Architecture for Secure and Private Vehicular Communications

P. Papadimitratos, EPFL, Lausanne, Switzerland
L. Buttyan, BUTE, Budapest, Hungary
J-P. Hubaux, EPFL, Lausanne, Switzerland
F. Kargl, Ulm Univesrity, Ulm, Germany
A. Kung, TRIALOG, Paris, France
M. Raya, EPFL, Lausanne, Switzerland

***Abstract*— The deployment of vehicular communication (VC) systems is strongly dependent on their security and privacy features. In this paper, we propose a security architecture for VC. The primary objectives of the architecture include the management of identities and cryptographic keys, the security of communications, and the integration of privacy enhancing technologies. Our design approach aims at a system that relies on well-understood components which can be upgraded to provide enhanced security and privacy protection in the future. This effort is undertaken by SeVeCom (http://www.sevecom.org), a transversal project providing security and privacy enhancing mechanisms compatible with the VC technologies currently under development by all EU funded projects.**

I. Introduction

Vehicular communications (VC) lie at the core of a number of industry and academic research initiatives aiming to enhance safety and efficiency of transportation systems. Vehicles and road-side infrastructure units (RSUs), i.e., network nodes, will be equipped with on-board processing and wireless communication modules. *Vehicle-to-vehicle (V2V)* and *vehicle-to-infrastructure (V2I)* communication will enable applications that provide warnings on environmental hazards (e.g., ice on the pavement), as well as traffic and road conditions (e.g., emergency braking, congestion, or construction sites).

VC offer a rich set of tools to drivers and administrators of transportation systems but, at the same time, they make possible a formidable set of abuses and attacks. Consider, for example, nodes that 'contaminate' large portions of the vehicular network with false information, or the deployment of nodes that collect VC messages, track the location and transactions of vehicles and infer sensitive information about their drivers. Worse even, vehicles and their processing and sensing equipment can be physically compromised, while any wireless-enabled device could pose a threat to the VC system.

These simple examples of exploits indicate that under all circumstances VC systems must be secured. Otherwise anti-social and criminal behavior could be made easier, actually jeopardizing the benefits of the VC system deployment. A comprehensive set of security mechanisms is thus critical, and facilities and protocols that mitigate attacks are necessary.

Securing vehicular communications is a hard problem, due to the tight coupling between applications and the networking fabric, as well as additional societal, legal, and economical considerations, which raise a unique combination of operational and security requirements.

In this paper, we propose a security architecture to address this challenge. Our objective is to design a baseline architecture, which, on the one hand, provides a sufficient level of protection for users and legislators, and, on the other hand, is practical and deployable. The baseline architecture relies on well-established and understood cryptographic primitives, which are already broadly implemented and scrutinized and thus deserve to be sufficiently trusted. At the same time, our architecture allows deployed systems to be tuned or augmented, in order to meet more stringent future requirements. We describe next the objectives and then the basic elements of our architecture.

II. Architecture Objectives

The fundamental aspects that our architecture seeks to address are: (i) identity and cryptographic key management, (ii) privacy protection, (iii) secure communication, and (iv) in-car protection and tamper-resistance. The architecture will also enable detection of faulty (inconsistent) data and node actions, aspects not discussed in this paper. The focus of our efforts is on securing communications and the operation of the wireless part of the VC system. At the same time, disclosure and inference of sensitive user information must be prevented. In particular, it must be difficult for two or more communications of the same node (in particular, of a private vehicle) to be linked. However, identification should be possible when necessary, e.g., for liability attribution or illegitimate node exclusion. Our design is fully cognizant of the projected co-existence of TCP/IP and VC-specific protocol stacks in VC systems. In the sections that follow, we describe the architecture components and mechanisms.

