Cross-layer Privacy Enhancement and Non-repudiation in Vehicular Communication

Frederik Armknecht[1], Andreas Festag[2], Dirk Westhoff[1], Ke Zeng[3]

[1] NEC Network Laboratories, Germany
[2] NEC Deutschland, Germany
[3] NEC Laboratories, China

Abstract. We propose a security architecture that provides two fundamental security services for VANETS: i) non-repudiation and ii) privacy enhancement. Due to a new PKI concept, referred to as PKI+, users are autonomous in deriving public keys, certificates and pseudonyms which minimizes the communication to the certificate authority. Security techniques are supported on all layers of the protocol stack. In particular we show how to link the PKI+ concepts to solutions for routing in vehicle-to-vehicle and vehicle-to-infrastructure communication.

1 Vehicular communication

Vehicular Ad Hoc Networks (VANETs) currently seem to be one of the civilian ad hoc network applications which are most relevant due to their impact to market. A set of nearly 50 applications have been submitted by major car manufacturers BMW, Daimler-Chrysler, Ford, and GM which are based on Dedicated Short Range Communication (DSRC) technology [1]. The applications are roughly classified into public safety and private applications. Public safety applications range from cooperative collision warning, toll collection, to vehicle safety inspection. Private applications include parking lot payment, rental car processing, data transfers like music data updates.

VANETs lack a central instance for network organization. They represent fully distributed and self-organizing networks for vehicle-to-vehicle and vehicle-to-roadside communication based on wireless multi-hop communication. Furthermore, VANET nodes are highly mobile which results in frequent changes in the network topology. This feature necessities appropriate routing mechanisms.

A currently missing aspect in VANET research development is an overall security architecture, which is flexible enough to address the security requirements of all the envisioned applications for vehicular communications. It is clear from the above enumeration of applications that the security requirements for the various public safety and private applications have significantly varying needs with respect to security.

Sharply defined security-requirements are mandatory in the automotive industry to convince traditionally defense decision makers. Although this is out of scope of this paper we believe that most DSRC-based applications need mechanisms which provide *non-repudiation* by ensuring a reasonable level of *privacy*

at the same time. Non-repudiation – the service which prevents an entity from denying previous commitments or actions – is mandatory in all applications where emergency calls may save lives so that sender who send wrong information on purpose can be called to account. Obviously, for DSRC applications with a (post)-paid charging and billing component non-repudiation is also necessary. *Privacy* – informally defined as confidentiality for personal data like user IDs, profiles or location – is probably the most challenging security requirement to be fulfilled in vehicular communication. As privacy on a single layer of the protocol stack is useless considering a relatively powerful attacker it is a cross-layer issue.

It is the contribution of this work at hand to come up with a VANET architecture which provides privacy enhancement and non-repudiation on any protocol layer. The paper is structured as follows. In Section 2 we describe the network and protocol architecture and derive security requirements in Section 3. Section 4 explains the proposed security architecture. Section 5 gives an overview of related work, and Section 6 concludes the paper.

2 Network and protocol architecture

The assumed network architecture splits into three domains (Fig. 1(a)): the in-vehicle domain is a sub-network with an *On Board Unit* (OBU) and potentially several *Application Units* (AUs), e.g. PDA, mobile phone. The ad hoc domain is composed of OBUs and stationary units along the road, termed *Road-Side Units* (RSUs). OBUs and RSUs are equipped with wireless technology based on IEEE 802.11 technology. They can either communicate directly or use multi-hop communication. The infrastructure domain provides connectivity to Internet nodes and servers and access to Internet services. The infrastructure access is provided via RSUs if available.

