Chapter 9
Privacy of Connected Vehicles

Jonathan Petit, Stefan Dietzel, and Frank Kargl

Abstract By enabling vehicles to exchange information with infrastructure and other vehicles, connected vehicles enable new safety applications and services. Because this technology relies on vehicles to broadcast their location in clear text, it also raises location privacy concerns. In this chapter, we discuss the connected-car ecosystem and its underlying privacy threats. We further present the privacy protection approach of short-term identifiers, called pseudonyms, that is currently foreseen for emerging standards in car-to-X communication. To that end, we discuss the pseudonym lifecycle and analyze the trade-off between dependability and privacy requirements. We give examples of other privacy protection approaches for pay-as-you-drive insurance, sharing of trip data, and electric vehicle charging. We conclude the chapter by an outlook on open challenges.

9.1 Introduction

A lot of research on location privacy has focused on privacy of transportation systems and, particularly, of vehicles. As cars become more and more equipped with information and communication technology, they facilitate recording, storage, transmission, and processing of location data. Protecting driver privacy despite this information exchange is a particular challenge, because location information often has special semantics that can be leveraged by adversaries interested in tracking. For example, vehicles follow certain mobility patterns rather than moving randomly.

J. Petit (✉)
OnBoard Security, Wilmington, MA, USA
e-mail: jpetit@onboardsecurity.com

S. Dietzel
Department of Computer Science, Humboldt-Universität zu Berlin, Berlin, Germany
e-mail: stefan.dietzel@hu-berlin.de

F. Kargl
Institute of Distributed Systems, Ulm University, Ulm, Germany
e-mail: frank.kargl@uni-ulm.de

A. Gkoulalas-Divanis, C. Bettini (eds.), *Handbook of Mobile Data Privacy*,
https://doi.org/10.1007/978-3-319-98161-1_9

This behavior allows to predict future positions and, thereby, allows to link even otherwise perfectly anonymous position data. In addition, linked (and unlinked) location samples may be correlated with user-specific points of interest, such as their known home or work addresses. Finally, location samples may not be perfectly anonymous—but rather pseudonymous—in order to support information integrity or authenticity requirements.

Douriez et al. [4] provide an illustrative example for how knowledge of location traces can negatively affect privacy, even when data is seemingly anonymized. New York City's taxi and limousine commission (TLC) published purportedly anonymized historical data of yellow cab trips in New York City. The published information consists of pick-up and drop-off locations and times, together with other data, such as, the distance, duration, fare, and tip for millions of trips. Although the published information did not contain any direct identifiers, people quickly started to de-anonymize the published data and link trips to individuals using freely available information. For instance, public pictures of celebrities entering cabs were linked to trip information using the pictures' meta information.

Linking these taxi trips is just one example that used a—relatively speaking—small data set. Under the term "connected vehicle," car manufacturers, fleet operators, and public authorities are preparing to exploit the numerous benefits of always knowing where each vehicle is located at every point in time. Such data is often called floating car data (FCD) and basically consists of data records with timestamp, position, vehicle identifier or pseudonym, speed, heading, and potentially other data about a single vehicle or about large numbers of vehicles. Using FCD, logistics operators can track their fleet, rental cars can be prevented from leaving their allowed operation region, city-wide traffic can be analyzed and optimized, and vehicles on a colliding trajectory can warn their drivers to break—to name just a few of the many possible applications.

Car-to-car (C2C) communication—also called vehicle-to-vehicle (V2V) communication—characterizes a particular flavor of a connected car where cars use short-range radio communication or cellular networks to communicate FCD to other vehicles in their vicinity. In contrast to other FCD applications, C2C communication is particularly interesting from a privacy perspective, because the foreseen information exchange largely relies on broadcasts: all vehicles frequently make their current FCD information known to all vehicles within their vicinity openly, that is, without any encryption. The underlying message formats have been standardized in both the EU, where they are called cooperative awareness message (CAM) [8], and in the US, where they are called basic service message (BSM) [36].

As has been done for the taxi data set, a large body of work has repeatedly shown that even anonymized or pseudonymized position samples can often be linked [11, 15, 20, 32, 42]. Once linked, the information reveals complete vehicle trips. In many circumstances, it may also be attributed to specific vehicles or drivers using known information about their home or work places. These works point out how badly weak privacy protection in connected cars could influence drivers' privacy and, consequently, market acceptance of such systems.

In general, it depends a lot on the particular scenario and application whether FCD is only communicated to close-by vehicles or gathered in global databases. Likewise, application requirements dictate whether data is used and stored temporarily or retained more permanently. But no matter what the particular application at hand is, it is clear that the frequent exchange of location information by connected cars creates privacy issues that need to be investigated and solved before their widespread deployment. Therefore, research and standardization have early on worked on privacy solutions to better protect location privacy for connected cars in a multitude of scenarios.

In this chapter, we will provide an overview of solutions and challenges in many common applications of car-to-X (C2X) communication. We will mostly focus on technical solutions while being aware that complementing protection must be established at a regulatory and policy level to provide clear rules on when and how location data from connected cars may be used. Section 9.2 will introduce a system model for connected cars that provides the basis for our further discussion. Section 9.3 discusses attacker models for connected cars to show how location privacy may be infringed. Next, we discuss privacy protection mechanisms for vehicle-to-vehicle communication in Sect. 9.4, and we discuss solutions for other vehicular services—such as pay-as-you-drive (PAYD) insurance, traffic analysis, and electric vehicle charging—in Sect. 9.5. We conclude this chapter with an outlook on open challenges in Sect. 9.6.

9.2 System Model

Nowadays, vehicles increasingly connect with other vehicles, other road users, infrastructure, and Internet services. Interconnecting these systems has the potential to increase safety, efficiency, and comfort. But at the same time, making detailed information from a car's sensors available can uncover many details of the drivers' lives. In this section, we give an historic overview of the connected car ecosystem and discuss example applications. We also present representative information exchange paradigms, and we introduce dependability requirements, which render the trade-off between privacy and fitness for safety applications a particular challenge.

9.2.1 The Connected Car Ecosystem

The vision of "connected cars" today subsumes many different ideas, applications, and communication paradigms. The first application scenarios evolved around the idea to automate emergency calls in cases of accidents. Basically, cars were to be equipped with mobile communication units, positioning devices, and crash sensors. Once an accident was detected, all necessary and useful information would be automatically transmitted to emergency responders. Systems that implement such kinds of applications have since been proposed and built by numerous car manufacturers, and they have been mandated by the European Parliament under the name "eCall" to be implemented in all new cars starting in 2018 [33].

The EU's eCall initiative has met resistance by numerous privacy-conscious groups, which demonstrates the fundamental conflict of many connected car applications. If implemented properly, automatic emergency calls can, ultimately, help to save lives. To better help emergency responders, it is beneficial to acquire as much sensor information as possible about the accident's nature and the current state of involved passengers. On the other hand, many questions need to be addressed properly in order to avoid privacy issues. Some examples are:

- Who is allowed to access sensor information?
- Under what circumstances is sensor information transmitted?
- What measures need to be taken to avoid unauthorized access?
- How can tracking during normal driving be prevented?

These questions can—and should—be answered by legislation. But even when access is legally prohibited, collecting and transmitting sensor information remains possible. Therefore, it is important to discuss technical means to protect driver privacy and enforce data collection restrictions.