III. Authorities

Drawing from the analogy with existing administrative processes and automotive authorities (e.g., city or state transit authorities), a large number of certification authorities (CAs) will exist. Each of them is responsible for the identity management of all vehicles registered in its *region* (national territory, district, county, etc.). Fig.1 illustrates a part of an instantiation of the CAs: an hierarchical structure within each CA and *cross-certification* among CAs. This way, the deployment of secure vehicular communications could still be handled locally to a great extent. At the same time, vehicles registered with different CAs can communicate securely

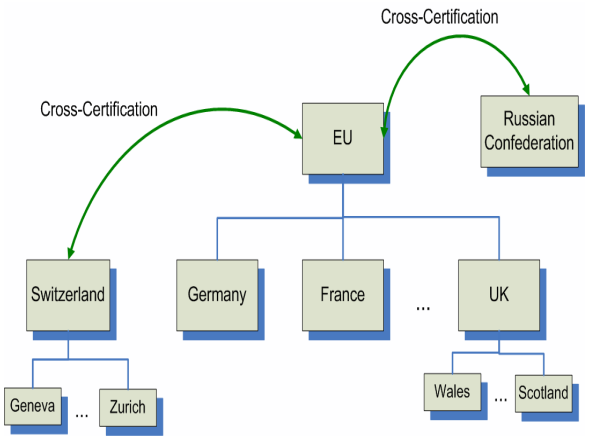

Fig. 1. Example of Hierarchical Organization and Relations of Certification Authorities.

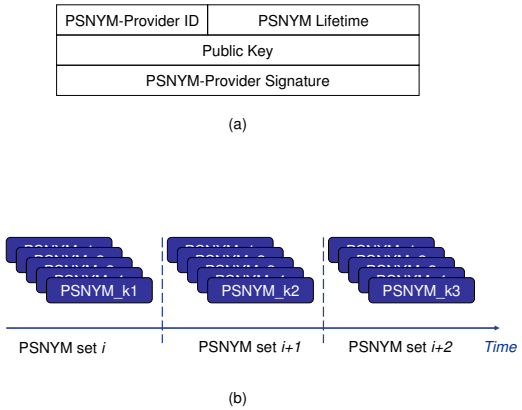

Fig. 2. Enhancing Privacy with Pseudonyms. (a) Basic pseudonym format, (b) Periodic vehicle "refill" with a new set of pseudonyms.

as soon as they validate the certificate of one CA_A on the public key of CA_B. Various procedures for easily obtaining these cross-certificates can be implemented.

Nodes of the vehicular network are registered with exactly one CA. Each node, vehicle or RSU, has a unique identity V and a pair of *private* and *public* cryptographic keys, k_V and K_V, respectively, and is equipped with a certificate $Cert_{CA}\{V, K_V, A_V, T\}$, where A_V is a list of node attributes and T the certificate lifetime. The CA issues such certificates for all nodes upon registration, and upon expiration of a previously held certificate.

We emphasize that the CA manages *long-term* identities, credentials, and cryptographic keys for vehicles. In contrast to short-lived keys and credentials, as those discussed in Sec.IV. The CA is also responsible for evicting nodes from the system, if necessary, either for administrative or technical reasons. This issue is discussed in Sec.VI. The interaction of nodes with the CA does not need to be continuous, while the road-side infrastructure or other infrastructure-based networks (e.g., cellular) could act as a gateway to the vehicular part of the network or offer an alternative method of connectivity.

IV. Privacy Enhancing Mechanisms

As a basic guideline, processes and policies for privacy protection should be defined, with minimum private information disclosure on a need-basis, and fine-grained control mechanisms for regulating private information disclosure. Nonetheless, signed messages can be trivially linked to the certificate of the signing node; thus, the removal of all information identifying the user (e.g., driver) from node certificates does make communications anonymous.

We extend this concept first introduced by [7]: we equip each private vehicle with a set of distinct certified public keys that do not provide additional identifying information, denoted as *pseudonyms*. Instead of using its long-term key pair, a node utilizes the private key corresponding to a pseudonym to sign outgoing messages, and appends the pseudonym to the messages. Messages signed under the same pseudonym (i.e., using the same corresponding private key) can be trivially linked to each other. Yet, as the vehicle changes pseudonyms, linking messages signed under different pseudonyms becomes increasingly hard over time and space.