For efficient and scalable communication in the ad hoc domain, position-based routing (PBR) is applied [2]. It provides wireless multi-hop communication between two nodes (unicast using so called 'greedy forwarding') and efficient broadcasting of data packets in geographical areas (geocast). Integral parts of PBR are beaconing and location service: Using beacons, a node periodically advertises its identifier and position to the direct neighbor nodes. With the location service a destination node is searched for its current position. Every OBU maintains a soft-state *location table* (LT) with (at least) identifier, position, speed, heading, and timestamp of the node the OBU communicates with. The LT comprises data from both, neighbors and non-neighbors. The data are acquired from beacons, data packets, etc. that are processed by a node. The LT is used for routing of unicast packets in order to make decisions on the next hop of a packet.

As OBUs have to deal with basically two different kind of messages, namely safety and non- safety, the diversity needs to be supported in the protocol architecture as well. In the remainder of the paper we envision a protocol architecture as displayed in Fig. 1(b). We principally distinguish among three basic types of wireless technologies: IEEE 802.11p wireless technology dedicated for
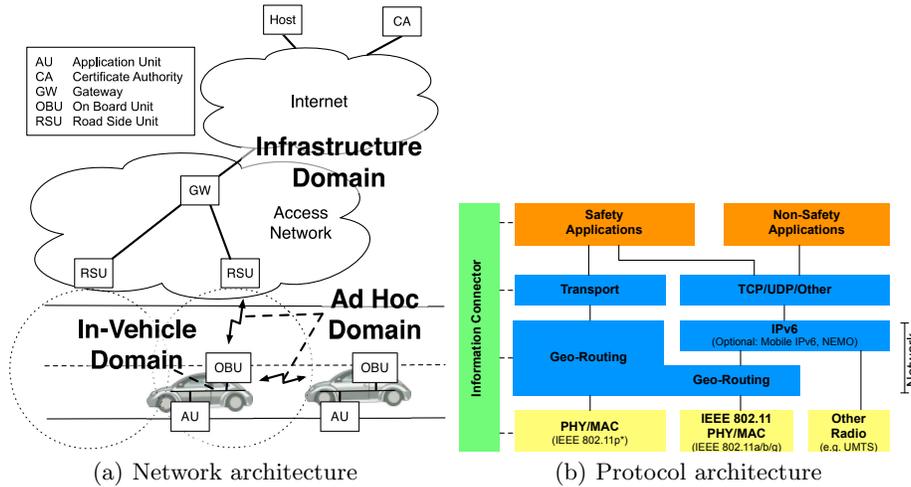
(a) Network architecture   (b) Protocol architecture

Fig. 1. High-level system architecture view

road safety, conventional wireless LAN technologies based on IEEE 802.11a/b/g and other radio technologies (like UMTS). On top of the radio protocol layers MAC and PHY of the specific technologies, the geo-routing layer provides wireless multi-hop communication based on geographic positions, and executes network-specific tasks like VANET congestion control. Non-safety applications can either use wireless multi-hop communication or the Internet via the regular TCP/IP protocol stack, for example to access wireless Hot Spots.

Safety messages should be treated with a higher priority than non-safety messages. Therefore, safety applications can access protected radio frequencies as specified in IEEE 802.11p. As non-safety applications are not allowed to use these, it is ensured that the transmission of safety messages is not blocked by non-safety messages. Of course, safety applications can likewise use the same radio technologies as the non-safety messages.

A particular property of the protocol architecture in OBUs is the existence of a specific module called the information connector. It coordinates the cross-layer data exchange among the different layers and provides an asynchronous exchange of events based on public or subscribed patterns. For example, if the location table reveals that a vehicle is approaching with high velocity, the safety application is informed to potentially warn the driver.

3 Security requirements

The transmission of safety information creates new types of threats. An adversary could influence the road traffic by distributing wrong information. Damages could range from a disproportional volume of road traffic by signaling free streets being blocked up to accidents by pretending wrong safety. Thus, safety related

messages are only valuable if the common driver can trust them. In [3] possible attackers are classified as insider vs. outsider, malicious vs. rational, and active vs. passive. The aim should be to provide protection against any of these kinds.