The emergency call application is just one example that demonstrates the trade-off between application utility and privacy requirements. In general, the connected car ecosystem can be coarsely subdivided into four categories:

1. safety applications,
2. driving efficiency and traffic management applications,
3. vehicular services, and
4. comfort and multimedia applications.

Safety applications aim to make driving safer and to reduce accidents or to provide better help in case of accidents. Some safety applications, such as the eCall discussed above, connect the vehicles to the service providers' backend infrastructure. Other applications depend on frequent exchange of sensor information directly between vehicles without involvement of additional infrastructure. Essentially, vehicles exchange broadcast messages to acquire a detailed view of their surroundings. This overview can be used to warn when drivers undertake dangerous driving maneuvers that may lead to crashes, and it can inform drivers about dangers that are not yet in the driver's field of view. Example applications are forward collision warning, intersection collision avoidance, and emergency electronic brake lights [18, Ch. 2]. Usually, safety applications use two types of information dissemination. Frequent sensor updates are pushed to all vehicles in the direct vicinity, which is typically assumed to be about 100 m in cities and up to 1000 m in highway scenarios. In addition, warnings about specific events may be transmitted to regions of affected vehicles with lower frequency, namely, only when the reported events occur. Besides connecting vehicles, safety applications can benefit from including other road users, such as pedestrians or cyclists, in the information exchange.

Efficiency applications provide support for navigation decisions and improve traffic flow. The simplest—and likely most privacy-preserving—example are traditional navigation systems, which use offline maps only. More advanced navigation systems may incorporate up-to-date traffic information from a centralized server to calculate better routes. At first, traffic information originated from manual observations using video surveillance or inductive loops that count vehicle flow. The acquired information was centrally managed and passively downloaded by individual vehicles. In recent years, navigation system providers have started to directly source information from each vehicle that uses their system. Indeed, navigation systems often come with a cellular data contract included, which is used to upload current location tracks to a centralized server, as well as to download current traffic predictions for requested routes. Current research aims to take live navigation one step further by calculating route recommendations that optimize the whole city's traffic flow rather than individual travel times [e.g., 2]. The more navigation systems use up-to-date sensor information, the higher their potential to infringe on user privacy. The potential danger to driver privacy is twofold: First, drivers that upload their current velocity, time, and location to improve travel time predictions may be subject to detailed surveillance of their whereabouts. Second, requests for current travel time information for specific routes may reveal the driver's destination to the navigation system provider. Sometimes, the way in which collected information affects drivers is surprising: in 2011, a manufacturer of navigation systems sold their gathered traffic information to the local police, which used it to optimize positioning of speed traps [25].

Under the term *vehicular services,* we subsume all kinds of applications that provide additional services based on location information. An increasingly popular example are pay-as-you-drive (PAYD) insurance models. In these models, drivers agree to base their insurance plan on real driving behavior rather than on surveys and statistical information. Some of these tariffs base their prices mainly on driven distance, but other influence factors, such as driving style or dangerous maneuvers can also be conceived to influence pricing. Besides insurance models, electric vehicle charging is another domain that introduces new information exchange patterns, which may influence driver privacy. For maximum convenience, drivers should be able to recharge their vehicles on arbitrary and widely available charging stations. One foreseen mode of operation is that the charging stations automatically detect the connected vehicle and, once the transaction is authorized, bill the consumed amount of energy to the driver's regular electricity plan.

Finally, *comfort and multimedia applications* generally aim to connect vehicles to the Internet. Usually relying to roadside infrastructure or cellular data connections, these applications aim to provide software downloads, updates, video streaming, or social applications to the drivers and passengers. Again, frequent requests for Internet content may enable infrastructure providers to track individual vehicles.

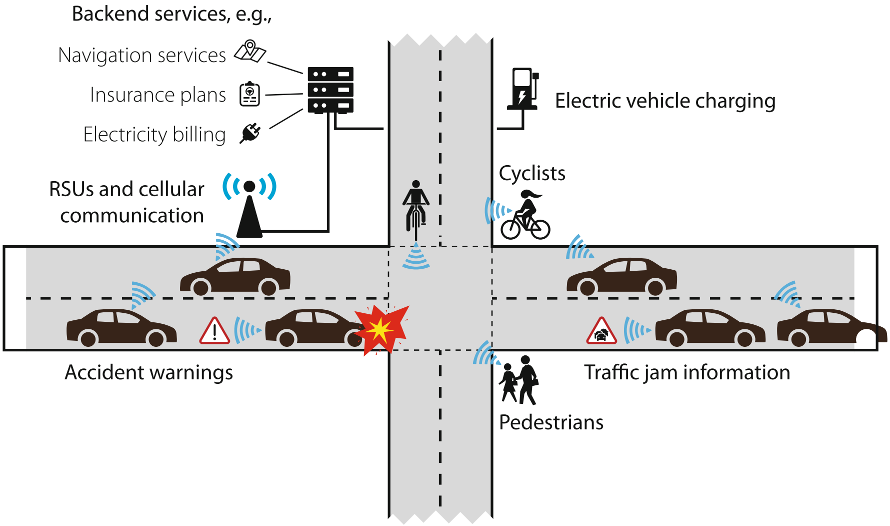

Fig. 9.1 The connected car ecosystem

Figure 9.1 shows an overview of the connected car ecosystem. To enable a wide range of applications, connected cars may exchange information with a wide range of potential communication partners, including

- infrastructure providers, such as, road-side units (RSUs) and traffic management centers (TMCs),
- providers of centralized services,
- other vehicles in their direct surrounding (using one-hop communication),
- other vehicles further away (using multi-hop or relayed communication),
- pedestrians, and cyclists (the latter two being especially vulnerable road users).

The transmitted information is often very detailed, especially when it targets safety applications. For example, very detailed timestamped location traces are required to calculate vehicle trajectories for crash avoidance warnings. Explicit identities of drivers, however, are typically not transmitted, as we will discuss in more detail in Sect. 9.4. Rather, short-term pseudonymous identifiers are used to link individual messages without directly referring to particular vehicles or drivers. Whether the transmitted information constitutes personal information, therefore, is subject to ongoing discussion in different legislations. In the USA, for instance, no federal law exists that governs such information, but existing recommendations and standards such as [6] would not regard most information transmitted by connect cars as personally identifiable. Contrarily in the European Union, the new general data protection regulation [27], which takes effect in 2018, specifically notes that even pseudonymous data falls under privacy regulations.

9.2.2 Information Exchange Paradigms

Researchers and practitioners have come up with a wide range of potential applications for connected cars, which require dissemination of different kinds of information with distinct granularity and frequency within certain regions or towards centralized servers. At the same time, the vehicular communication environment poses complex challenges for successful information transmission. Vehicles move at high speeds, which makes direct wireless communication between vehicles difficult. Also, cars roam within large areas, which makes complete wireless coverage by infrastructure, such as mobile network base stations, difficult. Finally, high vehicle density, such as found in traffic jams, poses scalability challenges for both vehicle-to-vehicle and vehicle-to-infrastructure communication.

As a result of these diverse requirements and challenges, a wide range of specialized information exchange protocols have been proposed [17, 38]. Here, we consider three representative categories of information exchange protocols, which imply different types of privacy properties and requirements:

- infrastructure-based networks,
- direct vehicle-to-vehicle communication, and
- information dissemination in geographic regions.

