2 Background

Companies want you to be secure, but not against them.

— Whitfield Diffie, 2015 [185]

In this chapter, we give an introduction to vehicular communication and provide background information on privacy. We introduce the notion of *verifiable privacy protection*, before we describe the specific privacy threats that arise in vehicular communication systems.

2.1 Vehicular communication

This section describes the basics of vehicular communication, focusing on inter-vehicular communication (IVC) based on Vehicle-to-X (V2X) communication, which comprises Vehicle-to-vehicle (V2V) and Vehicle-to-infrastructure (V2I) communication. V2X communication is sometimes also referred to as Car-to-X (C2X) communication and IVC systems are also called Vehicular Ad Hoc Networks (VANETs) or Intelligent Transport Systems (ITS). Cellular connectivity can also be seen as an aspect of vehicular communication and is used in the protocols presented in this thesis but is not subject to our examinations.

2.1.1 Motivation and use cases

Today, driving is safer than ever thanks to advances in active and passive safety systems. Still, the harm caused by traffic accidents is dramatically high and calls for further action: In 2013, 32 719 people were killed in accidents in the U.S. and 3 339 in Germany [74]. In Germany alone, a total of 2.4 million accidents resulted in 374 142 injured [75] and an estimated economic harm of 32.5 billion EUR in 2013 [73].

Another challenge we face today are the time and resources wasted in traffic jams: A recent study estimates the economic harm of traffic jams in 2013 to be 124.16 billion USD for the U.S. and 33.48 billion USD for Germany, and expects the numbers to rise 50 % and 31 % respectively by 2030 [45, p. 5].

D. Förster, *Verifiable Privacy Protection for Vehicular Communication Systems*, DOI 10.1007/978-3-658-18550-3_2

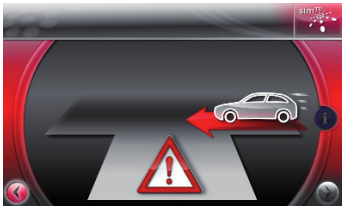
Finally, emission of greenhouse gases such as CO_2 must be reduced in order to fight climate change. While a reduction can be observed in the last years, the 2012 emissions from road transportation are still almost 20 % above the 1990 baseline, both in Europe [187, p. 130] and in the U.S. [199, p. 2-27].

Inter-vehicular communication (IVC) systems based on V2X communication are expected to deliver improvements for all of the challenges described above with its safety and traffic efficiency applications. Using ad-hoc radio communication, a variety of information can be exchanged between vehicles or with traffic infrastructure. The communication complements conventional on-board sensors and increases the vehicles' perception beyond line of sight: Cooperative Awareness Messages (CAMs) are continuously emitted by all participating vehicles. The messages contain the sender's location, speed, and direction of travel and allow for applications like Intersection Collision Avoidance (ICA), which warns drivers if other vehicles are detected that are on a collision course. Event-based Decentralized Environmental Notification Messages (DENMs) are forwarded over several hops and can be used to warn vehicles of hazardous situations such as the end of a traffic jam on the highway. Signal Phase and Timing (SPaT) messages sent out by traffic lights enable the Green Light Optimal Speed Advisory (GLOSA) application, which allows drivers to adjust their speed to a "green wave". The *geocast* communication mechanism allows sending messages addressed to all vehicles in a specific region. Schoch *et al.* give an overview over the different communication patterns in IVC systems [171]. Figure 2.1 shows examples for warnings and messages from the different V2X functions.

2.1.2 Research, standardization and deployment

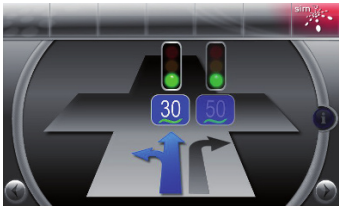
The European CAR 2 CAR Communication Consortium's roadmap foresees the introduction of V2X communication in several phases over the next years [32]: Phase 1 only covers the exchange of status data. Warning messages will be displayed to the driver when available, but only a low market penetration is expected in the beginning. Phase 2 includes cooperative sensing and functions such as ICA and GLOSA. Phase 3 introduces cooperative driving functions such as Lane-Merge Assistance and Platooning and will require a significant market penetration of V2X-equipped vehicles. Phase 4 adds synchronized cooperative functions, such as Cooperative Merging and Overtaking Assistance. "Accident-free driving" and an optimal traffic flow based on fully-automated driving is envisioned for phase 5. A precondition for reaching this phase is a high, if not full, market penetration.

