Security and privacy in vehicular networks

9

F. Kargl[1], *J. Petit*[2]
[1]Ulm University, Ulm, Germany; [2]University College Cork, Cork, Ireland

9.1 Introduction and security requirements

Vehicular networks have to support a challenging environment with high vehicle densities that generates a lot of broadcast communication. As many applications of vehicular networks are directly related to driving safety, it is of high importance to provide proper security. Otherwise, attackers could send out spoofed or forged information that may result in incorrect warnings to drivers, or even wrong automatic reactions of vehicles in the case of automated driving applications. Accidents, injuries, or even fatalities might be direct results. For example, a fabricated or replayed electronic emergency brake light message could cause the receiving vehicle to brake suddenly in order to avoid a nonexistent obstacle. Therefore, security mechanisms for intelligent transport systems (ITS) are of paramount importance to enable safety applications based on Car-to-X (C2X) communication. Initial proposals by Gollan and Meinel (2002) and Zarki et al. (2002) suggested using digital certificates to identify vehicles and authenticate messages in vehicular communications. Those initial works generated an influx of research (Hubaux, Capkun, & Luo, 2004; Papadimitratos, Gligor, & Hubaux, 2006; Parno & Perrig, 2005; Raya & Hubaux, 2007) and activities within projects and standardization bodies.

The following security requirements were identified for vehicular networks:

1. Confidentiality: Generally speaking, C2X communication aims at increasing the awareness of a vehicle's surroundings, e.g. regarding other vehicles or hazards. Therefore, vehicular communications are typically open, rendering confidentiality only a minor requirement. Only some specific-use cases like transactional applications (e-tolling, pay-per-view) require confidentiality.
2. Integrity: C2X messages are used to make decisions such as warning the driver or triggering an automated reaction by the vehicle. Therefore, message integrity is of the utmost importance. To ensure that a message has not been manipulated, integrity mechanisms such as digital signatures are used in the current European Telecommunications Standards Institute (ETSI) standards (ETSI, 2013).
3. Authentication: Each message sent in the vehicular network has to be authenticated to prevent malicious external attackers from injecting messages. Authentication is often provided by digital signatures and public key infrastructures.
4. Availability: The availability of C2X communication is important for real-time safety applications. However, it is hard to achieve given that jamming is always possible in wireless communication (Puñal, Aguiar, & Gross, 2012).

Vehicular Communications and Networks. http://dx.doi.org/10.1016/B978-1-78242-211-2.00009-X

5. Privacy protection: Despite the authentication requirements above, vehicles and drivers should not be identifiable in order to prevent location profiling of drivers.
6. Liability/non-repudiation: Non-repudiation ensures that any receiving entities could prove to a third party that a specific sender has sent a message. This is challenging to ensure in combination with privacy protection. It is a matter of on-going debate whether authorized entities like law enforcement should be able to identify vehicles or not.

As discussed in Section 9.2, current standardization efforts mainly follow an approach based on asymmetric cryptography. Messages are authenticated with ECDSA signatures and a corresponding public key certificate is attached, which is issued to vehicles by a CA.

However, this approach challenges the privacy of drivers, as periodic beacon messages convey exact location information of vehicles. Vehicular networks definitely require privacy protection (Schaub, Ma, & Kargl, 2009) but the exact degree of anonymity and the level of privacy protection are still a matter of debate. One key requirement is location privacy, which is defined as *the ability of an individual to move in public space with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use* (Blumberg & Eckersley, 2009). A metric for measuring the level of users' location privacy is crucial and indispensable (Ma, Kargl, & Weber, 2010) in order to assess a system's ability to preserve the users' location privacy and to evaluate the effectiveness of any protection mechanism. We discuss the challenges of privacy protection in Section 9.3.

Please note that while we will speak of vehicles throughout this chapter, the discussion applies likewise to any other ITS stations like roadside units (RSUs) if not explicitly noted otherwise.

Even with perfectly authenticated and integrity protected C2X communication, insider attackers could still generate fake data. To deal with this challenge, we present misbehaviour detection mechanisms in Section 9.4.

9.2 Identity management in C2X

9.2.1 Introduction and requirements

As discussed previously, one of the predominant security requirements in C2X security is ensuring authenticity and integrity of communication. Only legitimate vehicles should be able to send messages that other vehicles will accept as genuine. Such messages should be protected from modification.

At the same time, there are a number of additional considerations:

1. Any solution should be based on industry-proven and strong security mechanisms as any vulnerabilities discovered after initial deployment will be highly expensive or even impossible to be fixed with a system installed in vehicles.
2. Additional message payload introduced by security mechanisms needs to be limited in size. If messages grow arbitrarily large, they may not fit into the maximum transfer unit of IEEE 802.11p of approximately 2300 bytes. Beyond this, larger messages lead to a more congested channel and higher risk of collision.

3. Security mechanisms must not introduce large latency. As some applications will only tolerate end-to-end delay of 100 ms or even 50 ms, introduction of compute-intensive cryptographic algorithms may turn out to be prohibitive.

Early research efforts already proposed use of elliptic curve cryptography or more specifically the elliptic curve digital signature algorithm (ECDSA) and digital certificates similar to the well-known X.509 certificates in combination with a vehicular public key infrastructure (VPKI). This basic approach was already proposed by the initial IEEE 1609.2 standard (IEEE, 2013) and European research projects like SeVeCom (Papadimitratos, Buttyan, et al., 2008; Kargl, Papadimitratos, et al., 2008) and Networks-on-Wheels (Gerlach et al., 2005) and is now used also in standards from ETSI (2012a, 2012b, 2013).

9.2.2 VPKI and ECDSA signatures

We will first explain the basic scheme to describe how vehicles secure messages. It involves a VPKI and digital signatures based on the ECDSA. This basic scheme is very close to the IEEE 1609.2 standard (IEEE, 2013) while the ETSI security architecture (ETSI, 2012a; 2012b; 2013) already includes significant modifications related to privacy protection. We will discuss privacy in the next section.

As depicted in Figure 9.1, the different VPKI components will receive certificates from the root-level CA (step 1). After creating an ECDSA key pair (which includes a private and a public key), each vehicle will receive a digital certificate from a VPKI CA

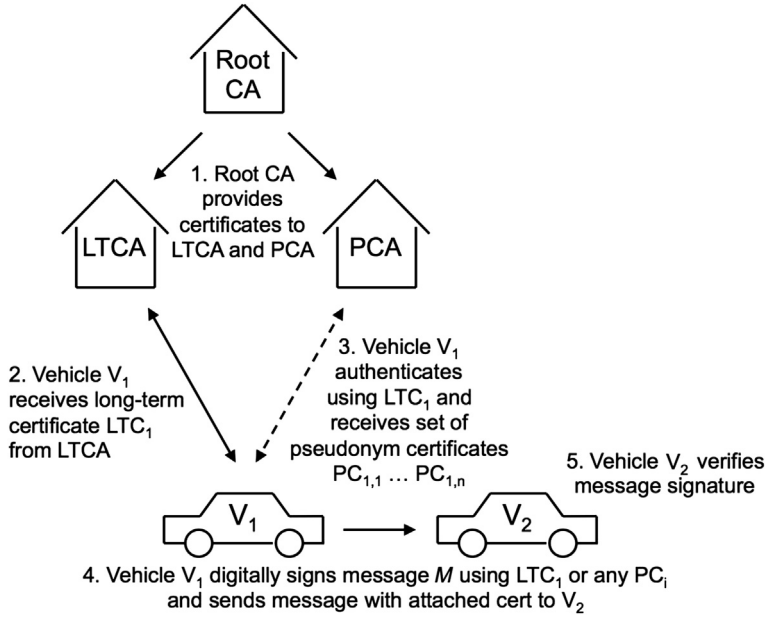

Figure 9.1 Overview of vehicular public key infrastructure (VPKI).