Fig. 2.(a) illustrates a pseudonym that has a lifetime and an identifier of the corresponding *pseudonym provider* A, which is in general an entity distinct from the CA. Note that there may be multiple pseudonym providers, either as independent entities specializing in this task, or as administered by different entities (e.g., various service providers, car manufacturers, highway or city transportation authorities).

Fig. 2.(b) clues on the concept of periodic vehicle "refills" with new pseudonyms: a node utilizing pseudonyms out of the i-th set, obtains an $(i+1)$-st set of pseudonyms while it can still operate with pseudonyms in the i-th set, and switches to those in the $(i+1)$-st once no pseudonym in the i-th can be used. Recall that each pseudonym is used for a period of time which can be determined by various factors. The rate of pseudonym changes determines, along with the frequency of "refills" the size of the pseudonym set the node should obtain.

Fig.3 summarizes factors determining when a pseudonym change, and a choice of a pseudonym among possibly multiple available sets, $S_1, \ldots, S_n$, of pseudonyms, should occur. The rate at which a node switches from one pseudonym to another depends on the degree of protection the vehicle seeks, local or system-wide policies, vehicle inputs (e.g., location or velocity), the verifier of the messages issued (signed) under a specific pseudonym, and other network operation considerations (e.g., communication with an access point through the TCP/IP stack).

The change of a pseudonym should be accompanied by a change of the node identifiers used by underlying networking protocols. In particular, this can be the Medium Access Control (MAC), and other identifiers such as IP addresses. If such identifiers do not change along with the pseudonym, messages generated by a node could be trivially linked according to

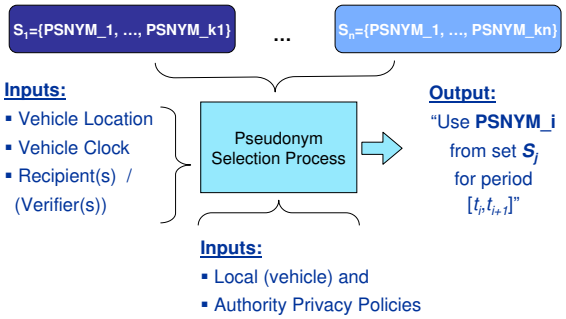

Fig. 3. Pseudonym Changing Framework.

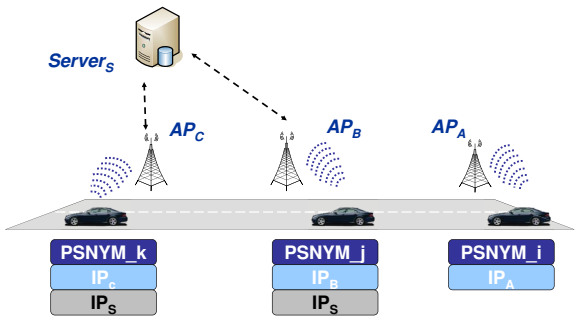

Fig. 4. Interaction of Pseudonym Changes and Network Protocol Stack Functionality.

the addresses used by the node's hardware and software. It is equally important to ensure that message transmissions from a node cannot be linked to each other due to the use of any alternative medium (e.g., cellular telephony) transceiver whose identifier remains fixed.

On the other hand, the network operation may require that node identifiers remain unchanged for a specific period of time. This implies that a change of pseudonym would be ineffective and thus meaningless throughout the period a protocol identifier must remain unchanged. Two such situations are shown in Fig.4. First, consider a vehicle within range of an access point AP_A, utilizing a pseudonym $PNYM_i$, and an IP address IP_A dynamically assigned by AP_A; the vehicle IP address must not be changed throughout, for example, a data download session. Similarly, while in range of an AP_B, the vehicle utilizes $PNYM_j$ and is assigned an IP_B, and establishes a session with a node S at the wire-line part of the network. If it is necessary for the vehicle to maintain the same identifier (e.g., an IP address IP_S) throughout such a communication with S, it could be tracked by an eavesdropper of the wireless medium transmissions, especially if IP_S is used as the vehicle reconnects to S through another AP_C. To remedy this, end-to-end traffic and identification (IP_S) should be encrypted. Then, only the newly assigned IP_C is visible over the wireless medium, as were IP_A, IP_B while in range of AP_A, AP_B. However, such addresses are at most locators, merely indicating that $PNYM_i, PNYM_j$ and $PNYM_k$ respectively are within range of the corresponding access points.