V2X communication has received extensive research attention in the last decade [52, 57, 98, 111, 140, 154, 177]. Several field operational tests have



(a) Intersection collision avoidance: Approaching vehicle from the right, detected by its Cooperative Awareness Messages (CAMs).

(b) Traffic jam ahead. Based on Decentralized Environmental Notification Messages (DENMs), which may be forwarded over multiple hops.



(c) Traffic light assistant: Timing information broadcast by traffic light allows adjustment of speed to a "green wave".

Figure 2.1 Use cases from the sim^{TD} project [151] and the corresponding messages, that are displayed to the driver.

been conducted in order to uncover and resolve practical deployment issues: In the U.S., the Crash Avoidance Metrics Partnership's (CAMP) Vehicle Safety Communications 3 (VSC3) Consortium examined the scalability of radio communication and interoperability in a scenario with 200 vehicles [128]. In the scope of the Connected Vehicle Safety Pilot at the University of Michigan, over 2 800 vehicles were deployed for 23 months in order to assess a real-world deployment of V2V technology [22]. In Germany, the sim^{TD} project included a large-scale field trial with 120 V2X-equipped vehicles and 100 road-side units (RSUs) [150, 182]. The DRIVE C2X project evaluated the effectiveness of V2X-based safety and traffic efficiency applications in several European countries using more than 200 vehicles [180]. Both projects reported high acceptance from test users for V2X-based functions. The German CONVERGE project examined an open communication and service architecture for an Intelligent Transport System

(ITS), that combines V2X and cellular communication [51, 210]. Many of the results presented in this dissertation were developed as part of the CONVERGE project.

The positive result from the field trials and a positive assessment by the U.S. Department of Transportation [181] have prompted politicians and policymakers to act: The "G7 Declaration on Automated and Connected Driving" [188] by the transport ministers of the G7 states and the European Commissioner for Transport acknowledges the importance of V2X communication for traffic efficiency and safety. Several pilot deployments are currently underway in Europe with the French SCOOP@F project [13] and the European C-ITS corridor from Rotterdam via Frankfurt to Vienna [97]. In the U.S., pilot deployments have started in New York, Florida, and Wyoming [197]. Furthermore, the U.S. Department of Transportation has initiated the process to make V2X-based safety functions a requirement for newly sold passenger cars [198]. The CAR 2 CAR Communication Consortium expects the deployment in Europe to start in 2019 [44] and car makers have announced the first V2X-enabled models [82].

Standardization efforts have progressed quite far, both in the U.S. and Europe: On the lower layer, IEEE 802.11p [107] is used, a flavor of wireless LAN in the 5.9 GHz band that supports low-latency ad hoc communication, also known as Dedicated Short Range Communications (DSRC). On the higher layers, IEEE WAVE [106] and several SAE standards [162, 163] have been established in U.S. In Europe, the European Telecommunications Standards Institute (ETSI) has defined ITS-G5 [70], which incorporates some of the lessons learned from WAVE. Both standards define channel management, message formats, and a security architecture. In order to harmonize the different standards, the U.S. Department of Transportation's Research and Innovative Technology Administration (RITA) and the European Commission's Directorate General for Information Society and Media (EC DG INFSO) have announced the "EU-US Cooperative Systems Standards Harmonization Action Plan" [62].

2.2 Privacy

The need for privacy protection was described as early as 1890 by Warren and Brandeis, when technological advances like photography and newspapers raised the need for regulation [202]. They argued that the law's protection of physical integrity and property must be extended to protect from damage to privacy by "the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers" [202, p. 195]. More than a century later, we are facing a different technological revolution, the one of digitalization and

connectivity. Again, new technologies require us to adapt our regulations, and we need to have a public dialog about what use of these new technologies we as a society deem appropriate or inappropriate. If we apply the "right to be let alone" to the data that is collected by us and about us, the following quote by Warren and Brandeis could not be more up-to-date:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual [...] the right "to be let alone". [202, p. 195]