(step 2). The distinction in long term and pseudonym certificates will be explained in the next section; for the purposes of this discussion, we can skip step 3. The long-term certificate (LTC) includes a unique vehicle identifier of some sort (like the vehicle identification number), the public key, an expiration date, and a digital signature of the CA to declare it valid. Other information, like vehicle dimensions or authorization attributes for vehicles with special right of way, can be included optionally. Once a vehicle has obtained these credentials, it can send authenticated messages (step 4). For this, it will sign the payload of message *M* (and optionally elements from the message header) using the secret key corresponding to certificate LTC_1 and append the signature plus certificate to the message. Usage of pseudonyms PC_i instead of LTC_1 will again be discussed in the next section. Receiving vehicles will then first verify the certificate and the signature before forwarding the message to the higher layers of the communication stack (step 5). Messages with invalid or incorrect signatures or certificates should be discarded. Certificates will only be considered valid by receiving vehicles if they have been issued by a CA from a trusted VPKI where a respective VPKI certificate has been installed in the vehicle's on-board unit (OBU) beforehand. The whole procedure ensures that only vehicles in possession of a valid certificate issued by a trusted CA can send messages that other vehicles accept.

ECDSA was selected because this asymmetric cryptographic algorithm provides significantly shorter key and signature lengths for a given security level compared to the more popular RSA cryptosystem. The NSA (NSA, 2009) argues that to reach a security level of 128 bits, ECDSA requires 256-bit key size while RSA would require 3072 bits. As the length of the key size is also directly linked to the length of the digital signature in both cases, this means that an RSA signature requires 12 times more space in a message compared to ECDSA − a very strong argument in favour of ECDSA considering the limited data rate in C2X communication.

From the list of requirements stated earlier, the presented approach fulfils the first and the second directly. It is a well-proven architecture relying on well-proven cryptographic primitives, and the resulting signature and certificate sizes are at least acceptable. However, when it comes to computational performance, ECDSA is actually even slower than its RSA counterpart. When running OpenSSL benchmarks on a standard laptop (Apple MacBook Air with Intel Core i7 1.7 GHz, OpenSSL 0.9.8 y), RSA-2048 scores at 8235 verifications per second while for ECDSAp-224 the same computer achieves only 959 verifications per second. While the situation is opposite for signature generation, we will later see that verification is the most important problem to be solved and that research has focused on this problem to come up with solutions.

IEEE 1609.2 (IEEE, 2013) is an example of a standard that implements the scheme described above. It provides various security services, such as signing and encrypting data, and is based on elliptic curve cryptography and digital certificates. Certificates include additional information, such as permissions and validity periods, and the standard also discusses how certificates can be refreshed or how they will be revoked. It also provides necessary protocols and message structures.

9.2.3 Performance

One of the major issues of the scheme outlined above is the additional overhead it creates in C2X communication. Figure 9.2 shows that there are two types of overhead: computational and communication. The first is created by complex cryptographic operations for signature generation and verification, and may either introduce significant latency or require extra hardware for cryptographic acceleration. Cryptographic overhead is also generated when certificates need to be verified, while certificate generation happens offline and is not relevant to our discussion. The communication overhead stems from the necessity to add signatures and certificates to messages. ETSI TS 103 097 (ETSI, 2013) lists a size of 96 bytes for the security envelope (which includes the signatures) and 133 bytes for a certificate. Therefore, a message would be enlarged by 229 bytes due to security payload. IEEE 1609.2 reaches similar sizes. Enlarging packets leads to additional latency and can also lead to extra packet collisions in case of a congested channel.

9.2.3.1 Computational overhead

One approach to address computational overhead is to introduce a HSM as it is, for example, designed and built by the European PRESERVE research project (Kargl, 2011). The project's specifications require such a module to be capable of at least 1000 verifications per second. The focus is put on verifications as they are more costly for elliptic curve cryptography, and as a vehicle in high-density traffic is assumed to receive a factor of 10−100 more messages than it sends out. While PRESERVE manufactures the HSM as a dedicated ASIC, it is expected that in the future it will be integrated with the OBU's microcontroller. Besides cryptographic acceleration, the HSM can also provide secure key storage, a secure random number generator, and a couple of other mechanisms like a trusted platform module, and can thus significantly enhance the system's security in various ways.

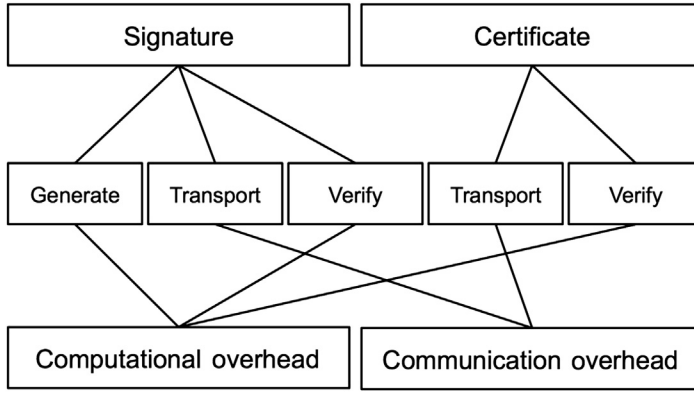

Figure 9.2 Computational and communication overhead created by signature and certificate.

While this would still introduce a certain delay in message generation and reception, the problem of computational overhead can basically be solved by the introduction of an HSM. An alternative or complementary approach is often called verification-on-demand, where the idea is to verify only a fraction of incoming packets based on their relevancy for applications (Krishnan & Weimerskirch, 2011). The intuition is that messages that applications do not consider further, for example, to display a warning message to a driver, will be discarded anyway and will not have a negative effect, even if sent by a malicious party. Only those messages that trigger applications to react in some way need to be verified cryptographically. An obvious issue with this strategy is that it requires a complex cross-layer design of the communication stack as the relevancy of a message can only be decided on the application layer. This may be hard to decide on in more complex software architectures, like the ones proposed by ETSI (2010) or CALM (ISO TC-ITS, 2007) where data are first stored in a local dynamic map (LDM) before it is accessed and used by applications (potentially in aggregated form).