A widely discussed approach is to link a sender's identity in a unique and non-repudiable way to his message. This means that it should be clear anytime who has send the message and the sender should not be able to deny its authorship. based on the assumption that every node has a unique and static *Global ID* (GID). The linking between a safety message and GID is usually achieved by digitally signing the message. A digital signature is a cryptographic tool, based on asymmetric cryptography, that can be used to authenticate the signer, and possibly to ensure that the message's content remained unchanged. A signer owns a private/public key pair where the public key is openly known. The private key is mandatory for signing data, whereas the validity of the signature can be checked by only knowing the public key.

As everyone can in principle create an own pair of private and public key, a trusted *certificate authority* (CA) is usually assumed. In practice the CA might be operated by the state, individual cities, or by an union of several vehicle manufactures. At the beginning, the CA signs the public key of the user. This signature is called a certificate of the user's key. Furthermore, it stores the user's GID together with his public key to trace back the identity from a signature in the case of need. Consequently safety messages should be ignored if they are not signed with a certified public key. This approach requires the existence of an appropriate public key infrastructure (PKI).

Unfortunately, by simply storing all messages connected to one GID an attacker could (at least partly) reconstruct where the vehicle has been at which time. Due to the long-time binding between a car and its owner, this is practically equivalent to observe the person. When the GID represents an *electronic license plate* [4], an adversary can even link the identifier to the personal data of the registered vehicle owner. Surely, this contradicts the usual privacy needs. Consequently, the vehicle's GID should be kept anonymous in the normal operation mode. In order to provide anonymity it is proposed that a user receives several different pseudonyms from the CA, together with associated private/public key pairs and certificates. To keep the descriptions simple we will refer to the public key as the pseudonym. A node can change its pseudonym and associated signature and certificate in order to prevent identity and location tracking. Only the CA can connect a pseudonym with the GID.

Summing up, it seems that non-repudiation and anonymity are two contradicting demands. Even more, this requirement needs to be satisfied on every protocol layer. For example it makes no sense to change pseudonyms on the application layer if the beacons on the routing layer remain connected to the same identifier.

4 Overview of the security architecture

In this section we propose a security architecture for VANETs that meets all security requirements explained in the previous section. Firstly, we describe in Section 4.1 an extended PKI, called PKI+. As opposed to conventional solutions, the users in PKI+ can generate certified pseudonyms on their own which significantly reduces the communication overhead. Secondly, we describe in Section 4.2 how to use these pseudonyms on any layer, especially on the routing level. In this way the overall protocol architecture benefits from PKI+. Additionally, our proposal can be combined with other publicly discussed security mechanism to achieve further security goals.

4.1 PKI+

The recent PKI+ approach [5] retains the concept of the well-known PKI approach, but provides the additional benefit that a user can autonomously generate pseudonyms together with appropriate certificates. It is based on using a special kind of elliptic curves. PKI+ itself is secure against all types of attackers on the basis of tamper-resistant hardware.

The PKI+ approach has five different operation stages (see Figure 2). At the first stage, the CA sets up the PKI by determining security strength, choosing appropriate elliptic curves, selecting a secret key, and publishing the public key. At the second stage, the user, based on his/her secret user key, proves its identity to the CA and gets a master key and master certificate from the CA. Although the user shares the master key with the CA, the secret user key effectively prevents the CA from impersonating the user. At the third stage, the user takes its master key, master certificate, and the CA's public-key as input, and creates a pseudonym with an appropriate certificate so that it can anonymously authenticate and securely communicate with other parties. Note that the generation can be offline or beforehand.

The fourth stage is for the CA to figure out the real holder of a pair of a certified pseudonym. This tracing capability is crucial to the CA (however only to the CA) when in case some user misbehaves. This stage may be followed by the fifth stage which is for the CA to revoke keys.