Infrastructure-based networks are often used for traffic optimization applications. Vehicles are either equipped with cellular network access, such as UMTS or LTE modems, or they use Wifi-style communication with dedicated road-side units. In these scenarios, information is typically collected by one or few centralized servers. As a result, information transmitted using infrastructure-based networks can be protected by encryption against overhearing by unauthorized entities, such as other cars or pedestrians. But since information is centrally collected, the operators of the infrastructure and servers can potentially access information from all vehicles that use the system.

Direct vehicle-to-vehicle communication is a core building block for many safety applications. Vehicles periodically broadcast information about their current location, time, velocity, heading, as well as a number of statistical parameters of their vehicle (e.g., length, width, type). These messages are transmitted up to ten times per second. They are received by all vehicles within wireless range, which is estimated to be between 100 and 1000 m, depending on the environment. Receiving vehicles do not forward these frequent updates, hence limiting their distribution to the direct wireless communication range. The received information is used to build a detailed, up-to-date virtual representation of the vehicles' direct surroundings. Based on this virtual representation, safety applications can calculate trajectories and issue warnings about potential collisions. While the message content does not contain direct identifiers, such as license plate numbers, all messages are signed using short-term cryptographic keys to fulfill dependability requirements. We will discuss signing strategies in more detail in Sect. 9.2.3. This direct type of information exchange potentially allows to build very detailed location tracks. But in contrast to infrastructure-based communication, messages—and consequently, location traces—can only be observed by close-by vehicles.

Geographic dissemination is used in all situations where information is useful for all vehicles within a certain geographic region. Warning all approaching vehicles about the end of a traffic jam or an accident is a typical example. These messages are forwarded using a number of proposed information dissemination and routing protocols (such as [9]) to eventually reach all vehicles within the pre-defined region. In contrast to direct communication, geographic messages are only triggered when specific events, such as accidents, occur. Therefore, geographically disseminated messages unlikely provide sufficient detail for longer location traces. They can, however, be observed by a larger number of vehicles, and they may contain personal information about sending vehicles.

9.2.3 Dependability Requirements

In this section, we focus specifically on dependability requirements for messages that are used for safety applications, as the tension between dependability requirements and drivers' privacy requirements renders protocol design for vehicle-to-vehicle communications particularly challenging. We regard dependability as an overarching design goal that encompasses security features, such as information integrity and accountability; safety requirements, such as required message frequency and real time constraints; and legal issues, such as liability requirements. Schaub et al. [37] presented a number of requirements for privacy-preserving protocol design. Here, we survey those requirements that are, at first sight, particularly contradictory to privacy requirements. We will discuss in Sect. 9.4 how thoughtful protocol design approaches can jointly support these seemingly contradictory requirements.

Real Time Constraints Many applications, including safety applications, require information transmission with low latency and high frequency. Due to their high relative speeds, vehicles may only have a short window to transmit information before they move out of their mutual communication range. In addition, safety applications may need to react quickly in order to prevent accidents, so information should be transmitted with low delay. Finally, safety applications may need to process a number of messages to detect vehicle trajectories or otherwise correlate information. Therefore, information should be transmitted with high frequency to provide sufficient information for trajectory detection.

Linkability In order to process several messages and determine trajectories that may lead to collisions, safety applications may need to link several messages from the same vehicle. If all messages appear to stem from different vehicles, applications may not be able to deduct sufficient information about dangerous situations, as shown by Lefèvre et al. [24].

Authentication Many connected car applications require authentication of participants to prevent unauthorized use. Some applications may be subject to membership fees and may want to avoid that freeloaders use their services without paying. For safety and other vehicle-to-vehicle applications, it may be desirable to exclude adversaries from the network that try to inject or modify messages in the network. Besides authenticating vehicle identities as message senders, authentication may also pertain to specific properties, such as to identify police cars or other vehicle attributes like length, permissible load weight, and so forth.

Accountability Closely related to the authentication requirement is accountability. In certain situations, such as when malicious messages lead to accidents, attacks on connected car applications may constitute crimes. Under those circumstances, it may be desirable to be able to identify and hold liable the individuals that committed those crimes.

Restricted Credential Use When vehicles use credentials, such as asymmetric cryptographic key pairs, it may be desirable to restrict their usage in time and to avoid parallel use. Credentials may be issued for a certain validity period only, and that period should be confirmable by message recipients. Preventing parallel use is a paramount feature to avoid so-called Sybil attacks [3] where a single vehicle could otherwise simultaneously transmit messages under multiple identities. Such Sybil attacks may otherwise lead to false warnings or manipulated navigation decisions.

Revocation In cases where credentials were used to conduct crimes or otherwise interfere with correct system operation, it may be desirable to revoke credentials before their originally intended usage period is over.

Obviously, these dependability requirements influence driver privacy. Many requirements call for identification of the driver's identity under certain circumstances. Or they may necessitate to transmit certain attributes or pseudonymous identities that reduce the potential search space for adversaries that aim to link information to identities.

9.3 Attacker Model

The previous sections illustrated the privacy risks of location tracking and re-identification. In order to understand who can perform such attacks on privacy, we have to define the privacy attacker model. We distinguish three types of attackers [31, 32]:

Local observer: An attacker that is in the vicinity of the target vehicle and can collect its broadcast messages or simply stalk it.

Mid-sized observer: An attacker that does not have a full coverage of the area but rather has sniffing stations located at deemed-strategic spots. This type of attacker collects floating car data (FCD) and may employ algorithms to try and fill their gaps to obtain a real-time location tracking.

Global observer: An all-seeing attacker that has universal coverage and can collect every broadcast messages.

Protection against a local observer is counter-intuitive, as the main benefit of FCD is to create *local awareness*. Therefore, neighboring entities (e.g., vehicles, pedestrians, and cyclists) must be able to track a vehicle in order to avoid collision or create a platoon for example.

The mid-sized attacker is likely to be interested in a zone-level tracking, i. e., knowing in which region a target is instead of an exact street. More sophisticated mid-sized attackers may use forms of re-identification to fill gaps in recorded FCD data. To that extend, the attacker may use computer vision or fingerprinting techniques that are able to distinguish communication devices based on their radio properties [13].

To defend against mid-sized observers, an objective is to harden inferences (e.g. medical condition, relationships, religion). Indeed, the goal of the attacker is to guess movements within gaps in coverage in order to reconstruct tracks (and gain similar knowledge as a global observer). Therefore, by using so-called pseudonyms as short-term identifiers and enforcing change of pseudonyms (see Sect. 9.4), we create more uncertainty, making it harder to perform location tracking. The global observer is even more challenging to prevent, because it can be seen as a constant local observer. So the goal is to create gaps in tracks to shift her toward a mid-sized observer.

Attacks on FCD have already been demonstrated. Petit et al. [32] presented an attack that can be mounted by a mid-sized observer who installs sniffing stations in order to track a target vehicle at a road-level and at a zone-level. This work demonstrates why pseudonyms are mandatory to preserve privacy, and it gives a cost model for frequent pseudonym change strategy.

Wiedersheim et al. [42] analyzed how effectively a global observer can create location profiles. That is, it determined the maximum length of tracks for the same vehicle. Utilizing an approach based on multi-target tracking, the authors found that linking samples under different pseudonyms for the same vehicle can be surprisingly successful under various system setups. Bissmeyer et al. [1] also demonstrated that by solely using the content of cooperative awareness message (CAM) [8] messages they were able to accurately recreate individual vehicles' paths.