The definition of privacy as the "right to be let alone" is rather hard to grasp and Westin is more specific:

> Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. [205, p. 7]

This definition is in line with today's most common interpretation of privacy as control of information disclosure but reflects only one of four facets of privacy as defined by Banisar and Davies [15]: *Information privacy* is complemented by *communication privacy*, which receives increased public attention in the context of Internet surveillance [89]. *Bodily privacy* and *territorial privacy* are less present in public awareness but describe important aspects of privacy as protection of a person's bodily or territorial private spheres against intrusion. This subdivision into four aspects comprehensively captures Warren and Brandeis' "right to be let alone". Even though the impact of ubiquitous computing on territorial privacy has been investigated [113], most privacy research in computer science is concerned with information privacy or communication privacy.

The right to privacy is rooted in article 12 of the UN Declaration of Human Rights [196] and in article 8 of the European Convention on Human Rights [68]. Nowadays, privacy is sometimes regarded as a matter of personal taste and as something that can be traded for convenience. But we must be aware that it is a fundamental, inalienable right and one of the pillars of our modern and open society. As Rogaway puts it in his essay "The Moral Character of Cryptographic Work":

> Ultimately, I'm not much interested in individual grievances over privacy; I am far more concerned with what surveillance does to society. Totalized surveillance vastly diminishes the possibility of effective political dissent. And without dissent, social progress is unlikely. [158, p. 29]

In this work, we focus on information privacy and communication privacy (which are sometimes hard to distinguish) and, more specifically, on location privacy, which is a particular type of information privacy.

2.2.1 Location privacy

Duckham and Kulik define location privacy as the "claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others" [59], based on Westin's definition of privacy [205]. Another common but less specific definition by Beresford and Stajano is "the ability to prevent other parties from learning one's current or past location" [19].

Location privacy has received increased attention in the last years in the context of ubiquitous computing [21, 167]. It becomes relevant when users are required to reveal their location in order to use a location-based service. For example, when a user queries a location-based recommendation service to find a restaurant nearby, he has to provide his location, at least with a certain accuracy. Similarly, vehicles that participate in an inter-vehicular communication system are required to broadcast CAM messages that contain their exact location, because those messages are needed for the intersection collision avoidance application. We can see that in these examples revelation of location information, and consequently a certain loss of location privacy, must be accepted in order to use a certain service or to participate in the V2X system.

In the context of ubiquitous computing and inter-vehicular communication, protection of location privacy is concerned with two challenges: 1) Making services more privacy-friendly by requiring less (or less accurate) location information and still deliver the desired functionality. 2) Preventing leakage of location information to third parties that are not the intended recipient. Note that many threats to location privacy are not immediately obvious but may arise from long-term collection of data and statistical inference. We describe tracking and de-anonymization attacks, which are the most relevant threats in the context of inter-vehicular communication, in Section 2.3.4. Krumm provides a comprehensive survey of inference attacks on location privacy and countermeasures [117].

2.2.2 Location privacy metrics

In order to assess and compare mechanisms for protection of location privacy, it is essential that the level of location privacy they provide can be quantified. Shokri *et al.* point out that location privacy is equivalent to an attacker's

expected estimation error [175]. There are many proposals how to quantify location privacy. Note that their applicability depends on the specific threat scenario that is considered and on the attacker model that is used.

k-anonymity was originally described in the context of databases [186] and later applied to location privacy [92]. It expresses the attacker's uncertainty as the size of a user's anonymity sets, i.e., "how many other users could a certain user be confused with based on the location data he reveals". This is particularly relevant with regard to plausible deniability. We use the metric in Chapter 5 where we describe it in more detail.

Tracking-based metrics such as the *maximum tracking time* [164] take into account not only individual location samples but tracking over time. They describe the success of an attacker that tries to link users' location samples (e.g., messages) over time. Therefore, they are well suited to assess the effectiveness of protection mechanisms that aim to establish unlinkability of messages. We use a tracking-based metric in our evaluation of pseudonym change strategies in Chapter 3.

Entropy-based metrics quantify location privacy as an attacker's uncertainty measured in terms of *entropy* [19, 53, 172]. They capture the fact that some of the attacker's hypotheses about users' locations may be more likely than others. The calculation of entropy-based metrics requires the exact probabilities of the attacker's different hypotheses, which might not always be available depending on the attacker model.