9.2.3.2 Communication overhead

Various authors have further addressed performance and overhead in C2X security. One of the first contributions is from Kargl, Schoch, et al. (2008) and Schoch and Kargl (2010) who propose approaches to reduce unnecessary overhead in periodic beaconing of safety messages. This includes various strategies to omit certificates from messages. The intuition is that once all neighbouring vehicles have received and verified the certificate of a vehicle, those neighbours can cache it and it does not need to be included in future messages as signatures can be verified based on cached data. Only when new vehicles enter the communication range of a sender does the certificate again need to be attached to messages. However, if the certificate is omitted in such a situation, the new neighbour will not be able to verify received packets and has to discard them — an effect called 'cryptographic packet loss' in Feiri, Petit, and Kargl, (2012a). The challenge is to find an optimal strategy that reduces the percentage of packets with certificates attached — thus leading to smaller messages and fewer collisions on a congested channel — while at the same time keeping the cryptographic packet loss small.

The authors investigate simple schemes like periodic omission of certificates in every *n*th packet, which are also analysed in great detail in works by Papadimitratos, Calandriello, et al. (2008) and Calandriello et al. (2011). However, they also propose more adaptive schemes like certificate omission where certificates are attached only if messages from a new vehicle are received (neighbour-based omission). Feiri et al. (2012a), Feiri, Petit, and Kargl (2012b), Feiri et al. (2013) continue this work and propose omission schemes based on channel load. This is motivated by the observation that there is no need for omission in a free channel, as the benefit of smaller messages would be minimal, but cryptographic packet loss may be high due to high mobility of vehicles. In case of a highly congested channel, vehicles may be stuck in a traffic jam and neighbourhood changes slower. This gives the opportunity for a more aggressive omission scheme that will significantly reduce collision-induced packet loss. Figure 9.3 illustrates a variety of those certificate omission strategies.

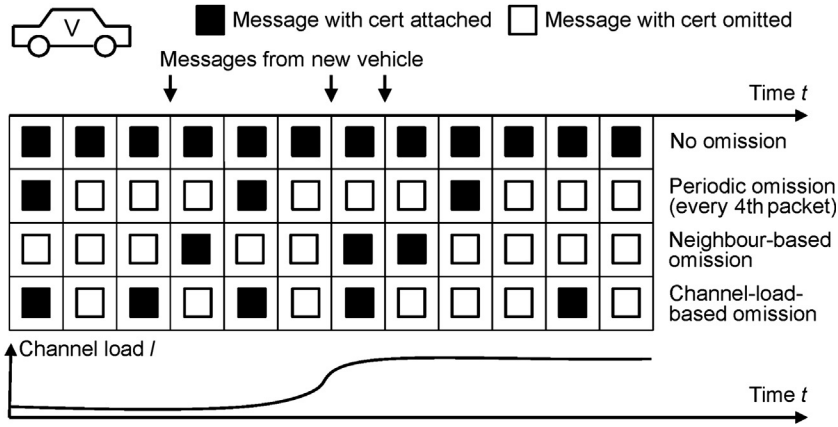

Figure 9.3 Illustration of various certificate omission strategies.

In all analysed cases, the benefits of such schemes on packet delivery and cooperative awareness became evident.

9.2.4 Alternative schemes

Many alternative proposals have tried to further increase the efficiency of message authentication in vehicular networks. Many approaches focused on the replacement of asymmetric by symmetric cryptography, exchanging digital signatures by cheaper message authentication codes (MACs). This provides performance advantages of two to three orders of magnitude. At the same time, it creates massive problems with key management and non-repudiation. Most proposals either rely on trusted hardware (Paruchuri & Durresi, 2010), where symmetric keys are safeguarded by 'secure-by-default hardware', or on trustworthy entities like RSUs that forward all messages for verification (Zhang et al., 2008). The latter may work for very special circumstances and applications; both approaches are neither generic nor do they provide good security properties.

One of the most interesting and feasible schemes that relies on symmetric primitives is the application of Timed Efficient Stream Loss-Tolerant Authentication (TESLA) to C2X communication as proposed by Studer et al. (2009). Here, time is divided into discrete time slots that are synchronized between all participants. As shown in Figure 9.4, vehicles create hash chains by repetitively hashing a starting value x_1 to produce x_2, x_3, until x_n. The vehicle then digitally signs x_n and publishes this, e.g. by attaching the value and signature to messages. As the hash function is non-invertible, knowing x_i, one can reproduce any later x_i+j, while knowing only any x_k, one could not determine an earlier x_k-l. Every element in the hash chain corresponds to a specific time slot, where x_n belongs to time slot 0, x_n-1 to time slot 1 and so forth. In time slot m, the corresponding hash chain element x_n-m can be used to authenticate a message using it as a key for a MAC function like HMAC-SHA1. This key is unknown to receivers and will only be published by the

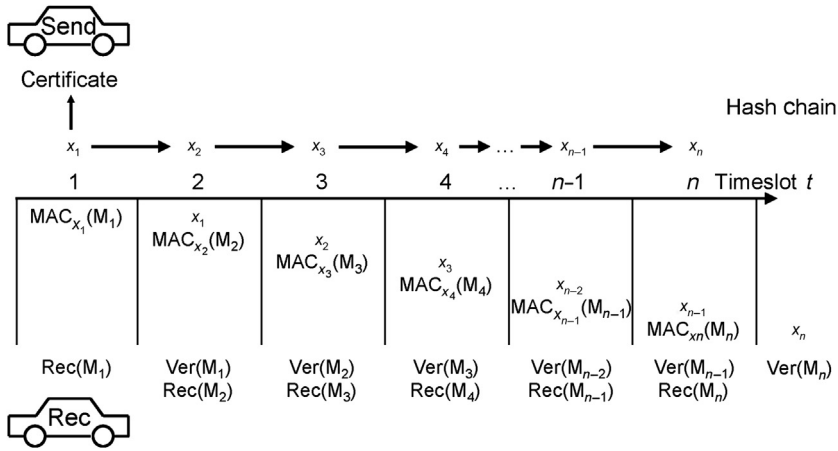

Figure 9.4 The TESLA authentication scheme for vehicular communication.

sender in the next time slot $m + 1$ in a later message. The receiver will then complete the hash chain until *x_n* and check whether this corresponds to the signed *x_n* that was distributed earlier. This means that receivers need to cache a message for one time slot before they can verify it and forward it to applications. This added delay and the dependency between messages are the main drawbacks of TESLA in a vehicular setting. However, Studer et al. (2009) show results that indicate that use of TESLA may actually be feasible.

So far, we neglected the negative impact that vehicle authentication may have on privacy. This was recognized early on, and there is therefore a large body of work trying to enhance the basic authentication scheme by privacy-friendly mechanisms. This will be discussed in the next section.