As explained in Section 3, safety messages should be digitally signed and be verifiable with the sender's pseudonym. The pseudonym itself is verifiable by the certificate generated by the user and the CA's public-key. When the pseudonym is certified by the CA, it is also determined that the pseudonym and certificate pair are traceable to the CA. In other words, a sender that is known to the CA, although anonymous to the other users, cannot deny its authorship of the message (non-repudiable keys). On the other hand it was shown in [5] that it is computationally infeasible for an attacker to link any two pairs of pseudonyms and certificates, what supports the sender's identity.

Finally, it does not matter how many users have registered with and how frequent messages are exchanged among registered vehicles as no user needs to communicate with the CA any more for privacy protection purpose such as
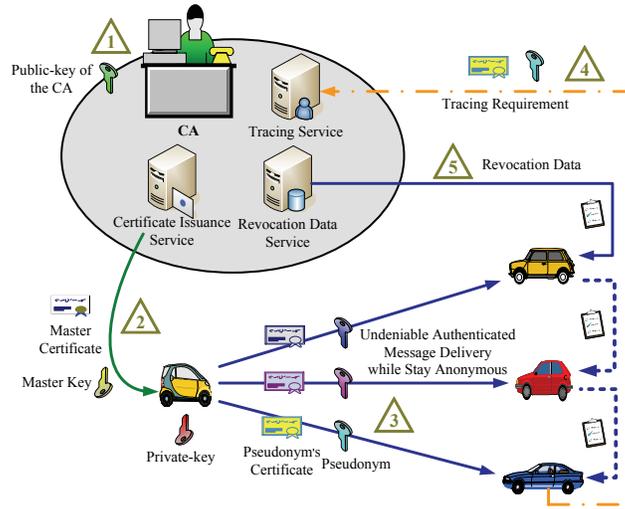
Fig. 2. Operation stages of PKI+

refreshing certificates. This merit is unique to the PKI+ based approach since previous solutions [6] cannot generate certificates by themselves. Instead, they are pre-filled with a number of keys and certificates. Therefore it is inevitable for the vehicles to contact the CA and renew the certificates from time to time in case the pre-filled certificates are all used up.

When utilized in VANET messaging system, the PKI+ approach has another special advantage in case of revocation. Whenever a key has to be revoked the CA publishes some data depending on which the nodes have to update their keys. For this purpose the data is chosen such that it cannot be used by the excluded node, thus impeding it from updating its master key. Previous PKI proposals don't share this merit because each vehicle's public-key and certificate would have to be revoked independently. When some vehicle is revoked, all its certificates need to be added in the revocation data. The size of revocation data could be so big that it becomes impractical to exchange the revocation data between fast moving cars. However, with PKI+ due to the small data size this may still be practical. As a concrete example, when the underlying elliptic curve for bilinear mapping is selected as MNT curve [7] of embedding degree 6, finite cyclic groups of order 170 over it, gives approximately the same security strength as a standard 1.024 bits RSA signature scheme. In this setting, the size of revocation data per each revoked vehicle is no more than 1.367 bits.

Data efficiency makes the PKI+ approach particularly advantageous for VANETs. With the above setting, the vehicle generated pseudonym is 342 bits long, anonymous certificate 680 bits, and message signature 340 bits. The num-

ber of pseudonym and certificate pairs a vehicle can generate would be 2^{170}, being practically infinite.

4.2 Secure geographical routing

Similar to other ad hoc routing protocols, geographical routing is vulnerable against spoofing and forging of routing signaling messages that can result in creation of routing loops and mal-functioning of the network [8]. A specific attack on geographical routing is based on forging of location information carried in routing headers. This is illustrated in Figure 3: The left figure shows a regular forwarding process from the source via forwarders F1, F2, and F3 to the destination. In the middle figure, the attacker *Att* forges its location such that node F3 selects the attacker as next hop in the forwarding chain. The attacker then drops all received packets ('sinkhole' attack). In the right figure, the attacker forges its position and forwards the received packets back to the previous node. The resulting routing loop causes packets to be sent forth and back.