Distance-based metrics take into account the distance between a user's estimated and actual position [101, 175]. They can be applied to single location samples as well as to location traces over time, and are often combined with entropy-based metrics.

Ma proposes a location privacy metric specifically for inter-vehicular communication systems [129]. It considers linkability of single location samples to users, linkability of location samples over time, and linkability of trips to users. The metric takes into account interrelations of probabilities in the assignment of trips to users, and models them using conditional probability distributions and Bayesian networks. While the metric is very comprehensive, it is also very complex and requires detailed information about the probabilities of the attacker's hypotheses.

2.2.3 Verifiable privacy protection

Privacy and security can be enforced by two different kinds of control mechanisms:

Organizational controls define certain rules how data must be handled, e.g., the four-eyes principle. The separation of duties between the Pseudonym Certificate Authority (PCA) and the Long-Term Certificate Authority (LTCA) in the basic pseudonym scheme, which we will describe in Section 2.3.3, is an example for an organizational control. Privacy is protected, as long as the parties adhere to the rules, but users have no way of verifying the parties' correct behavior. Organizational controls can be violated if employees misbehave, if organizations are forced to cooperate with intelligence services, or if they are hacked.

Technical controls protect data by technical means such as encryption. If data is encrypted prior to uploading it to a cloud storage provider, a malicious employee cannot access the data even if he manages to circumvent the organizational controls. The protection's effectiveness can be verified by the user, e.g., by examining the encrypted data prior to uploading.

The two kinds of controls require different levels of trust to be placed into central parties. Implementation of organizational controls can be demonstrated by certifications, e.g., ISO 27001, and validated in audits, but they can be violated without the users noticing. Technical controls, in contrast, can provide verifiable privacy protection, which we define as follows:

Verifiable privacy protection is the protection of privacy by technical controls, implemented in such a way that a well-versed user can examine their effectiveness and detect their removal or modification.

We use this definition of verifiable privacy protection as the leading design paradigm for the development of new privacy protection mechanisms throughout this dissertation.

The term *trust* warrants further discussion. The Oxford dictionary describes the colloquial meaning of the term as the "Firm belief in the reliability, truth, or ability of someone or something" [137]. But in security engineering, a "trusted system or component is one whose failure can break the security policy" [11, p. 29]. When we apply this definition to privacy, *a trusted party is an entity whose failure can violate its users' privacy.* It is crucial to note that in the context of privacy the term *trusted party* indicates that a system's privacy

guarantees depend on the party's correct behavior, not that the party is in fact *trustworthy*.

By applying technical instead of organizational controls, systems can be built in which users need to place less trust in central parties. Apple recently provided insights how user data stored at its data centers is protected even from the company itself by encryption and other mechanisms [116]. The company also announced plans [86] to analyze user behavior in its iOS mobile operating system but prevent inference of individual users' behavior by the use of differential privacy [61]. While no implementation details are known yet, this could be another example for privacy protection by a technical control.

Bitcoin is an example for verifiable enforcement of *security* by technical controls [134]: In our traditional financial systems, a customer trusts that the bank does not alter his account balance and that he will be able to withdraw his money at any time. But he has no technical means to enforce this. With Bitcoin, the correctness of all transactions is ensured by a cryptographic protocol, and no party can alter account balances or introduce invalid transactions.

Data minimization is a technical control that is particularly effective: The high number of data breaches in the last years [109, 206] have shown how hard it is to keep high profile systems secure. Prominent examples are attacks on Sony [16], Ashley Madison, a dating site for extramarital affairs [131], and Hacking Team, an Italian-based security firm [148]. The breaches have caused great damage to the affected companies and their customers. This illustrates that from a risk management point of view, collections of sensitive data are not only an asset but also a liability [112], which can be reduced by data minimization.

It is the goal of this dissertation to apply the paradigm of verifiable privacy protection, by technical controls and data minimization, to vehicular networks and to reduce the trust required in central parties. Therefore, throughout this work, we consider a strong adversary who can also compromise back-end systems.