V. Trusted Components

Implementing security for vehicular communications requires the vehicles to be equipped with a *Trusted Component (TC)*. Many vehicles are already equipped with components, such as speed limiters, tachographs, and event data recorders (*EDRs*), considered critical by manufacturers and legislators. We assume that nodes are equipped with a Trusted Component, i.e., tamper-resistant hardware and firmware.

The main role of the TC is to store sensitive cryptographic material (e.g., private keys) and to perform cryptographic operations using that material. For this reason, the TC must have a processing unit, a memory module, and some non-volatile storage. In addition, in order to ensure the freshness of the cryptographically protected messages produced by the TC, it must also have a real-time clock, and consequently, a battery module that ensures the independent operation of this clock.

Note that having a trusted clock is indispensable, as otherwise the TC could be coerced to produce cryptographically protected beacon messages *in the future* that can later be used to mislead other vehicles. For instance, someone that has unsupervised access to the vehicle (e.g., a mechanic in a garage) could feed the TC with a clock value t in the future, and with appropriately chosen, fake position and speed information, $\vec{p}$ and $\vec{v}$, respectively. The TC would then produce a signed beacon message containing the fake timing, position, and speed information, which could be recorded and broadcast later at time t and at position $\vec{p}$, without the TC being present.

Note also that one could include the positioning system and the other sensors of the vehicle within the TC, but in our opinion, this is not indispensable as long as the TC is equipped with its own trusted clock. The TC could still be fed with incorrect position information and sensorial data, but now the attacker must do this *in real-time*, which is considerably more difficult. In particular, not having unsupervised access to the vehicle constantly, the attacker must install some rogue equipment inside the vehicle that feeds the TC with corrupted position information and other fake sensorial data. In-vehicle intrusion detection mechanisms could be used to mitigate this problem.

We require the TC to be physically protected against tampering; indeed, this property of the TC is where trust in it is derived from. The physical protection of the TC should ensure at least tamper evidence. However, this may not be enough, as regular inspection of the vehicles is rather infrequent (e.g.,

in some countries it happens in every second year), which results in a large vulnerability window. Therefore, it is desired that the physical protection of the TC also ensures some level of tamper resistance. We understand that high-end tamper resistant hardware modules are very expensive, therefore, in order for our baseline architecture to be practically feasible, we require only a minimal level of tamper resistance that can be achieved with special packaging and coatings.

Finally, we note that tamper resistant devices can be compromised by exploiting weaknesses in their API [5], a software layer that provides access to the functions of the device for applications running outside of the device (in our case, on the on-board computer of the vehicle). Therefore, the API of the TC must be carefully designed so that it does not contain exploitable weaknesses. The provision of guidelines for this is on our future research agenda.

VI. Pseudonymity and Credential Revocation

Pseudonyms are bound to the vehicles' long-term identities, with a *pseudonymity resolution* authority *PRA* being able to infer this mapping if necessary, for example, for liability attribution. Messages signed by the same vehicle using different pseudonyms can be linked by PRA. In the simplest system configuration, the CA is the pseudonym provider and the pseudonymity resolution authority. Then, it suffices for the CA to maintain a map of pseudonyms to the long-term identity of the vehicle. In general, different solutions with differing properties are possible; for example, the pseudonym to long-term identity mapping could be maintained by the pseudonym provider itself, or the pseudonym provider could maintain evidence of the mapping that only PRA can utilize to resolve the pseudonym.

Beyond pseudonym resolution, a node that is deemed illegitimate (e.g., its registration expired) or malfunctioning can be removed from the network. This is possible by revoking the pseudonyms and the long-term credentials of the node. If the long-term credentials of a node are revoked, the node is evicted but it is not automatically prevented from participating in the VC system operation. This is so because the pseudonyms that the node is equipped with, rather than the long-term credentials, are utilized for communication.