In order to secure wireless multi-hop communication based on geographic routing we target at the following security objectives: *(i) Integrity* of the routing header prevents malicious and accidental altering of header fields in an unauthorized manner by an outsider attacker. *(ii) Authentication* enables forwarders and receivers to verify that a data packet originated from source and sender in a multi-hop forwarding chain.[1] *(iii) Non-repudiation* in our scenario provides a means that the source of a data packet cannot deny having sent the packet. In addition to these conventional security objectives, *(iv) Anonymity* ensures that a node – sender, forwarder, and receiver – is not identifiable for other nodes and hence hides personal data like location, speed, and heading. Anonymity, however, should allow a node to reveal its identity to other nodes for reasons like reputation and session establishment or to legal authorities.
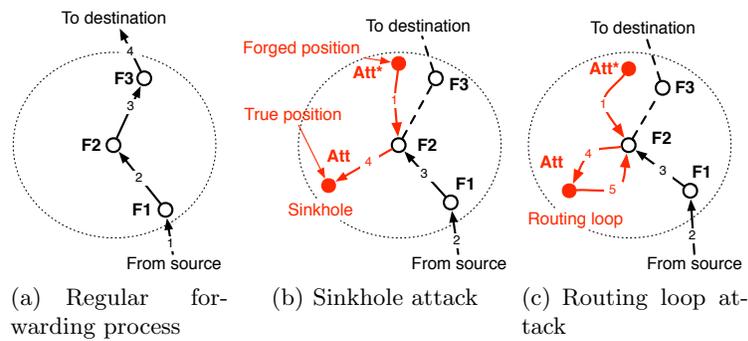

(a) Regular forwarding process (b) Sinkhole attack (c) Routing loop attack

Fig. 3. Two exemplary attacks in geographical routing based on location spoofing

---

[1] With multi-hop forwarder we refer to source as the origin of the packet, and sender to the previous wireless hop.

The core of the proposed approach is based on digital signatures. For this the PKI+ solution described in Section 4.1 is perfectly suited to provide the required infrastructure. A CA issues a master key pair and master certificate to a vehicle's on-board unit (OBU). The OBU then generates a set of pseudonyms together with appropriate certificates.

The header used in a geo-routing packet can be divided in mutable and immutable fields. Immutable are those fields that remain unchanged from sender to destination while intermediate hops forward the packet towards the destination, e.g. destination and source addresses and source position. Mutable fields, such as sender address, position and time-to-live (TTL) are allowed to be altered by intermediate nodes. For packets being sent via multiple wireless hops, two signatures are added: An end-to-end signature is created by the source node over the immutable fields of the packet header.[2] Additionally, a hop-by-hop signature is added for the mutable fields. On reception of a data packet a node verifies both signatures, and replaces the hop-by-hop signature by a new one for the altered mutable fields and keeps the end-to-end signature. Eventually, the combination of end-to-end signatures results in a trusted forwarding chain. As an option to hop-by-hop signatures, so called 'onion signatures' can be used to create a signature on the signature of the previous node in the forwarding chain. Then the receiver of the packet can reconstruct the forwarding chain and the plausibility checks made by predecessor nodes. The whole concept is depicted in Figure 4. The colors indicate which fields are signed by which node. For example, in the data package showed in the middle, two signatures are included. One has been created by node S for the immutable fields and the second signature by node $F1$ for the mutable fields.
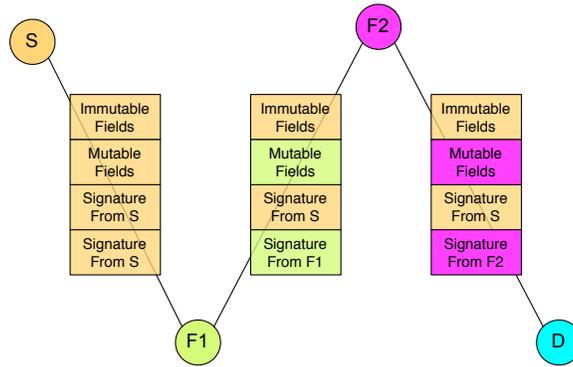

Fig. 4. Signature operations on mutable and immutable fields

The approach achieves authentication by requiring that only signatures using certified keys are accepted. As explained in Section 4.1, signatures based on

---

[2] For efficiency, the signature should be generated for all immutable fields of the overall data packet, including the payload with application data.