2.3 Security and privacy in vehicular communication

Security is important for V2X systems, as suppression, injection, or alteration of messages could have direct safety implications. In addition, new privacy challenges arise for two reasons: 1) Vehicles are often personal items that are used by a single person or a small group. 2) Where we go reveals a lot of personal information about ourselves.

Eckhoff and Sommer give a good introduction to the privacy challenges that might arise from the deployment of inter-vehicular communication systems [63].

2.3.1 Security and privacy requirements

V2X systems must be protected against different kinds of attacks [144, 154]: Manipulation of messages or injection of bogus warnings could lead to unwarranted warning messages or automated interventions, whereas suppression of messages could lead to missing warnings or interventions. The sybil attack, the impersonation of several different participants by a single vehicle, could be used to gain an unfair advantage, e.g., by creating the illusion of a traffic jam. At the same time, special care must be taken to avoid that security controls introduce new privacy problems: Participants can be uniquely identified and held accountable for abusive actions using certificate-based message authentication. But the certificates as unique identifiers also expose drivers to tracking attacks based on their messages, in particular the CAMs, which are broadcast at a frequency of 1 to 10 Hz. Availability of messages to all participants is crucial for safety functions, therefore, they are not encrypted and can be received by anybody within communication range, no matter if he is a legitimate participant of the V2X network or not. Of course, tracking vehicles has always been possible, e.g., by physically following them or by planting a GPS bug. In fact, each car's license plate is a publicly available unique identifier, which is widely accepted today. Yet, V2X messages dramatically increase the exposure for tracking, because their reception does not require visual contact and due to their transmission range of up to several hundred meters. Unlike other communication devices like mobile phones, which can also be used for tracking attacks, drivers cannot simply switch of their car's inter-vehicular communication system when they desire privacy, because it will be an important component of the vehicle's safety system and might be required by law.

Schaub *et al.* describe security and privacy requirements for V2X systems [169]:

- *Message authentication* is required to ensure the correctness of information received. It comprises sender authentication and message integrity, and should include *restriction of credential usage* to prevent sybil attacks.
- *Revocation* is required to remove misbehaving participants from the system.
- *Minimum disclosure of information* should be applied. In particular, "the exposure of information to any authorities should be kept minimal".
- *Sender anonymity* is the first step for protecting drivers' privacy. Additionally, *unlinkability of messages* is required to prevent long-term tracking.

- *Accountability* (by the possibility to resolve the sender of any message) is given as a security requirement. While the suggestion of a *distributed resolution authority* offers some privacy protection, *resolution* obviously conflicts with the requirement of *anonymity*.
- Additional constraints must be considered when implementing security and privacy protection: *Real-time constraints* apply for safety-critical communication. *Scalability* is needed to cope with very large systems, both with regard to the number of participants and the geographical extend.

We will refer to these requirements throughout this dissertation. In particular, we will address the inherent conflict between privacy and control (by resolution of pseudonyms) in Chapter 4.

2.3.2 Security research projects

Some of the V2X field trials and research projects described in Section 2.1.2 have also considered security and privacy aspects. The CONVERGE project for example developed a security architecture for a hybrid network of V2X communication and cellular back-end connectivity [50]. In addition, several research projects specifically focused on security and privacy aspects of inter-vehicular communication:

The SEVECOM project [123], 2006-2008, laid the groundwork for current security mechanism in inter-vehicular communication and was the context for some of the authoritative publications on the subject [111, 140, 141].

The EVITA project [99], 2008-2011, defined a secure on-board architecture and secure on-board communications protocols, and explored the use of hardware security modules (HSMs) in the automotive domain. While not focused on IVC exclusively, the project demonstrated a secure e-safety application based on V2X communication.

The PRECIOSA project [54], 2008-2010, examined privacy protection in cooperative systems and safety applications, using model-driven approaches, a privacy-enhanced policy language, and a privacy-enforcing runtime architecture.

The OVERSEE project [90], 2010-2013, focused on the creation of a secure, standardized and generic communication and application platform for vehicles, leveraging the HSM definitions from the EVITA project [91].

The PRESERVE project [149], 2011-2015, built on previous research projects (both security- and non-security-specific) and aimed to provide practical security solutions in the form of a V2X software stack and an HSM.