Thus, even if pseudonyms are mandatory, one can see that the key question is how to change them so that linking pseudonyms consumes prohibitively time-consuming, requires massive amounts of data, or is computationally infeasible. In the following section, we will delve further into the details of how pseudonyms are used and how their lifecycle can influence or prevent different types of attacks.

9.4 Privacy Protection Using Pseudonyms

Pseudonyms are a wide-spread strategy to combine authentication and accountability requirements with suitable privacy protection. In connected car systems, pseudonyms are the predominant solution to combine dependability and privacy requirements of safety and efficiency applications in car-to-car communication. Pseudonyms' main feature is to prevent trivial linking of all messages from an individual car. In contrast to completely anonymous transmissions, pseudonyms can help to provide authentication and accountability under well-defined circumstances, despite maintaining driver privacy. They allow to link messages that have been sent with the same pseudonym and only break linkability when a vehicle changes its pseudonym. This is important to allow local tracking of vehicles, e.g., to calculate their trajectories. Given a suitable pseudonym scheme, a car's transmitted messages could, for instance, remain completely anonymous and unlinkable until proof for mischievous behavior is brought forward, whereafter the originator of all messages could be identified.

Combining the seemingly contradictory requirements of anonymity (or pseudonymity), linkability for dependability, and accountability, often requires the combination of complex cryptographic primitives, and many such proposals have been discussed in literature [30]. In addition, standardization for vehicle-to-vehicle communication in both the USA [21] and in Europe [7] include pseudonym architectures. Basically, they all follow a similar lifecycle: Each vehicle is first assigned cryptographic credentials—e.g., an elliptic-curve digital signature algorithm (ECDSA) key pair—that are bound to its long term identity, such as a license plate or the car holder's identity. The key pairs can be generated locally and, together with their identifying attributes, are signed by a trusted authority. To prevent trivial privacy leakage, the long term identity is, however, not used to sign outgoing messages. Rather, the vehicle periodically uses its long term identity to obtain one or more certificates for short term credentials, again this can be ECDSA key pairs. These certificates are issued by another trusted authority, and they attest the holder's authenticity but not their identity. Vehicles then use their short term key pairs to sign outgoing messages. Receivers can verify the signature and attached certificate without learning the sender's identity. In cases of misuse, the short term keys' certificates can be used in cooperation with authorized authorities to prevent issuing fresh certificates.

While similar from a bird's eye perspective, many different proposals with distinct features and restrictions exist for each step of the pseudonym lifecycle. Petit et al. [30] provide a comprehensive survey including details on individual pseudonym schemes. Here, we provide an overview of the canonical pseudonym lifecycle.

9.4.1 Canonical Pseudonym Lifecycle

Today, many different proposals for pseudonym schemes exist, and their implementations vary greatly in the used cryptographic primitives. Petit et al. [30] identifies the following generic steps of a pseudonym's lifecycle, as shown in Fig. 9.2.

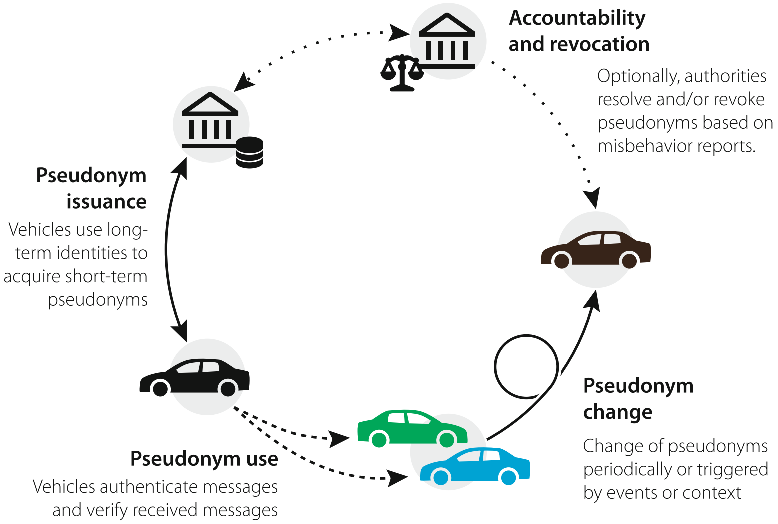
Accountability and revocation
Optionally, authorities resolve and/or revoke pseudonyms based on misbehavior reports.
Pseudonym issuance
Vehicles use long-term identities to acquire short-term pseudonyms
Pseudonym change
Change of pseudonyms periodically or triggered by events or context
Pseudonym use
Vehicles authenticate messages and verify received messages

Fig. 9.2 Abstract pseudonym lifecycle

Pseudonym Issuance First, vehicles contact a centralized authority to obtain one or more pseudonyms. Vehicles typically use their long term identifier to authenticate towards the pseudonym provider. The long term identity can be a form of an electronic license plate that is issued by the same authorities that also manage vehicle registrations. To prevent privacy issues at the Public Key Infrastructure level, another authority acts as pseudonym provider. Usually, more than one pseudonym is requested at once. Pseudonyms are then stored locally in the cars; as part of their certification attributes, they may contain a maximum permitted usage period in order to avoid parallel pseudonym use and pseudonym reuse.

Pseudonym Use Vehicles then use pseudonyms to sign all outgoing messages. Likewise, vehicles use the attached signatures and pseudonymous certificates to verify the authenticity of received messages. The major challenge during pseudonym use is scalability: Vehicles may be required to perform hundreds, perhaps thousands, of signature verifications per second, and they may need to generate ten or more signatures per second. As some pseudonym schemes require computationally expensive cryptographic primitives, it is a challenge to implement sufficiently fast cryptographic processors [35].

Pseudonym Change To prevent the creation of detailed location traces, vehicles should change pseudonyms frequently. One challenge of pseudonym change is scalability: The more often vehicles change their pseudonyms, the more pseudonyms need to be acquired and stored for future use. In terms of privacy, a major challenge is when to perform pseudonym change such that adversaries cannot match the old with the new pseudonym. If, for instance, a sole vehicle changes its pseudonym on an empty road, it is trivial for adversaries to match both pseudonyms.

Accountability and Revocation Finally, it may be desirable to hold drivers accountable for their messages in certain well-defined scenarios. For instance, vehicle-to-vehicle messages may prove involvement in accidents, or it may prove injection of manipulated messages. Depending on legislative requirements, pseudonym schemes should support mechanisms that reveal drivers' identities under these circumstances. Ideally, revealing identities should be *technically* restricted to the scenarios required by law. That is, underlying cryptography—rather than laws and regulations alone—should prevent unlawful pseudonym resolution.

From a privacy perspective, strategies for pseudonym change and mechanisms for accountability and revocation are the most challenging aspects of the pseudonym lifecycle. In the following, we discuss these aspects in more detail.

9.4.2 Pseudonym Change Strategies

When pseudonyms are used to sign messages, messages signed with the same pseudonym can be linked to each other. To achieve privacy, it is therefore necessary to frequently change pseudonyms. It is a difficult challenge, however, to decide in what context and how frequently to change pseudonyms. This difficulty arises, because pseudonym change affects both dependability and privacy. Certain safety applications may require to determine short vehicle trajectories in order to work correctly [24]. For instance, consider an application that warns about potential collisions. To determine whether two vehicles would collide if the drivers do not alter their routes, trajectories are an important source of information. If pseudonyms are changed during intersection crossing, the application will necessarily regard messages signed with the new pseudonyms as originating from a different vehicle. As a result, both false warnings and omitted warnings may occur, which significantly reduces the application's dependability.