PKI+ keys are non-repudiable. Additionally integrity is ensured as changing the content of signed data would require to change the signature as well which is not possible for an attacker.

In order to preserve anonymity of users, OBUs should use pseudonyms that can only be linked to their GID by an authority. In order to prevent tracking, a node changes the pseudonym frequently such that an attacker cannot link the old and the new pseudonym. For this purpose, the advantage of PKI+ that a vehicle can locally create its pseudonyms from a master key becomes extremely useful. However, the change of a pseudonym has a number of implications. Too frequent changes may result in a loss of reachability, e.g. cf. [9], but this is outside the scope of our proposal. To establish communication sessions between two nodes, a secure resolution protocol allows to resolve a node's identity to it's currently used pseudonym. Also, when the pseudonym changes, addresses on all protocol layers (such as MAC address) and the certificate carried in data packets need to be changed [10].

Therefore we propose to use the pseudonyms not only for signing the messages but also to generate node addresses. Clearly, it is not sufficient to use pseudonyms on one protocol layer, but on all layers of the protocol stack. In order to generate addresses for the network layer, we rely on the concept of *Cryptographically-Generated Addresses (CGA)* [11]. A CGA is an IPv6 address where the host part is defined by the hash value of the public key. This links the public key to the IPv6 address. This concept is adapted to other protocol layers, where the same hash value of the public key is also converted to a MAC address and an address for geographic routing (see Figure 5). In this way, all addresses are linked to the currently used pseudonym. The main benefit lies in the process of pseudonym change: By generating a single hash value of the actual pseudonyms, the addresses on all protocol layers can be changed simultaneously and privacy is provided on all layers.
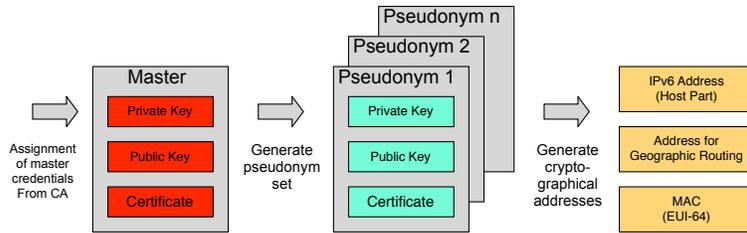

Fig. 5. Derivation of addresses for different protocol layers from pseudonyms

Apart from the approaches described above based on digital signatures and pseudonyms, we propose to additionally use plausibility checks. A receiving node, either a forwarder or the destination node, checks the data carried by the packet header for its plausibility. In general there are two methods: In the first method, more than one node distribute the same or similar information, and hence the

information is assumed to be trustable because of colluding attacks are considered to be unlikely. This method represents a legitimate application layer mechanism where an information, for example about an icy road hazard, needs to be received from another node before being regarded as plausible. The second method verifies the data values in a packet based on heuristics that check the values to lie inside of data boundaries. This second method is applicable at the routing layer.

We propose plausibility checks for the data carried by the routing header of a data packet, i.e. position, speed, heading, and time stamp that utilize implicit knowledge about physical constraints. As an example for position verification a node checks the position value of the neighbor node and calculates the distance. The information is plausible when the distance is smaller than the assumed maximum wireless transmission range (typically less than 1000 meters). Speed and heading are checked for feasible values (less than maximum speed and between 0 and 360°, respectively). Time is checked to be in a time window in the range of seconds up to the current time and must not lie in the future.

While outsider attacks are prevented by verification of the digital signatures, the plausibility checks verify routing header values to make insider attacks more difficult.