9.3 Privacy protection

As pointed out in the previous sections, C2X communication should not jeopardize the privacy of users. Vehicles equipped with C2X technology will regularly broadcast position beacons to create cooperative awareness. This means that an eavesdropper capable of collecting these position beacons could create a mobility pattern about the targeted user. Therefore, short-term certificates, named pseudonyms, were introduced to protect against long-term linkability.

Looking at the means of achieving pseudonymity, the schemes differ in the cryptographic mechanisms they employ. Four major categories can be distinguished for pseudonymity in vehicular networks. Schemes based on *asymmetric cryptography* aim for PKI-oriented privacy solutions as presented in Section 9.2. Pseudonyms are typically represented by public key certificates without identifying information. As discussed above, those pseudonym certificates are sent along with messages. Schemes based on *identity-based cryptography (IBC)* extend this idea by removing

the need of explicit public key certificates as public keys are directly derived from vehicles' address identifiers. This reduces communication overhead for pseudonym use but introduces new challenges for pseudonym issuance. Pseudonym schemes based on *group signatures* introduce one joint public key for a whole group of vehicles. Group-based schemes reduce the need for pseudonym changes but pose new challenges for pseudonym resolution and revocation. Schemes based on *symmetric cryptography* are attractive because of their computational efficiency but must be embedded into protocols that can enable reliable authentication and ensure non-repudiation. Due to the different challenges posed by each cryptographic paradigm, many solutions combine different mechanisms to achieve more effective schemes.

9.3.1 Pseudonym life cycle

In C2X communications, pseudonyms pass through a common abstract pseudonym life cycle. Depending on the specific pseudonymous authentication scheme, some of the actual life cycle phases may diverge from the abstract life cycle model. However, the phases outlined in the following can be found in almost all existing pseudonymous authentication schemes. Figure 9.5 gives an overview of the phases of the abstract pseudonym life cycle: *issuance*, *use*, *change*, *resolution*, and *revocation*. One should notice that pseudonym issuance must already consider pseudonym resolution and pseudonym revocation. Those phases in turn inherently depend on the measures taken in the pseudonym issuance process to be effective. Pseudonym use and pseudonym change influence each other and also depend on how pseudonyms are issued or obtained by vehicles. Some of the phases are also optional, e.g. not all schemes foresee or support pseudonym resolution or revocation.

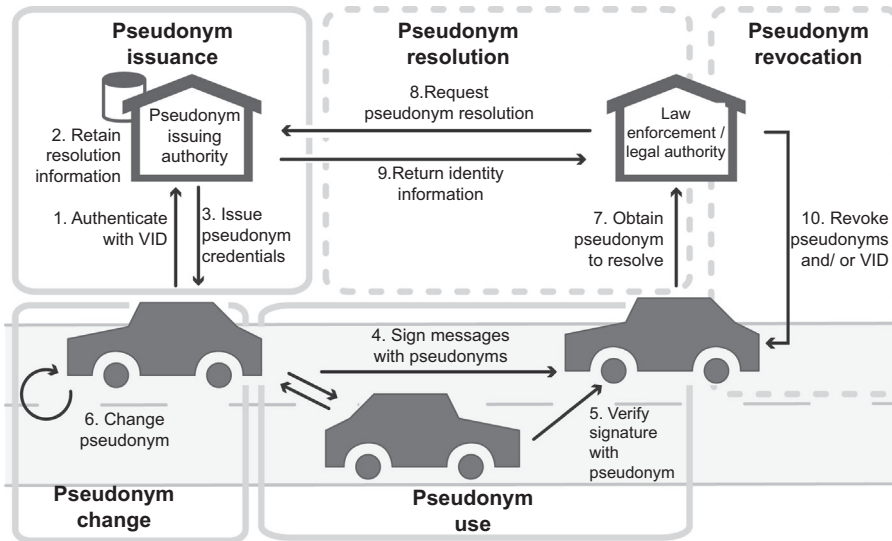

Figure 9.5 Abstract pseudonym life cycle.

9.3.2 Main approach: asymmetric cryptography schemes

Let us now describe the main approach selected by standardization bodies based on asymmetric cryptography. Pseudonymous communication can be achieved with traditional public-key cryptography schemes by equipping vehicles with a set of public-key certificates and corresponding key pairs (Bissmeyer et al. 2011). The public-key certificates are stripped of any identifying information and are used as unlinkable pseudonyms. Vehicles sign messages with the secret key of the currently active pseudonym and attach the resulting signature and the corresponding pseudonym certificate to the message. Receivers can verify a message signature based on the pseudonym certificate but are unable to determine the sender's vehicle identifier.

Figure 9.6 shows the adapted pseudonym life cycle for asymmetric pseudonym schemes. We describe the corresponding phases of this scheme in the following.

Pseudonym issuance: In asymmetric schemes, the pseudonym issuance process is similar to certificate issuance in a PKI. As depicted in Figure 9.6, and described in Section 9.2, certificate authorities (CAs) are organized hierarchically. CAs manage and issue long-term identity certificates to vehicles while pseudonyms are issued by separate pseudonym providers (PPs). As pseudonyms are only valid for a short period of time, vehicles must request new pseudonyms in certain intervals, which introduces the need back-end connectivity and some scalability issues. When issuing pseudonyms, a PP authenticates a vehicle by its LTC before issuing pseudonyms. It may then keep the pseudonyms-to-identity mapping as escrow information in case of liability investigation. In case of a rogue or compromised PP, this may leak privacy sensitive information. Therefore, many of the schemes provide some additional protection.

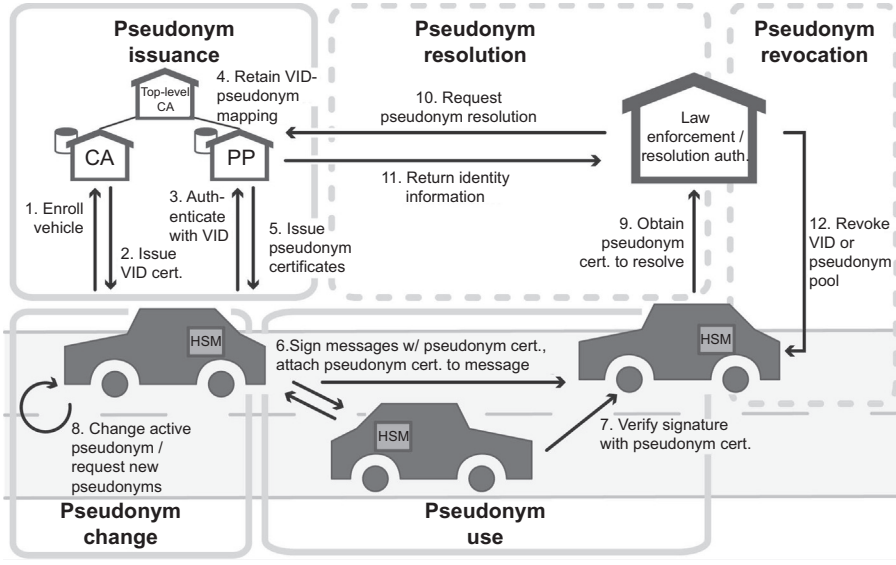

Figure 9.6 Abstract pseudonym life cycle for asymmetric cryptographic schemes.