However, long-term credentials are used by vehicles to obtain new sets of pseudonyms: nodes use them to establish with the pseudonym provider that they are legitimate members of the system, i.e., registered with a CA. This implies that one option is to notify directly the pseudonym providers regarding revoked nodes. This way, no communication overhead over the wireless medium is necessary.

Yet, the need to revoke not-already-expired pseudonyms previously provided to a revoked node remains. If pseudonyms are not issued by the CA, coordination of the CA and the pseudonym provider is necessary. Furthermore, we identify a trade-off: the more frequent the pseudonym "refills" are, the easier the revocation (fewer pseudonyms to revoke), at the expense of higher cost and inferior usability due to frequent executions of the "refill" protocol. For example, one can imagine a situation when the vehicle fails to obtain new pseudonyms, after having utilized all available valid ones, if the pseudonym provider is unreachable.

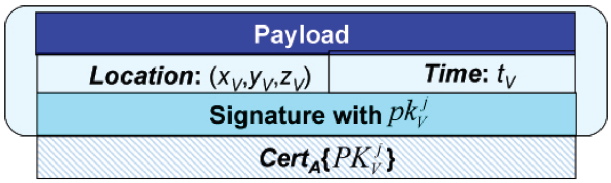

Fig. 5. Secure Communication: Basic Message Format.

We provide multiple revocation options tailored to the scale of VC systems. First, a Revocation of the Trusted Component (RTC) protocol, with the CA instructing directly the TC to erase all cryptographic material and acknowledge the cease of operation, and in case RTC does not conclude successfully. Second, revocation through the distribution of compressed certificate revocation lists, namely, the RCCRL protocol, which utilizes RSUs or low-speed broadcast media to distribute the revocation information. The infrastructure acts as a gateway for dissemination of revocation information and the execution of the revocation protocols. The three methods are discussed in [29]. An alternative third approach could be to require that vehicles regularly acquire proofs that their credentials remain valid. Instead of requiring them to download revocation information, vehicles download *verifiers* from the CA or the pseudonym provider. These verifiers are then included when the certificate is presented to other nodes [24], [18].

VII. Secure Communication

The basic tool to secure communications is digital signatures, and can be used for all messages. Fig. 5 illustrates a typical message format, with a signature calculated by a node V using the private key pk_V^j corresponding to the j-th pseudonym PK_V^j of V, that is, public key PK_V^j. $Cert_A\{PK_V^j\}$ denotes PK_V^j and the signature of the pseudonym provider A (as illustrated in Fig.2.(a).). For simplicity, we omit notation on the pseudonym set. The messages also have a time-stamp, the sender's clock value, and a geo-stamp, the sender's coordinates, at the sending time.

This mechanism can be applied to different types of messages, which fall roughly in the following three main categories, as expected in VC systems:

Beaconing: Frequently broadcasted messages at the data link layer; the beacons include information on the sender, such as sensor information or warnings.

Restricted Flooding: Messages, for example disseminating warnings, throughout a targeted area, are relayed by nodes. Their propagation is restricted by the use of traditional time-to-live fields, and/or by use of geographic distance constraints ("geo-casting").

Position-Based Routing: Data are unicasted from a sender to a specific destination across multiple wireless hops: the coordinates of the destination are given in the data packet,

and relaying nodes forward the packet to their neighbor with the minimum remaining distance to the destination.

For beaconing, a single signature suffices. For multihop propagation, depending on the type of message, the originator appends its signature, while hop-by-hop signatures can also be added and removed. The latter option, with the combination of signatures, is also meaningful for securing Position-Based Routing [13].

A. Other Considerations

We assume that confidentiality is needed only for unicast message transport, for example, using a symmetric session key transported by the sender to the receiver via public key cryptography. Entity authentication is rather straightforward to achieve in our context. Prevention of denial of service attacks against lower layers (e.g., jamming) or by injection of faulty data, especially if aggregation is performed, are also relevant. Yet, to mitigate them, specialized mechanisms, e.g., detection of faulty nodes, other than the above-discussed ones are necessary.