2.3.3 Pseudonymous authentication

For privacy-friendly message authentication, a scheme of changing *pseudonym certificates* (short: pseudonyms) has been proposed [140, 141] and is included in emerging standards [71, 108]. Outgoing V2X messages are signed with short-lived pseudonym certificates, which do not contain any information about their holder. Any incoming messages that do not bear a valid signature are discarded. To prevent tracking based on pseudonymous identifiers, pseudonyms are changed "every once in a while".

A multitude of different pseudonym systems have been proposed [146] and we will cover them in more detail in the following chapters. In this section, we describe the pseudonym issuance process according to the *basic pseudonym scheme* due to the European CAR 2 CAR Communication Consortium [24]. See Figure 2.2 for an overview.

A *Root CA* acts as a system-wide trust anchor and issues CA certificates to the Long-Term Certificate Authority (LTCA, sometimes also called *Enrollment Authority*) and the Pseudonym Certificate Authority (PCA, sometimes also called *Authorization Authority*). New vehicles are registered with the LTCA and receive a *long-term certificate* when joining the system. They obtain *pseudonym certificates* from the PCA after authenticating with their long-term certificate.

For each pseudonym the PCA issues, it stores the mapping to the corresponding long-term certificate in its *mapping database*. This mapping information is required if a participant is sending invalid or malicious messages and must be removed from the system. Based on any of his signed messages, his corresponding long-term certificate can be resolved and added to a certificate revocation list (CRL), thus preventing him to obtain any more pseudonym certificates. In contrast to the pseudonym scheme that will likely be used for U.S. deployments [208], the basic pseudonym scheme does not foresee revocation of pseudonym certificates. This delays the effectiveness of a vehicle's revocation until all of its pseudonyms have expired. Identification of misbehaving participants, *misbehavior detection*, is described by Bißmeyer [23]. It is a research area on its own and not in the scope of this work.

Privacy-friendly pseudonym issuance can be implemented by a separation of responsibilities between the LTCA and the PCA: When requesting pseudonyms, the vehicle encrypts its long-term certificate with the LTCA's public key. The PCA, unable to check the certificate itself, forwards it to the LTCA for validation, which only reports back authentication success or failure. Neither of the parties learns the mapping between the long-term certificate and the pseudonyms issued. If resolution is required, they can jointly determine the mapping by decrypting the long-term certificate which is stored in the mapping database in encrypted

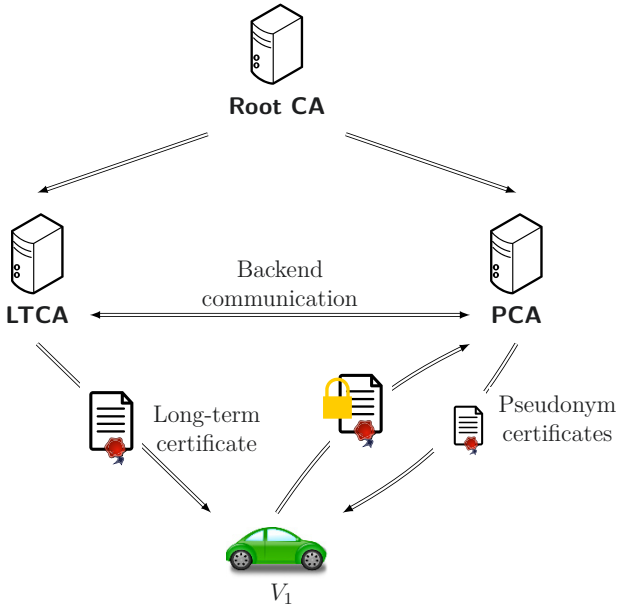


Figure 2.2 The *basic pseudonym scheme* [24]: A vehicle V_1 obtains pseudonym certificates after authentication with his long-term certificate. The root CA acts as a system-wide trust anchor. Privacy protection can be implemented by separation of responsibilities between the LTCA and the PCA.

form. Note, that the protection is based on an organizational control only and is void if both parties are compromised.

Pseudonyms can be obtained via a cellular connection to the back-end systems, via road-side units (RSUs), or can be pre-loaded during maintenance. We present an alternative, more privacy-friendly protocol for pseudonym issuance in Chapter 4.