Pseudonym use: Pseudonyms are used to sign every outgoing packet. Public/private keys of previously obtained pseudonyms may be stored and managed by an HSM, which is tamper resistant to restrict the parallel usage of pseudonyms. The assurance level of the HSM determines the pseudonym restriction scheme (lifetime, amount of pseudonyms available in parallel, etc.). The available secure storage space impacts the number of pseudonyms that can be stored in parallel inside the HSM. For signing or encryption tasks, only the currently valid pseudonym certificates can be used.

Pseudonym change: A pseudonym has a lifetime to hamper long-term tracking based on pseudonyms. When a pseudonym expires, the OBU either loads a new pseudonym from its store or requests new pseudonyms from the PP (which corresponds to pseudonym issuance). In the first case, pseudonyms are changed according to the current context by the vehicle while driving. The employed pseudonym change strategy is crucial to prevent linking of pseudonyms when changing.

Pseudonym resolution: Pseudonym-identity resolution is performed by pseudonym resolution authorities, which either have access to pseudonym-vehicle ID mappings kept by PP or CAs or directly map from pseudonyms to vehicle identifiers by some cryptographic mechanism.

Pseudonym revocation: Because of scalability reasons, revocation of pseudonym certificates is commonly limited to revoking the VID. If the long-term identity is revoked, no new pseudonyms can be obtained. Hence, certificate revocation lists (CRLs) must only be distributed to PP and not to all individual vehicles. In addition, letting OBUs verify pseudonyms of other vehicles against CRLs would not be practical due to high message frequency and potential large CRLs, especially in dense traffic scenarios. On the other hand, by revoking only the VID, a revoked vehicle can continue participating in the network pseudonymously until all its pseudonyms are expired. A solution is to effectively reduce the lifetime of pseudonyms to very short intervals, which in turn increases the frequency of pseudonym refills.

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

9.3.3 Other existing approaches

Three other approaches, based on IBC, group signature and symmetric cryptography, respectively, have been proposed to ensure pseudonymity within C2X communication.

9.3.3.1 Identity-based cryptography

IBC (Shamir, 1985) is related to asymmetric cryptography with the significant difference that a node's identifier serves as that node's public key. A corresponding private key is derived from the identifier to sign messages. Knowing the sender's identifier is sufficient to verify the signature, and thus no additional certificate is required. However, to prevent that any node with knowledge of another node's identifier can derive a corresponding private key (i.e. key escrow), only a centralized trusted authority with full knowledge of a secret system parameter is able to extract private keys and

assign them to nodes. Thus, a node's authenticity is implicitly guaranteed rather than explicitly stated with a certificate, because only authorized nodes would receive a private key corresponding to a specific identifier.

Compared to a conventional PKI, IBC avoids the use of certificates for public key verification and the exchange of public keys and associated certificates, while providing similar authentication characteristics. The resulting communication and storage efficiency make IBC attractive for authentication in vehicular communications (Kamat, Baliga, & Trappe, 2006). A drawback is the requirement that a trusted authority must extract private keys from vehicle identifiers rather than having vehicles generate their own key pairs.

9.3.3.2 Group signature schemes

The downside of using a changing set of anonymous keys as pseudonyms is the necessity for generation, delivery, storage and verification of numerous certificates for pseudonym public keys (or private keys in case of IBC). To mitigate this overhead, Calandriello et al. (2007) presented an approach that uses group signatures to enable vehicle OBUs to generate and certify their own pseudonyms without interacting with the CA. Basically, group signatures are used to support issuance of traditional public key certificates. The group manager (GM) is a new entity that sets group parameters, changes group public keys and may revoke anonymity if supported by the scheme. In contrast to the PP or CA, the GM role can be filled by a vehicle and need not necessarily be a trusted third party. In any case, the GM has a key role in the pseudonym generation. This raises issues of group leader election, identity escrow and revocation.

9.3.3.3 Symmetric cryptography schemes

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

For C2X communication, utilization of symmetric authentication schemes offers the benefits of short generation and verification time as well as less security overhead (Choi, Jakobsson, & Wetzel, 2005). Moreover, the need for deployment and maintenance of PKI and associated costs, as need for asymmetric schemes, could be replaced by potentially simpler key distribution. In a naïve scheme, each OBU could have the same secret key preinstalled, or even a set of shared secret keys (Xi et al., 2007). Due to the potential benefits, symmetric schemes have been considered for vehicular ad hoc network authentication. However, reliable authentication requires that exposure of single secret keys should not compromise authentication of all OBUs. This requirement,

paired with the desire for accountability, makes actual symmetric authentication schemes more complex.

9.3.4 Summary

As we have seen, privacy in vehicular networks is mainly protected by cryptographic means (i.e. pseudonyms). We presented the four main categories of pseudonym schemes with a focus on the asymmetric cryptography, as it is the one adopted by standardization bodies. However, the current sets of standard are unclear about pseudonym management, especially regarding pseudonym change strategies. Therefore, additional research efforts are required in defining a common privacy metric to compare pseudonym change strategies in order to decide the most appropriated one(s). Another underdeveloped aspect is the impact of privacy protection mechanisms on the C2X system, especially regarding safety level and routing protocol.

9.4 Misbehaviour detection

9.4.1 Definition and categorization

So far, we have discussed two central pillars of C2X security, one being secure identity management using a VPKI, certificates and digital signatures, and the other providing privacy protection through pseudonyms. We saw that the vehicular setting poses special challenges for both, and that dedicated and specifically adapted solutions were required.

In order to provide a complete security solution, we need to address yet an additional attacker model: insider attackers. So far, we are able to efficiently keep external attackers from successfully injecting malicious messages into the system – or at least we can ensure that receivers will notice that those malicious messages have not been sent by valid and authorized vehicles or RSUs and can ignore them. Furthermore, curious eavesdroppers will not be able to identify and track vehicles for a prolonged time as vehicles use pseudonyms that can only be resolved by specifically authorized entities and will change their pseudonyms frequently.

However, even if cryptographic credentials were securely stored inside a hardware security module (HSM), it would be unwise to completely ignore the threat posed by an attacker successfully breaching security mechanisms and then sending correctly signed messages containing incorrect information. Beyond, incorrect information may also come from perfectly benevolent vehicles that have, for example, malfunctioning sensors and therefore disseminate unreliable information. The consequences may range from none – if the information sent is not further regarded by receivers – to annoying – if drivers receive incorrect warning messages that they need to ignore – to fatal – if incorrect information would lead to unsafe driving or even accidents.

We define *misbehaviour detection* as the detection of such misbehaving nodes that disseminate incorrect information where we typically do not care whether misbehaviour is caused by malicious intent or by normal malfunction. Therefore, while C2X

misbehaviour detection is somehow related to (anomaly-based) intrusion detection, it differs in that it should cover all kinds of misbehaviour and that it specifically aims to detect incorrect data about real-world events.