In addition, frequent pseudonym change may affect scalability. When pseudonyms are changed frequently—perhaps even after each message—, significant communication capacity, as well as storage and computational capacity is required in order to manage and certify each car's fresh pseudonym pool. From a scalability standpoint, it is, therefore, beneficial to change pseudonyms with lower frequency.

Interestingly, it is also desirable from a privacy standpoint to curate pseudonym changes rather than performing them frequently at will [14]. If only a single vehicle is present on a road segment, it is very likely that an adversary can link its messages despite frequent pseudonym changes. Therefore, it is desirable that vehicles change their pseudonyms in situations where sufficient other vehicles are present, which increase the size of the anonymity set. Also, vehicles should change their pseudonyms within an agreed time period that is preceded by a silence period. That way, attackers can only observe a larger set of pseudonyms before and after the change period, which makes it harder to correlate pseudonyms of individual vehicles. This concept of synchronizing pseudonym change in time and location is known as mix zones [12]. Mix zone placement is complicated by the contradicting requirements of safety applications. For example, intersections are good candidates for ideal mix zone locations, because vehicle density tends to be high in the vicinity of intersections and vehicles change directions there. But as discussed above, intersections are also points with high accident potential where safety applications can benefit from analyzing trajectories. It is a topic of ongoing research where (geographically) and how to implement mix zones for vehicular communication.

9.4.3 Accountability and Revocation

In some situations, it may be desirable to resolve pseudonyms. For example, pseudonyms may help to determine whether drivers were involved in an accident or in a crime scene. Moreover, resolving identities can help to identify people that misuse vehicular communication for their own benefit or to disturb normal system operation. When such misuse is detected, resolved identities can be used to revoke other active pseudonyms of the same user or to invalidate their long term identity. Whether and to what extent such pseudonym resolution and revocation functionality should be implemented is a topic of active debate, and it is a question that cannot be answered technically. Here, we give an overview of technical solutions that can be implemented to support a pseudonym resolution and revocation mechanism that prevents misuse by network operators and authorities.

The simplest solution for pseudonym resolution is to keep a mapping from all issued pseudonyms to their corresponding long term identity at a centralized entity. This implementation, however, would allow operators of the centralized service to reveal identities at will. More advanced resolution mechanisms, as proposed in the US by the Crash Avoidance Metrics Partnership (CAMP), are based on the idea to distribute pseudonym resolution authority over several entities to avoid misuse by individuals. For example, pseudonym distribution can be distributed over regional pseudonym authorities, so that these distributed authorities need to be contacted for pseudonym resolution. Similarly, secret sharing techniques can be used to encrypt pseudonym-identity links such that at least k out of n authorities need to cooperate before a pseudonym's corresponding identity can be decrypted.

Once pseudonyms are linked, it depends on the pseudonym lifetime how their revocation should be implemented. If pseudonyms are restricted to short lifetimes anyways, the central authority can simply revoke the vehicle's long term identity in order to prevent further misuse. Otherwise, so-called certificate revocation lists can be used to revoke individual pseudonyms before they expire. These lists contain—usually in an efficiently encoded form—the identifiers of all pseudonyms that are to be revoked. It is, however, challenging to implement timely and scalable dissemination of such certificate revocation lists.

9.5 Privacy Protection for Vehicular Services

In the previous section, we discussed how pseudonyms can improve privacy in safety-oriented vehicle-to-vehicle communication. In other scenarios, where FCD is collected, stored, and processed in backend systems, different solutions are required for privacy protection. Here, application-specific privacy protection designs are required, which are engineered individually on a case-by-case basis following a privacy-by-design approach.

Exemplarily, we will discuss solutions for three increasingly common example applications: pay-as-you-drive (PAYD) insurance, collection of trip data for traffic analysis, and automated charging for electric vehicles.

9.5.1 Pay-as-You-Drive Insurance

Troncoso et al. [40, 41] discussed the concept of so-called pay-as-you-drive (PAYD) insurance and its implications for drivers' privacy. The basic idea of PAYD systems is that you can earn an additional discount on your car insurance fee by adhering to certain rules laid out in your insurance policy. You may, for example, only drive a certain maximum distance per year or not speed more often than twice a year. Rather than relying on statistical information, your insurance company verifies that you comply with these rules before granting you the discount.

First, the authors surveyed a number of PAYD insurance providers and conclude that a common approach is to install a tracking device in the car that monitors driving behavior and reports this data via cellular network to a central database where it is evaluated for compliance. This architecture is shown in Fig. 9.3 (left).

In order to check eligibility for the discount, the insurance company evaluates the data sent by the vehicles. Some of the surveyed companies also evaluate the data for secondary purposes or provide access to third parties, typically in anonymized or aggregated form. Obviously, this approach requires substantial trust of users in insurance companies to handle the data correctly and keep it secure from malicious access.

The authors therefore propose an alternative scheme called PriPAYD, which is illustrated in Fig. 9.3 (right). It basically relies on a trustworthy black box being installed in the car, which will—locally and offline—determine the appropriate insurance fee and report it to the insurance company. The company then uses the aggregated data for billing, and therefore, no position information leaves the car. Both the insurance company and the user, however, have to trust the black box to correctly calculate the fee. Both would have a rational interest in cheating with the box, the insurance company to raise the fee, the driver to lower it.

Therefore, PriPAYD foresees an audit mechanism, which enable both parties to verify that the correct fee was calculated. The black box inside the car records all data necessary for calculating the insurance fee, such as, distance driven, speeds,

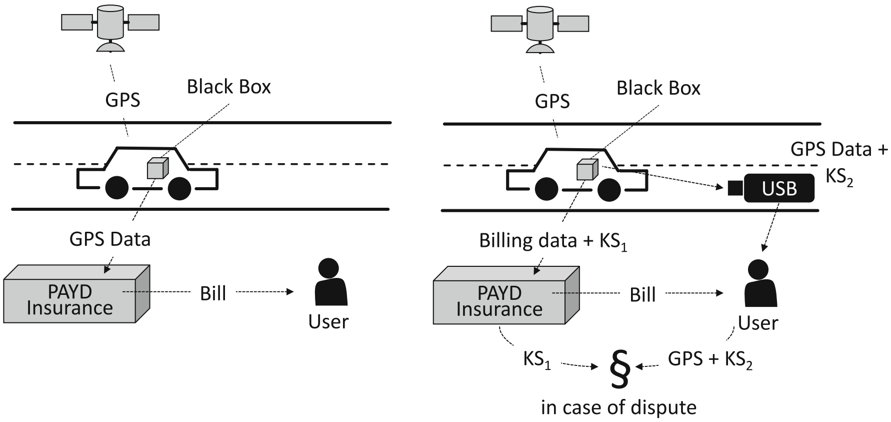

Fig. 9.3 Pay-as-You-Drive insurance models, once with the classical, privacy-invasive model (left) and once with the PriPAYD model that ensures no user data is inadvertently leaked (right)

GPS positions, and so forth, in encrypted form on a removable storage device, such as, a USB stick. The encryption key is split into two key shares ks_1 and ks_2; one is given to the driver, and the other one is sent to the insurance company. In case of a dispute, both parties have to combine the key shares and to decrypt the raw data in order to verify whether the correct fee was calculated.