2.3.4 Tracking attacks

Even when pseudonym certificates do not contain any information about their holder, drivers' privacy can be violated by tracking attacks. Privacy infringement based on V2X messages can be as simple as linking two observations of the same vehicle, e.g., recording which vehicles attended a labor union meeting and matching it with the vehicles on the companies' parking lot in order to

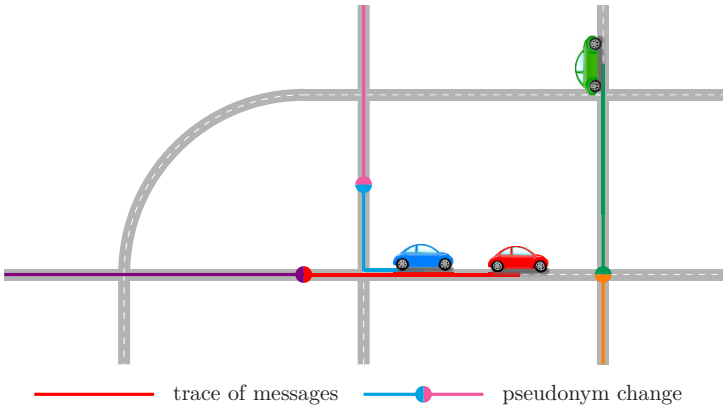


Figure 2.3 Vehicles leaving a trace of messages signed with different pseudonyms (indicated by different colors). The intention of changing pseudonyms is to split their trips into unlinkable pieces.

identify union members among employees. Using V2X communication, this is a lot easier than, for example, scanning everybody's license plate.

In general, an attacker who can link observations of V2X participants could identify groups of drivers based on locations they visited and derive information about their political orientation, personal preferences, and many more. Some illustrative examples are: Identify political activists based on their regular meetings, identify people that suffer from a particular illness, e.g., based on their visits to an AIDS clinic, or identify officials who engage in activities they would rather keep secret and that might make them susceptible to blackmail.

Drivers' privacy is threatened in particular by the continuous trace of CAMs they leave and which can be received by anybody within communication range, including non-members of the V2X network. Hoh *et al.* showed that drivers' home locations can be inferred from their GPS traces with an accuracy of about 85 %. In a similar experiment, Krumm determined peoples' home location from GPS traces and was able to identify 5 % of them by name using a freely available web service [118]. Using data from the U.S. Census Bureau, Golle and Partridge find that the majority of the U.S. working population can be uniquely identified if both home and work locations are known [85].

The pseudonymous authentication scheme described in the previous section is designed to prevent this kind of tracking by splitting a trip into several unlinkable pieces as shown in Figure 2.3. Ideally, observations of the same vehicle before

and after a pseudonym change should be unlinkable. However, Gruteser and Hoh and Wiedersheim *et al.* showed that mobile nodes that emit messages with a high frequency can be tracked using multi-target tracking even if their messages contain no identifier at all [93, 209]. This illustrates that pseudonym changes are only effective when performed outside the observation range of an attacker and that they cannot provide protection against an adversary with global coverage.

We examine the effectiveness of pseudonym changes for protection against tracking attacks in Chapter 3.

2.4 Notation

We use a semi-formal notation for algorithms and protocols based on common set notation shown in Table 2.1.

Table 2.1 Notation elements for algorithms and protocols

Notation	Description
$:=$	Assignment operator
$\{e_1, e_2, \dots\}$	Set of elements
(e_1, e_2, e_3)	Fixed size, ordered tuple of elements
$S := S \cup \{e\}$	Add the element e to the set S
$S := S \setminus \{e\}$	Remove the element e from the set S
$ENC_{key}(p)$	Symmetric or asymmetric encryption of plaintext p with key *key*. The type of encryption will be clear from the context and the key used.
$DEC_{key}(c)$	Symmetric or asymmetric decryption of the ciphertext c using the key *key*. The type of encryption will be clear from the context and the key used.
$SIG_{skey}(v)$	Signature of the value v using the signing key *skey*
$VER_{vkey}(\sigma, v)$	Verification of the signature σ on v using the verification key *vkey*

http://www.springer.com/978-3-658-18549-7

Verifiable Privacy Protection for Vehicular Communication Systems

Förster, D.

2017, XV, 150 p. 30 illus., 13 illus. in color., Softcover
ISBN: 978-3-658-18549-7