Van der Heijden, Dietzel, and Kargl, (2013) and Dietzel et al. (2014) distinguish different approaches for misbehaviour detection. *Node-centric* mechanisms focus specifically on identities of misbehaving nodes, while *data-centric* misbehaviour detection covers those mechanisms that use semantics associated with the exchanged information for detection.

Node-centric mechanisms may use information related to the sender of a message like distance to the sender, frequency of messages sent by the node, or similar to detect misbehaviour. This category can be further subdivided into behavioural and trust-based mechanisms where the first category includes detection of unusual patterns in the behaviour of nodes, e.g. sending an extremely high number of messages or not conforming to protocol specifications when forwarding messages. Trust-based mechanisms, on the other hand, often use other mechanisms to build up long-term reputation scores for other nodes and then rate the trustworthiness of information received based on this reputation.

On the other hand, data-centric mechanisms focus on information itself, e.g. whether node positions contained in beacon messages are correct or not. There are two fundamental approaches for such detection: plausibility and consistency checking. Plausibility is trying to evaluate whether received data are considered valid within the scope of some model. This often involves models on driving physics and traffic. If a vehicle reports driving at 500 km/h, this is a lot less plausible than a reported speed of 50 km/h. If regular and misbehaving vehicles share streets, their reported information will almost inevitably create inconsistencies, like one vehicle reporting a road blocked by an obstacle where other vehicles report just driving through the obstacle. This can be detected by consistency-checking mechanisms.

9.4.2 Detection approaches

Leinmüller, Schoch, and Kargl, (2006), Leinmüller et al. (2010) were among the first to propose a variety of sensors capable of detecting spoofed position claims in C2X messages. They proposed a variety of heuristics to determine invalid positions and also an initial framework of how to combine outputs of multiple local or cooperative sensors based on weighted averaging. One example of the proposed sensors is the acceptance-range-threshold (ART), which detects if vehicles send beacons claiming to be at a position that would prevent reception of the messages at the local position, assuming a maximum communication range r. Another example is the mobility grade threshold (MGT) that checks if a vehicle would exceed a certain speed limit when moving from the position reported in one beacon to the next. Both ART and MGT are examples of data-centric plausibility checking. The authors show in simulations that a combination of two such basic sensors is already sufficient for effective detection of a simple attacker that fakes positions more or less randomly.

However, a more sophisticated attacker will likely use a cleverer spoofing scheme that will not be that easy to detect. Therefore, more advanced detection mechanisms

have been proposed to narrow down the spoofing opportunities for attackers. For example, Stübing, Firl, and Huss (2011) use Kalman filters and manoeuver recognition based on hidden Markov models to predict possible behaviour of a vehicle as depicted in Figure 9.7. Implausible deviations are considered as misbehaviour. An extension by Biβmeyer et al. (2012) checks if multiple vehicles would occupy the same physical space based on their reported positions, dimensions and headings. The latter is a good example of a mechanism from the data-centric, consistency-checking category.

Still, all the listed mechanisms will not provide hard evidence of misbehaviour but rather rate credibility of received messages on a scale that typically ranges from 0 to 1 or −1 to 1. Likewise, all detection mechanisms will detect some type of misbehaviour but not others.

9.4.3 Detection frameworks

In order to implement a truly robust and effective misbehaviour detection, one will have to combine multiple detection approaches within a detection framework. Leinmüller et al. (2006) proposed an early example of such a framework, and Raya et al. (2008) came up with a more sophisticated approach based on Dempster−Shafer logic. Stübing et al. (2011) came up with a highly effective − but also very specialized and complicated − framework that combines multiple sensors to detect spoofed positions. Figure 9.7 (Stübing, 2013) provides an overview of the multiple steps in this framework.

One of the most generic frameworks was recently introduced in Dietzel et al. (2014), which uses subjective logic to combine outputs of various sensors in a highly flexible way. Beyond simply providing a rating of the belief or disbelief in the correctness of information, subjective logic allows including uncertainty in the inference mechanisms and therefore automatically considers the accuracy of different detection mechanisms.

All the proposed mechanisms and frameworks can work on different levels of the C2X system. They can either be *local*, *cooperative* or *global* mechanisms working just inside one vehicle, cooperatively among neighbouring vehicles or in a central place like a traffic information centre, respectively.

9.4.4 Summary

In contrast to ID management and privacy protection through pseudonyms, which are both well covered by standardization efforts (especially the former; see Section 9.3.4), misbehaviour detection is still more of a research topic. While a broad range of mechanisms have been investigated and frameworks to integrate the various mechanisms have been proposed, there is not yet a clear consensus how to address the problem posed by insider attackers injecting incorrect information. This is partially due to a lack of understanding on the nature of attacks to expect and to the fact that all proposals can thus be only preliminary proposals that are evaluated against synthetic attacks. The best advice may be that standards should foresee a generic framework for misbehaviour detection that can flexibly and quickly react to appearing threats and can be extended by new detection mechanisms in the field.

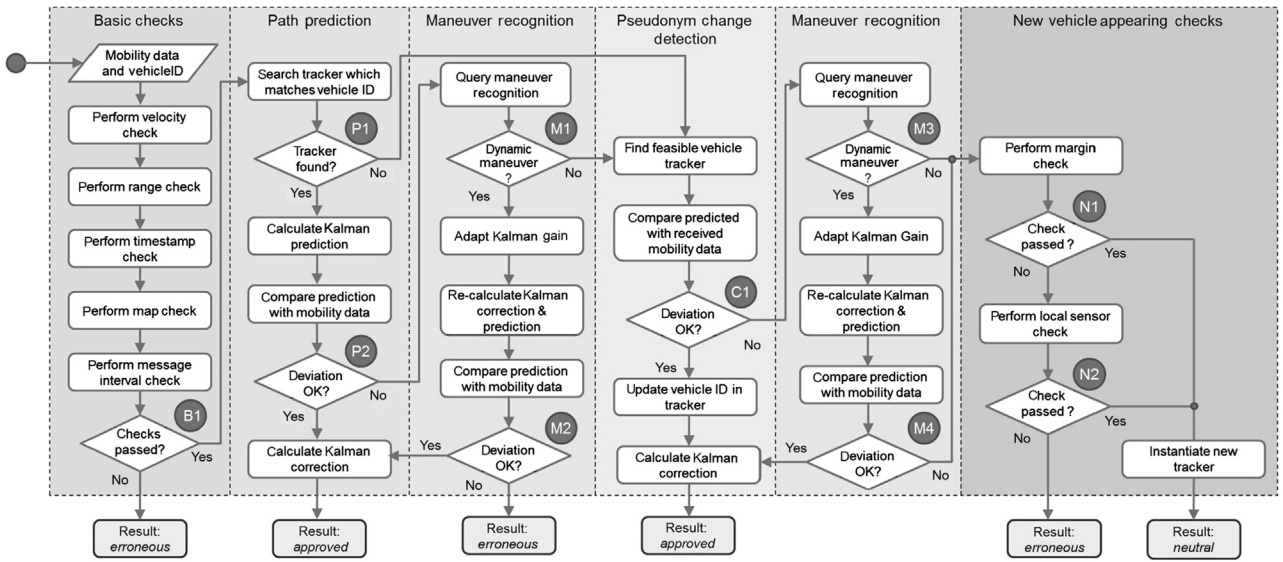

Figure 9.7 Verification flow of mobility data in C2X communication using path prediction and probabilistic manoeuvre recognition (from Stübing, 2013).