5 Related work

Vehicular communication has attracted strong interest from public and private, including governments, industry, academia, and standardization bodies. The technology development has gathered momentum from two main directions. In the first direction, roads and vehicles are understood as part of a vision for ubiquitous networking which enables communication anywhere and anytime. By extending current cellular networks and incorporating alternative wireless technologies like wireless LAN, infra-red, and others, communication and information services for drivers and passengers can increasingly be based on in-car equipment and wireless base stations along roads and highways. An example is CALM[3] [12], an ISO standardization effort towards continuous and seamless use of different communication media by in-vehicle and roadside communication modules.

The other main direction primarily targets at making future road traffic safer and more efficient. Here, vehicular communication is regarded as the underlying technology for future *Intelligent Transportation Systems (ITS)*. These systems are based on a variant of IEEE 802.11 dedicated for vehicular environments, also referred to *Dedicated Short Range Communication (DSRC)*. The development of these vehicular communication systems is driven by a number of national and international activities, including research projects, such as *PATH* [13], *Fleet-Net* [14], *NoW - Network on Wheels* [15], *PREVENT* [16], *ASV3* [17]. The research is accompanied by efforts to set up a communication infrastructure on the roadways, such as the *Vehicle-Infrastructure Initiative (VII)* in the US [18],

---

[3] Continuous air interface, long and medium range

and development programs, such as the European *eSafety* program [19]. Consortia like *Car-to-Car Communication consortium (C2C-CC)* [20] and Internet ITS [21] attempt to develop common specifications. Finally, standardization bodies – *American Society for Testing and Materials (ASTM)*, the *Institute of Electrical and Electronic Engineers (IEEE)*, and the *Society of Automotive Engineers (SAE)* – have already published draft standards (IEEE 802.11p, IEEE P1609 [22,23,24]). Conclusively, in some countries, frequencies have been pre-allocated for ITS, such as in the 5.9GHz frequency range in North America and Europe.

While research development efforts have achieved first results in development, proof-of-concepts, and initial real-world measurements, there is considerably little existing work in security for vehicular networks. Since a security solution is regarded as challenging due to its potentially high requirements for real-time and scalability, it gets more into the focus. The tradeoff between strong security and driver anonymity has been recognized as a particular demand [4,25,26].

The *Vehicle Safety Communication Project (VSC)* [27] has developed a high-level security architecture for a road safety communication system which provides message integrity, origin authentication, correctness, and privacy of safety messages. With the assumption that RSUs and public safety OBUs (PS-OBUs) have no anonymity requirements opposed to OBU, a dual authentication structure is proposed. For security of RSUs and PS-OBUs a conventional *public key infrastructure (PKI)* is responsible for issuance of digital certificates and revocation information. In contrast, OBUs utilize *anonymous certificates* for message authentication. An escrow would be able to link certificate and vehicle identity under certain conditions. As discussed in [27] anonymous certificates imply a considerable complexity for key management, mainly due to the need of re-issuance of expired certificates and handling of compromise through certificate *Certificate Revocation Lists*.

6 Conclusions

In this paper, we proposed a security architecture for VANETS. It is based on two new concepts: an extended PKI called PKI+ and secure geographical routing. Compared to conventional PKI concepts, PKI+ allows the user to act almost completely autonomous. After receiving one master key and a master certificate from the CA, the user can create his own certified pseudonyms without interaction with the CA. These pseudonyms are not only useful on the application layer but can be used to sign the messages on lower protocol layers to ensure secure geographical routing. The proposed secure geographical routing scheme provides protection of mutable and immutable fields in the data packet headers by combination of end-to-end and hop-by-hop signatures. We discussed how to derive addresses for the different layers from the pseudonyms in order to provide cross-layer non-repudiation and privacy enhancement.