Kargl et al. [22, 23] report on an architecture for enforcement of privacy policies relying on trusted computing mechanisms that provide a different approach to build generic systems that can enforce privacy policies of arbitrary kinds which is also suitable for PAYD insurance scenarios.

9.5.2 *Privacy-Preserving Sharing of Trip Data*

Next, we want to focus on another common privacy problem in transportation systems. Municipalities and other organizations are often interested in trip data. Especially, they want to find out which vehicles went from which origin to which destination. Knowing how many vehicles travel from one part of the city to another at certain times of the day is very useful for, amongst others, road capacity planing. So far, inductive loops or manual traffic counts are often used to get this kind of data. But using connected vehicles, the vehicles themselves could report where they are traveling to provide more detailed and accurate information.

Most people will happily contribute to such a data collection in anonymized form, but may feel uneasy with the idea that every trip they do is recorded and may potentially be deanonymized based on their specific origin-destination pairs. One potential solution to the problem is to report trip origins and destinations in coarser detail. For instance, a vehicle may only report to have driven from on district of the town to another. Ideally, the granularity would be determined such that your own trip becomes *k-anonymous* with k other trips with same origin-destination pairs. If many vehicles do similar trips, you can report more precise data, but if you are the only one going from place A to place B, you will reduce the level of detail accordingly.

Mechanisms like this and similar ideas have been proposed based on a central proxy that collects all the data and then adjusts the spatial and temporal granularity of data accordingly [16]. Eliminating the need for a central trusted entity, Förster et al. [11] propose a distributed scheme that achieves the same goal. The distributed scheme consists of three phases:

1. Participants establish location- and time-specific keys, both at the start and destination of their trips. They do this by exchanging key shares with other nearby vehicles, eventually converging towards the same keys for certain spatial and temporal granularity levels. The scheme assumes a global spatial and temporal granularity hierarchy to be a pre-defined system parameter. The authors show via simulations that the success rate of this decentralized key agreement scheme is reasonably close to the theoretically achievable maximum.
2. Participants upload copies of their trip reports with different accuracy levels, encrypted with the appropriate keys from step 1, to the trip database. The system defines a decentralized, non-interactive secret sharing scheme by which each vehicle additionally uploads one share of each key to a central database.
3. Traffic authorities query the trip database. If, for a certain temporal and spatial granularity level, enough key shares have been uploaded, they will be able to reconstruct this key and can decrypt the corresponding reports. This is true only if at least k vehicles have uploaded trip reports for the same origin-destination pair, and thus, provided key shares to the corresponding location- and time-specific key. Therefore, the scheme naturally ensures k-anonymity. Obviously, the chance of collecting sufficient key shares for decryption increases with coarser spatial and temporal resolution.

The interesting aspect of this scheme is that, while the application requires central collection of mobility data, the scheme itself does not require trust in any central entity to ensure privacy. Establishing keys locally among neighboring cars using direct car-to-car communication together with a secret-sharing-scheme is sufficient to provide a fully de-centralized privacy protection mechanism that only reveals data if k-anonymity can be maintained.

9.5.3 Privacy-Preserving Charging of Electric Vehicles

Another domain of connected vehicles is communication of electric vehicles with charging infrastructure. The ISO/IEC norm 15118 [34] defines standards for smart charging where vehicles communicate with the road-side charging units and backend systems in order to authenticate the vehicle, control the charging process, and digitally sign the charging bill in order to automate payment.

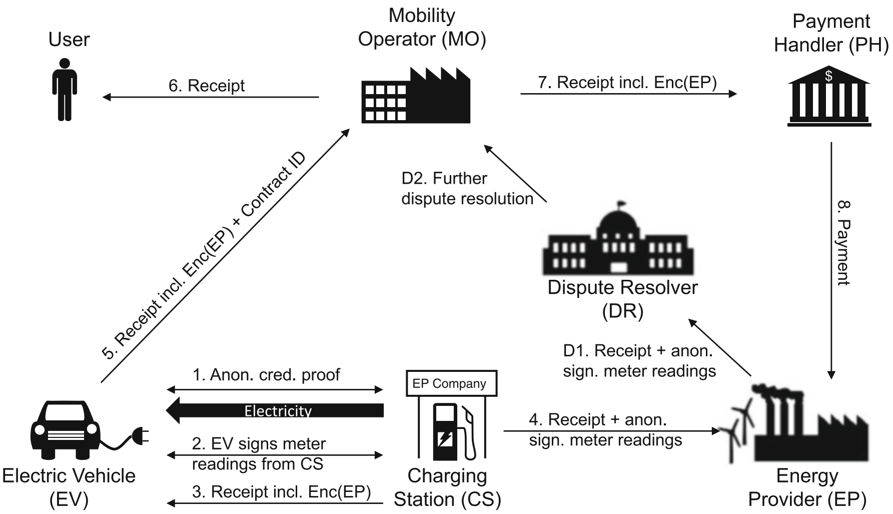

Fig. 9.4 POPCORN protocol for privacy-preserving charging of electric vehicles

Figure 9.4 illustrates a privacy-preserving variant of the ISO's protocol called POPCORN. The norm itself foresees the electric vehicle (EV), charging station (CS), the mobility operator (MO), and the electricity provider (EP) as acting entities. POPCORN in its full version adds a payment handler (PH) and dispute resolver (DR). EV uses a communication link to CS to authenticate via MO with whom it has a contractual relationship to settle the bills incurred during charging. During charging, V will periodically digitally sign partial bills that CS will forward to MO and EP after charging completed. Finally, MO will use the billing information to pay EP.

While this high degree of automation is very convenient from a usability point of view—the driver just plugs the car in and out of the charging station and everything else happens automatically—, the norm lacks a proper treatment of privacy concerns. Particularly, MO and EP will both learn about every charging process, including the location of the CS and thus the EV. Hence, they are in the position to generate fine-grained mobility traces, particularly if one assumes widely spread charging stations and frequent vehicle charging. Current discussions on inductive charging, where an enhanced version of ISO 15118 will be used, will foster this trend.

Höfer et al. [19] have taken these privacy concerns as a motivation to first conduct a privacy impact assessment (a PIA) to clearly identify the privacy shortcomings of the standard. They furthermore propose a step-wise reengineering of the protocols. The result is a privacy-enhanced version of ISO 15118, which they call POPCORN.

As illustrated in Fig. 9.4, POPCORN applies group signatures (GS) and anonymous credentials (AC) to build a protocol that is functionally identical with the original ISO protocol in that drivers can plug in and out from the charging station and everything else happens automatically in the backend systems. At the same time, vehicles will remain anonymous to the CS and EP, and the MO will not learn where its customers have been charging. So location privacy is fully provided except in the case of payment irregularities where a trusted dispute resolver will be provided with encrypted evidence that can be used to link vehicles to a charging process.