9.5 Outlook and open issues

In this chapter, we addressed the issues related to security and privacy protection in vehicular networks. We highlighted the importance of proper security and privacy protection for the success of C2X and showed the three major building blocks of a secure C2X system: (1) identity management, authentication, and message integrity; (2) privacy protection; and (3) misbehaviour detection. There is a broad body of scientific literature in all three areas, and we only discussed a small percentage of it due to space constraints. In ETSI, IEEE and ISO, a C2X security architecture is currently under standardization. While the first two building blocks can be considered final in ETSI and ISO, IEEE is still lacking a clear concept for privacy protection mechanisms. Beyond, misbehaviour detection still has to be considered a research field that has not yet presented a conclusive solution, mostly because real attacker models are unclear.

Furthermore, the integration with IP communication is still an open issue. In order to provide a consistent approach to security and privacy, IP- and safety-communication have to be integrated. Otherwise, privacy provided by pseudonyms for safety communication may be breached if stations have persistent IP addresses.

Another area of on-going research is scalability. When we will reach high deployment rates and have high-density traffic situations, our currently envisioned performance measures (like HSM and certificate omission) will be put under test. No such testing efforts have yet been conducted; previous field operation tests like simTD or DRIVE C2X have often left out complete security and privacy mechanisms from their tests. The European PRESERVE project is planning such performance testing under realistic conditions once its HSM becomes available.

Further challenges arise with the advent of automated driving. In 2013, the European Commission and United States Department of Transportation announced that automated vehicles will be connected[1] and that C2X technology will be deployed in automated vehicles. This will create additional security requirements and risk analysis that only assume assistive applications may have to be reassessed. The worst-case scenario of accidents and fatalities caused by malicious hackers needs to be avoided at all cost.

References

Bissmeyer, N., Stübing, H., Schoch, E., Götz, S., & Lonc, B. (2011). A generic public key infrastructure for securing Car-to-x communication. *18th world congress on intelligent transport systems*.

Bißmeyer, N., Njeukam, J., Petit, J., & Bayarou, K. M. (2012). Central misbehavior evaluation for VANETs based on mobility data plausibility. In: *Proceedings of the ninth ACM*

[1] February 3, 2014: decision by the U.S. Department of Transportation (USDOT) and the National Highway Traffic Safety Administration (NHTSA) to move forward with vehicle-to-vehicle communication for light vehicles. They believe that V2X technology could be a building block to achieving safe and reliable highly automated and self-driving automated vehicles.

international workshop on vehicular inter-networking, systems, and applications - VANET'12 (p. 73). New York, NY, USA: ACM Press. http://dx.doi.org/10.1145/2307888.2307902.

Blumberg, A. J., & Eckersley, P. (August, 2009). On locational privacy, and how to avoid losing it forever. *Electronic frontier foundation tech rep August* (pp 1−7). http://www.eff.org/files/eff-locational-privacy.pdf

Calandriello, G., Papadimitratos, P., Hubaux, J.-P., & Lioy, A. (2007). Efficient and robust pseudonymous authentication in VANET. In: *Proceedings of the fourth ACM international workshop on vehicular ad hoc networks VANET 07, 07,* 19. http://dx.doi.org/10.1145/1287748.1287752.

Calandriello, G., Papadimitratos, P., Hubaux, J.-P., & Lioy, A. (2011). On the performance of secure vehicular communication systems. *IEEE transactions on dependable and secure computing, 8*(6), 898−912. http://dx.doi.org/10.1109/TDSC.2010.58.

Choi, J. Y., Jakobsson, M., & Wetzel, S. (2005). Balancing auditability and privacy in vehicular networks. In: *Proceedings of the first ACM international workshop on quality of service & security in wireless and mobile networks* (pp. 79−87). http://dx.doi.org/10.1145/1089761.1089775.

Dietzel, S., van der Heijden, R., Decke, H., & Kargl, F. (2014). A flexible, subjective logic-based framework for misbehavior detection in V2V networks. *IEEE WoWMoM workshop on smart vehicles (IEEE SmartVehicles'14).*

ETSI. (2010). *ETSI EN 302 665 V1.1.1 (2010-09) − Intelligent transport systems (ITS); communications architecture*.

ETSI. (2012a). *ETSI TS 102 940 V1.1.1 (2012-06) − Intelligent transport systems (ITS); security; its communications security architecture and security management*.

ETSI. (2012b). *ETSI TS 102 941 V1.1.1 (2012-06) − Intelligent transport systems (ITS); security; trust and privacy management*.

ETSI. (2013). *ETSI TS 103 097 V1.1.1 (2013-04) − Intelligent transport systems (ITS); security; security header and certificate formats*.

Feiri, M., Schmidt, R. K., & Kargl, F. (2013). The impact of security on cooperative awareness in VANET. *2013 IEEE vehicular networking conference* (pp. 127−134). IEEE. http://dx.doi.org/10.1109/VNC.2013.6737599.

Feiri, M., Petit, J., & Kargl, F. (2012a). Congestion-based certificate omission in VANETs. In: *Proceedings of the ninth ACM international workshop on vehicular inter-networking, systems, and applications - VANET'12* (p. 135). New York, NY, USA: ACM Press. http://dx.doi.org/10.1145/2307888.2307915.

Feiri, M., Petit, J., & Kargl, F. (2012b). Evaluation of congestion-based certificate omission in VANETs, 2012. *IEEE vehicular networking conference (VNC)* (pp. 101−108). IEEE. http://dx.doi.org/10.1109/VNC.2012.6407417.

Gerlach, M., Festag, A., Leinmüller, T., Goldacker, G., & Harsch, C. (2005). Security architecture for vehicular communication. *World of intelligent transportation*. WIT, 2005. doi:10.1.1.121.453.

Gollan, L., & Meinel, C. (2002). Digital signatures for automobiles. In: *Proceedings of systemics, cybernetics and informatics* (SCI'02).

Van der Heijden, R., Dietzel, S., & Kargl, F. (2013). Misbehavior detection in vehicular ad-hoc networks. In: *Proceedings of 1st GI/ITG KuVS Fachgespräch inter-vehicle communication (FG-IVC 2013)* (pp. 23−25). http://www.ccs-labs.org/bib/pdf/vanderheijden2013misbehavior.pdf.

Hubaux, J. P., Capkun, S., & Luo, J. (2004). The security and privacy of smart vehicles. *IEEE Security & Privacy Magazine, 2*(3), 49−55. http://dx.doi.org/10.1109/MSP.2004.26.