References

1. Dedicated Short Range Communications (DSRC) Working Group. http://grouper.ieee.org/groups/scc32/dsrc/index.html.
2. H. Füßler, M. Mauve, H. Hartenstein, C. Lochert, D. Vollmer, D. Herrmann, and W. Franz. Position-Based Routing in Ad-Hoc Wireless Networks. In *Inter-Vehicle-Communications Based on Ad Hoc Networking Principles —The FleetNet Project*, pages 117–143. Universitätsverlag, Karlsruhe, Germany, 2005.
3. M. Raya and J.-P. Hubaux. The Security of Vehicular Ad Hoc Networks. In *Proc. of SASN 2005*, pages 11–21, Alexandria, VA, USA, 2005.
4. J. P. Hubaux, S. Capkun, and J. Luo. The Security and Privacy of Smart Vehicles. *IEEE Security and Privacy Magazin*, 2(3):49–55, 2004.
5. K. Zeng. Pseudonymous PKI for Ubiquitous Computing. In *Proc. of EuroPKI*, pages 207–222, Turin, Italy, 2006.
6. J.-P. Hubaux. The Security of Vehicular Networks. In *Proc. of WiSe 2005*, pages 31–32, New York, NY, USA, 2005. ACM Press.
7. A. Miyaji, M. Nakabayashi, and S. Takano. New Explicit Conditions of Elliptic Curves for FR-Reduction. *IEICE Trans. Fundamentals*, E84-A(5):1234–1243, 2001.
8. A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, T. Leinmüller, and R. Kroh. Attacks on Inter Vehicle Communication Systems - an Analysis. In *Proc. of WIT*, pages 189–194, Hamburg, Germany, 2006.
9. F. Kargl, T. Leinmüller, P. Papadimitratos, S. Schlott, and E. Schoch. Impact of Pseudonym Changes on Geographic Routing in VANETs. In *Proc. of ESAS*, 2006.
10. E. Fonseca, A. Festag, R. Baldessari, and R. Aguiar. Support of Anonymity in VANETs - Putting Pseudonymity into Practice. In *Proc. of WCNC*, Hong Kong, CN, 2007.
11. T. Aura. Cryptographically Generated Addresses (CGA). RFC 3972, IETF, 2005.
12. ISO TC 204 ETSI ERM TG37. The CALM Handbook, 2004.
13. Project PATH. http://www.path.berkeley.edu.
14. Project FleetNet – Internet on the Road. http://www.et2.tu-harburg.de/fleetnet/.
15. Project NoW – Network on Wheels. http://www.network-on-wheels.de.
16. Project PReVENT. http://www.prevent-ip.org.
17. Project ASV3: Advanced Safety Vehicle – Phase 3. http://www.mlit.go.jp/ jidosha/anzen/asv/ASV3%20HP/syasyakannhanfu/ gizyutusetumei.pdf.
18. Vehicle Infrastructure Integration (VII). http://www.its.dot.gov/vii/.
19. eSafety Program of the European Union. http://europa.eu.int/information_society/ activities/esafety/.
20. Car 2 Car Communication (C2CC) Consortium. http://www.car2car.org.
21. Internet ITS Consortium. http://www.internetits.org.
22. IEEE. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Wireless Access in Vehicular Environments (WAVE), 2006.
23. Committee SCC32 of the IEEE ITS Council. Draft Standard for Wireless Access in Vehicular Environments. IEEE P1609/1,2,3,4, 2005.
24. Society of Automotive Engineers (SAE). Dedicated Short Range Communications (DSRC) Message Set Dictionary. SAE J2735, 2006.
25. B. Parno and A. Perrig. Challenges in Securing Vehicular Networks. In *Proc. of HotNets-IV*, College Park, MD, USA, 2005.
26. J. Crowcoft. The Privacy and Safety Impact of Technology Choices for Command, Communications and Control of the Public Highway. *ACM SIGCOMM Computer Communication Review*, 36(1):53–57, 2006.
27. Vehicle Safety Communication Project. Final report. Submitted to the US Department of Transportation, FHWA and NHTSA, 2005.