In an initialization phase, EVs get equipped with credentials for the GS and AC schemes. When an EV connects to a CS (1.), it creates an AC proof that it is eligible to charge and provisioning of electricity starts. The EV will periodically receive meter readings from the CS which it signs with its GS credentials (2.). When charging ends, the CS provides a receipt to the EV (3.) and the EP (4.). Here, it is important to note that receipt in step 3 contains the recipient of the payment in encrypted form that only the PH can decrypt and that the receipt in step 4 does not reveal the identity of the EV or details on the MO (this would only be deducible through the GS by the DR which is the group manager for the GS). EV forwards the receipt augmented with its contract ID to the MO (5.) which will send the receipt to the user for information purposes (6.) and will trigger the payment via the PH (7.). Here, MO does not learn the recipient of the payment, this is only revealed to the PH when it decrypts $Enc(EP)$. On the other hand, PH will not receive details about the EV involved in this payment and therefore the scheme achieves unlinkability of payments. Payment is then forwarded to the EP (8.) and the process ends. If EP detects unpaid bills, it can trigger dispute resolution (D1.) by sending the (group-) signed meter readings, receipt and other proof data to DH. As key distribution center of the group signature scheme, DH (and only DH) is able to reveal the identify from the signed meter readings and can inform MO about the missing payment (MO) to further investigate and resolve the issue.

Fazouane et al. [10] verified the protocol using a model-checking approach to formally verify the privacy properties of POPCORN, thereby identifying one collusion attack that the original paper missed to notice and proposed a fix to the protocol to resolve the issue.

POPCORN and its enhanced version illustrate how existing protocols that have deficiencies in location privacy can be re-engineered to come up with functionally equivalent solutions that provide strong privacy guarantees.

9.6 Open Challenges and Conclusion

In this chapter, the connected-car ecosystem and its underlying privacy threats were discussed. We presented the privacy protection approach of short-term identifiers, called pseudonyms, and discussed its lifecycle. Then, we analyzed the trade-off between dependability and privacy requirements before presenting examples of other privacy protection approaches for pay-as-you-drive insurance, sharing of trip data, and electric vehicle charging.

Despite the large body of work on location privacy protection for FCD in vehicular systems, researchers have not yet found the optimal solution to jointly maximize privacy, dependability, and utility. In this section, we highlight a couple of open challenges and give directions to address them.

Pseudonym Change Strategy As discussed earlier in this chapter, pseudonym changes have to be carefully orchestrated to be efficient against location tracking by mid-sized and global attackers. Privacy is context-dependent, and so should be the pseudonym change strategy. Depending on the activity performed or the area passed by, the pseudonym change strategy can be more or less effective. For example, grid-style road network patterns offer a higher intrinsic level of privacy than other road networks because of its high density of intersections [28]. Therefore, researchers should define a context-adaptive pseudonym change system. For example, Emara, Woerndl, and Schlichter [5] proposed a scheme that adapts the strategy according to the density of neighboring vehicles and the user privacy preferences. This work could be extended by also considering the type of road network.

Impact of Privacy Protection Lefèvre et al. [24] were the first to investigate the impact of privacy protection techniques on safety applications. Their impact, however, extends beyond safety applications. For example, pseudonym changes and silent periods can affect the computation of estimated travel time (which is an important metric for traffic planning) [43]. Thus, one should take a holistic approach on privacy and perform a comprehensive analysis of its impact, individually for each application and also on the whole communication stack, as noted by Schoch et al. [39]. The impact of pseudonymity on safety raises the question of its impact on FCD utility as a whole. Analyzing how the use of pseudonyms could affect data analyses using collected FCD is an open research question.

Cross-Reference and Re-identification of FCD FCD are being shared between stakeholders (e.g., original equipment manufacturers, service providers, data aggregators). It is a challenge, however, to prevent cross referencing of FCD datasets with each other and with external information that would lead to re-identification of drivers or inference of sensitive information [26, 29]. A survey of location data stakeholders in automotive systems should be performed in order to identify threats and to design corresponding privacy controls.

Privacy of Automated Vehicles automated vehicles (AVs) require a rich data set in order to fully exploit their potential. For example, AVs will form a platoon and, thus, should share their final destinations to ensure stable groups. So, by sharing rich data sets, the privacy concerns increase. Also, because AV cannot rely on a human operator anymore, it is important to maximize predictability, which may render pseudonyms less effective. Knowing how an AV reacts makes profiling (and prediction) easier and more accurate. Therefore, sharing of AV data exhibits more stringent privacy requirements than connected vehicle data. One challenge is to design a privacy-preserving AV data sharing protocol while ensuring a high level of dependability.

Research and industry are well aware of these and other issues involved in making connected cars a success, and there are strong efforts to protect privacy and, particularly, to ensure driver acceptance of such new technologies. At the same time, there are a hard challenges that need to be solved, and a constant privacy engineering effort is required to make sure that future connected vehicles will not become a “big brother” on wheels. With this chapter, we have provided a broad overview on the various aspects of location privacy for connected vehicles, and we have shown where contradictions between dependability and privacy requirements can be solved using clever protocol designs and where further work is required.

References

1. Norbert Bissmeyer et al. “Assessment of Node Trustworthiness in VANETs Using Data Plausibility Checks with Particle Filters”. In: Nov 2012. https://doi.org/10.1109/VNC.2012.6407448
2. D. Cagara, B. Scheuermann, and A. L. C. Bazzan. “Traffic Optimization on Islands”. In: *2015 IEEE Vehicular Networking Conference (VNC)* Dec. 2015, pp. 175–182. https://doi.org/10.1109/VNC.2015.7385574
3. John Douceur. “The Sybil Attack”. In: *Iptps ’01: First International Workshop on Peer-to-Peer Systems* Springer, 2002, pp. 251–260.
4. Marie Douriez et al. “Anonymizing NYC Taxi Data: Does It Matter?” In: *Proc. of IEEE Intl. Conf. on Data Science and Advanced Analytics (DSAA ’16)* Montreal, Canada, Oct. 2016.
5. Karim Emara, Wolfgang Woerndl, and Johann Schlichter. “CAPS: Context-Aware Privacy Scheme for VANET Safety Applications”. In: *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks* WiSec ’15. New York, NY USA: ACM, 2015, 21:1–21:12. ISBN: 978-1-4503-3623-9. https://doi.org/10.1145/2766498.2766500
6. Erika McCallister Tim Grance, and Karen Scarfone. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* Special Publication SP 800-122. NIST, 2010. URL: https://doi.org/10.6028/NIST.SP.800-122
7. ETSI. *Intelligent Transport Systems (ITS); Security; ITS Communications Se- curity Architecture and Security Management* TS 102 940. 2012.
8. ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service* EN 302 637–2. 2013.
9. ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service* EN 302 637–3. 2013.
10. Marouane Fazouane et al. “Formal Verification of Privacy Properties in Electric Vehicle Charging”. In: *Engineering Secure Software and Systems* Springer Cham, Mar 4, 2015, pp. 17–33. https://doi.org/10.1007/9783319156187_2
11. David Förster, Frank Kargl, and Hans Löhr. “A Framework for Evaluating Pseudonym Strategies in Vehicular Ad-Hoc Networks”. In: *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Net- works* WiSec ’15. New York, NY USA: ACM, 2015, 19:1–19:6. ISBN: 978-1-4503-3623-9. https://doi.org/10.1145/2766498.2766520
12. J. Freudiger et al. “Mix-Zones for Location Privacy in Vehicular Networks”. In: Vehicular Networks (VNs) seek to provide, among other applications, safer driving conditions. To do so, vehicles need to periodically broadcast safety messages providing preciseposition information . . . 2007.
13. Ryan M. Gerdes et al. “Device Identification via Analog Signal Fingerprint- ing: A Matched Filter Approach.” In: *NDSS* 2006.
14. M. Gerlach and F. Guttler “Privacy in VANETs Using Changing Pseudonyms Ideal and Real”. In: *Vehicular Technology Conference 2007. VTC2007- Spring. IEEE 65th* Apr 2007, pp. 2521–2525. https://doi.org/10.1109/VETECS2007.519