IEEE. (2013). *IEEE 1609.2: Standard for wireless access in vehicular environments (WAVE) — security services for applications and management messages*.

ISO TC-ITS. (2007). *ISO 14813-1:2007-Intelligent transport systems — reference model architecture(s) for the its sector — Part 1: ITS service domains, service groups and services*.

Kamat, P., Baliga, A., & Trappe, W. (2006). An identity-based security framework for VANETs. In: *Proceedings of VANET* (pp. 94—95). http://dx.doi.org/10.1145/1161064.1161083, 2006.

Kargl, F. (2011). *PRESERVE fact sheet*. Available at: http://www.preserve-project.eu/about.

Kargl, F., Schoch, E., Wiedersheim, B., & Leinmüller, T. (2008). Secure and efficient beaconing for vehicular networks. In: *Proceedings of the fifth ACM international workshop on vehicular inter-networking - VANET'08* (p. 82). New York, NY, USA: ACM Press. http://dx.doi.org/10.1145/1410043.1410060.

Kargl, F., Papadimitratos, P., Buttyan, L., Muter, M., Schoch, E., Wiedersheim, B., et al. (2008). Secure vehicular communications: implementation, performance, and research challenges. *IEEE Communications Magazine, 46*(11), 2—8. http://dx.doi.org/10.1109/MCOM.2008.4689253.

Krishnan, H., & Weimerskirch, A. (2011). "Verify-on-Demand" - a practical and scalable approach for broadcast authentication in vehicle-to-vehicle communication. *SAE International Journal of Passenger Cars — Mechanical Systems, 4*(1), 536—546. http://dx.doi.org/10.4271/2011-01-0584.

Leinmüller, T., Schoch, E., Kargl, F., & Maihöfer, C. (2010). Decentralized position verification in geographic ad hoc routing. *Security and Communication Networks, 3*(4), 289—302. http://dx.doi.org/10.1002/sec.56.

Leinmüller, T., Schoch, E., & Kargl, F. (2006). Position verification approaches for vehicular ad hoc networks. *IEEE Wireless Communication Magazine, 13*(5), 16—21. http://dx.doi.org/10.1109/WC-M.2006.250353.

Ma, Z., Kargl, F., & Weber, M. (2010). Measuring long-term location privacy in vehicular communication systems. *Elsevier Computer Communications, 33*(12), 1414—1427. http://dx.doi.org/10.1016/j.comcom.2010.02.032.

NSA. (2009). *The case for elliptic curve cryptography*. http://www.nsa.gov/business/programs/elliptic_curve.shtml.

Papadimitratos, P., Calandriello, G., Hubaux, J.-P., & Lioy, A. (2008). Impact of vehicular communications security on transportation safety. *IEEE INFOCOM 2008-IEEE conference on computer communications workshops* (pp. 1—6). IEEE. http://dx.doi.org/10.1109/INFOCOM.2008.4544663.

Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., et al. (2008). Secure vehicular communications: design and architecture. *IEEE Communications Magazine, 46*(11), 2—8. http://dx.doi.org/10.1109/MCOM.2008.4689252.

Papadimitratos, P., Gligor, V., & Hubaux, J.-P. (2006). Securing vehicular communications - assumptions, requirements, and principles. *Fourth workshop on embedded security in cars (ESCAR'06)*, 10.1.1.140.4967.

Parno, B., & Perrig, A. (2005). Challenges in securing vehicular networks. *Workshop on hot topics in networks (HotNets-IV)*, 10.1.1.97.4852.

Paruchuri, V., & Durresi, A. (2010). PAAVE: protocol for anonymous authentication in vehicular networks using smart cards. *2010 IEEE global telecommunications conference GLOBECOM 2010* (pp. 1—5). IEEE. http://dx.doi.org/10.1109/GLOCOM.2010.5683087.

Puñal, O., Aguiar, A., & Gross, J. (2012). In VANETs we trust?: characterizing RF jamming in vehicular networks. In: *Proceedings of the ninth ACM international workshop on vehicular inter-networking, systems, and applications. VANET'12* (pp. 83—92). New York, NY, USA: ACM. http://dx.doi.org/10.1145/2307888.2307903.

Raya, M., Papadimitratos, P., Gligor, V. D., & Hubaux, J.-P. (2008). On data-centric trust establishment in ephemeral ad hoc networks. *2008 IEEE INFOCOM − the 27th conference on computer communications* (pp. 1238−1246). IEEE. http://dx.doi.org/10.1109/INFOCOM.2008.180.

Raya, M., & Hubaux, J.-P. (2007). Securing vehicular ad hoc networks. *Journal of Computer Security, 15*(1), 39−68 (JCS).

Schaub, F., Ma, Z., & Kargl, F. (2009). Privacy requirements in vehicular communication systems. *IEEE international conference on privacy, security, risk, and trust (PASSAT 2009), symposium on secure computing (SecureCom09)*. Canada: Vancouver. http://dx.doi.org/10.1109/CSE.2009.135.

Schoch, E., & Kargl, F. (2010). On the efficiency of secure beaconing in VANETs. In: *Proceedings of the third ACM conference on wireless network security − WiSec'10* (p. 111). New York, NY, USA: ACM Press. http://dx.doi.org/10.1145/1741866.1741885.

Shamir, A. (1985). Identity-based cryptosystems and signature schemes. *Advances in cryptology (CRYPTO'84)*. Springer. http://dx.doi.org/10.1007/3-540-39568-7_5.

Stübing, H. (2013). *Multi-layered security and privacy protection in cooperatove vehicular networks - solutions from application down to physical layer* (Ph.D. thesis). TU Darmstadt.

Stübing, H., Firl, J., & Huss, S. A. (2011). A two-stage verification process for Car-to-X mobility data based on path prediction and probabilistic maneuver recognition, 2011. *IEEE vehicular networking conference* (pp. 17−24). IEEE. http://dx.doi.org/10.1109/VNC.2011.6117119. VNC.

Studer, A., Bai, F., Bellur, B., & Perrig, A. (2009). Flexible, extensible, and efficient VANET authentication. *Journal of Communications and Networks, 11*(6), 574−588. http://dx.doi.org/10.1109/JCN.2009.6388411.

Xi, Y., Sha, K., Shi, W., Schwiebert, L., & Zhang, T. (2007). *Enforcing privacy using symmetric random key-set in vehicular networks. Eighth international symposium on autonomous decentralized systems (ISADS'07)* (pp. 344−351). http://dx.doi.org/10.1109/ISADS.2007.37.

Zarki, M. El, Mehrotra, S., Tsudik,, G., & Venkatasubramanian, N. (2002). Security issues in a future vehicular network. *Europea'n wireless (EW'02)*, 10.1.1.122.2138.

Zhang, C., Lin, X., Lu, R., & Ho, P.-H. (2008). RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks, 2008. *IEEE international conference on communications* (pp. 1451−1457). IEEE. http://dx.doi.org/10.1109/ICC.2008.281.