intelligent transportation system, wireless and vehicular communication.

Florian Schaub is a postdoctoral fellow in the School of Computer Science at Carnegie Mellon University. He received his PhD in Computer Science from the University of Ulm, Germany. He further holds a Diplom in Computer Science from the University of Ulm, and a Bachelor in Information Technology (Multimedia Technology) from Deakin University, Australia. His research is focused on human factors of privacy, as well as usable and context-adaptive privacy mechanisms. Further research interests include intelligent transportation systems, ubiquitous computing, mobile security, and human-computer interaction.

Michael Feiri is a PhD candidate in the Services, Cybersecurity and Safety research group at the University of Twente. He holds a Diplom in Computer Science from the University of Ulm. His research is focused on key management and broadcast authentication in vehicular networks.

Frank Kargl Frank Kargl holds the chair of Distributed Systems at University of Ulm, as well as a part-time professor position in the SCS group at the University of Twente. His research interests include dynamic and cooperative distributed systems and their security and privacy with a special focus on cooperative intelligent transportation systems. In this area, he participated in a number of projects, like SeVeCom and PRECIOSA. Currently, Frank Kargl is coordinator of the on-going PRESERVE project that aims to make security and privacy in V2X a reality for the upcoming ITS deployment. He co-authored more than 100 peer-reviewed publications and is actively contributing to the cooperative ITS community through participation in bodies like the C2C-CC and as co-chair of events like ACM WiSec, IEEE WiVeC, or IEEE VNC.