15. Philippe Golle and Kurt Partridge. “On the Anonymity of Home/Work Loca- tion Pairs”. In: *Pervasive Computing* Springer Berlin, Heidelberg, May 11, 2009, pp. 390–397. https://doi.org/10.1007/9783642015168_26
16. Marco Gruteser and Dirk Grunwald. “Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking”. In: *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services* MobiSys ’03. New York, NY USA: ACM, 2003, pp. 31–42. https://doi.org/10.1145/1066116.1189037
17. H. Hartenstein and L. P. Laberteaux. “A Tutorial Survey on Vehicular Ad Hoc Networks”. In: *IEEE Communications Magazine* 46.6 (June 2008), pp. 164–171. ISSN: 0163-6804. https://doi.org/10.1109/MCOM.2008.4539481
18. Hannes Hartenstein and Kenneth Laberteaux, eds. *VANET Vehicular Applica- tions and Inter-Networking Technologies* 1 edition. Chichester U.K: Wiley Feb 15, 2010. 466 pp. ISBN: 978-0-470-74056-9.
19. Christina Höfer et al. “POPCORN: Privacy-Preserving Charging for Emobility”. In: *Proceedings of the 2013 ACM Workshop on Security Privacy & Dependability for Cyber Vehicles* CyCAR ’13. New York, NY USA: ACM, 2013, pp. 37–48. ISBN: 978-1-4503-2487-8. https://doi.org/101145/25179682517971
20. Baik Hoh et al. “Enhancing Security and Privacy in Traffic-Monitoring Systems”. In: *IEEE Pervasive Computing* 5.4 (Oct. 2006), pp. 38–46. ISSN: 1536-1268. https://doi.org/10.1109/MPRV.2006.69
21. “IEEE Standard for Wireless Access in Vehicular Environments Security Ser vices for Applications and Management Messages”. In: *IEEE Std 1609.2-2016* (2016), pp. 1–289. https://doi.org/10.1109/IEEESTD.2016.7426684
22. Frank Kargl, Florian Schaub, and Stefan Dietzel. “Mandatory Enforcement of Privacy Policies Using Trusted Computing Principles”. In: *Intelligent Information Privacy Management Symposium (Privacy 2010)* Stanford University USA: AAAI, Mar 2010.
23. Frank Kargl et al. “Enforcing Privacy Policies in Cooperative Intelligent Transportation Systems”. In: *ACM 15th Annual International Conference on Mobile Computing and Networking (ACM Mobicom 2009) Poster Session* Beijing, China, Sept. 2009.
24. S. Lefevre et al. “Impact of V2X Privacy Strategies on Intersection Collision Avoidance Systems”. In: *2013 IEEE Vehicular Networking Conference* Dec. 2013, pp. 71–78. https://doi.org/10.1109/VNC.2013.6737592
25. Maija Palmer. *TomTom Sorry for Selling Driver Data to Police* Financial Times. 2011. URL: https://wwwft.com/content/3f80e432719911e09b7a00144feabdc0 (visited on 01/09/2017).
26. Min Mun et al. “PDVLoc: A Personal Data Vault for Controlled Location Data Sharing”. In: *ACM Transactions on Sensor Networks* 10.4 (2014).
27. *On the Protection of Natural Persons with Regard to the Processing of Per sonal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* 2016.
28. Balaji Palanisamy and Liu Ling. “Attack-Resilient Mix-Zones over Road Networks: Architecture and Algorithms”. In: *IEEE Transactions on Mobile Computing* 14.3 (2015), pp. 495–508.
29. Fayola Peters et al. “Balancing Privacy and Utility in Cross-Company De- fect Prediction”. In: *IEEE Transactions on Software Engineering* 39.8 (2013), pp. 1054–1068.
30. J. Petit et al. “Pseudonym Schemes in Vehicular Networks: A Survey”. In: *IEEE Communications Surveys Tutorials* PP.99 (2014), pp. 1–1. ISSN: 1553-877X. https://doi.org/10.1109/COMST.2014.2345420
31. Jonathan Petit, Michael Feiri, and Frank Kargl. “Revisiting Attacker Model for Smart Vehicles”. In: Sept. 2014. https://doi.org/10.1109/WIVEC.2014.6953258
32. Jonathan Petit et al. “Connected Vehicles: Surveillance Threat and Mitigation”. In: *Black Hat Europe* Nov 2015.
33. *Regulation (EU) 2015/758 of the European Parliament and of the Council of 29 April 2015 Concerning Type-Approval Requirements for the Deployment of the eCall in-Vehicle System Based on the 112 Service and Amending Directive 2007/46/EC* 2015.
34. *Road Vehicles – Vehicle to Grid Communication Interface* ISO 15118. ISO/IEC.

35. Carsten Rolfes et al. *PRESERVE Deliverable 3.2: FOT Trial 2 Results* July 31, 2015. URL: https://www.preserve-project.eu/deliverables
36. SAE. *Dedicated Short Range Communications (DSRC) Message Set Dictionary* Standard J2735. SAE, 2016.
37. F Schaub, Zhendong Ma, and F Kargl. “Privacy Requirements in Vehicular Communication Systems”. In: *International Conference on Computational Science and Engineering, 2009. CSE ’09* Vol. 3. Aug. 2009, pp. 139–145. https://doi.org/10.1109/CSE.2009.135
38. E. Schoch, F. Kargl, and M. Weber. “Communication Patterns in VANETs”. In: *IEEE Communications Magazine* 46.11 (Nov 2008), pp. 119–125. ISSN: 0163-6804. https://doi.org/10.1109/MCOM.2008.4689254
39. Elmar Schoch et al. “Impact of Pseudonym Changes on Geographic Routing in VANETs”. In: *Security and Privacy in Ad-Hoc and Sensor Networks* Springer Berlin, Heidelberg, Sept. 20, 2006, pp. 43–57. https://doi.org/101007/11964254_6
40. C. Troncoso et al. “PriPAYD: Privacy-Friendly Pay-As-You-Drive Insurance”. In: *IEEE Transactions on Dependable and Secure Computing* 8.5 (Sept. 2011), pp. 742–755. ISSN: 1545-5971. https://doi.org/10.1109/TDSC.2010.71
41. Carmela Troncoso et al. “Pripayd: Privacy Friendly Pay-as-You-Drive Insur ance”. In: *Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society* WPES ’07. New York, NY USA: ACM, 2007, pp. 99–107. ISBN: 978-1-59593-883-1. https://doi.org/10.1145/1314333.1314353
42. Björn Wiedersheim et al. “Privacy in InterVehicular Networks: Why Sim- ple Pseudonym Change Is Not Enough”. In: *Wireless On-Demand Network Systems and Services (WONS), 2010 Seventh International Conference on* IEEE, 2010, pp. 176–183.
43. Fangfang Zheng and Henk Van Zuylen. “Urban Link Travel Time Estimation Based on Sparse Probe Vehicle Data”. In: *Transportation Research Part C: Emerging Technologies* 31 (June 2013), pp. 145–157.