VIII. System Performance Validation

Security mechanisms add overhead to the systems they safeguard. Among other affected system properties, real-time performance is usually degraded due to several factors. Vehicular communications are not an exception, with security on performance affected by security overhead. In the context of our architecture, security costs are due to the following parameters: (i) costly public key cryptography, (ii) frequent periodic broadcasts, and (iii) large network scale. Building on the above observations, it is crucial to consider the real-time performance properties of any security mechanism developed for vehicular communications. Hence, validation of security protocols must include their real-time performance footprint in a vehicular communications scenario. In this section we discuss two approaches to achieve this, namely *worst-case analysis* and *realistic simulation* of typical scenarios.

A. Worst-case analysis

The application of worst-case analysis on an early version of a protocol provides an estimate on its suitability for vehicular communications. If its performance footprint does not exceed a worst-case upper bounds, a candidate security protocol can be further evaluated and compared to alternative protocols. This stage involves realistic simulation in several typical scenarios as discussed earlier. As an example, we applied the above approaches to evaluate the suitability of digital signatures for use in vehicular communications [28], first using worst-case analysis then simulation in both fluid and congested highway scenarios, and identified that among three different public key cryptosystems Elliptic Curve Cryptography (ECC) is more suitable for secure vehicular communications.

As is often the case in other networking paradigms, scenarios and deployment settings for vehicular communications vary considerably as well. For example, the number of lanes, the time of the day and the road section all affect the number of vehicles that can broadcast safety messages within mutual communication range. Hence, it is hard to come up with precise evaluations of the security costs. This is why one could opt for worst-case back-of-the-envelope analysis: roughly estimating the highest number of security-related messages a vehicle has to process at any given moment. Such an estimation yields an upper bound on the allowable security cost. Which, in turn, is used to evaluate the appropriateness of different security mechanisms for vehicular communications. The advantage of this approach is that it accounts for most possible scenarios. On the downside, it is approximate, thus a more detailed evaluation method is needed.

B. Realistic simulation

Given the large scale of vehicular networks and the diversity of possible scenarios, realistic simulation of vehicular communications can yield the desired performance figures for specific protocols. In contrast to the worst-case analysis, simulation should consider specific scenarios to compare security protocols. This is notably motivated by the fact that network topology and mobility seriously affect the performance of different protocols. Hence, some protocols perform better in static scenarios (e.g., congestion) and others are more suitable in highly mobile scenarios (e.g., fluid highways). An early example beyond the VANET context related to this distinction with respect to security costs can be found in [14].

Realistic simulation of security protocols is more tedious than worst-case analysis, but gives a fine-grained performance evaluation. Several tools for VANET simulations have been recently developed. Some of them are not publicly available [23], some are not yet fully developped [8], [30], others do not use realistic mobility models [31], whereas none of those efforts implements security mechanisms. To fill these gaps, we are currently developing *TraNS (Traffic and Network Simulation Environment)* [17], a simulation environment that integrates both traffic and network simulators. The incorporation of the traffic simulator allows defining a network topology based on real road networks and road-side infrastructure, e.g. traffic lights. It allows to generate realistic mobile traces used by the network simulator. The latter simulates wireless communication among vehicles and implements the logic of applications running on top of VANETs. Current implementation uses SUMO (traffic simulator) [15] and ns2 (network simulator) [16]. In addition, we are working on the integration of several security mechanisms into TraNS.

IX. Related Work

Recent works outline challenges for securing vehicular communications [33], [27], [25]. Attacks specific to VC systems are described in [4], [2], [10] and attacker models are analyzed in [26]. Security and privacy requirements are outlined in [28], [1], [19], [25]. Principles for designing security and privacy-enhancing mechanisms for VC systems are proposed in [26]. Frameworks and architectures for vehicular security were proposed in [29], [21], [32], [11], [3].

A range of security mechanisms not cited above have been proposed proposed. For example, [12] detects malicious data and [21] validates position data; communication security proposals in [29], [20], [13]; privacy enhancing mechanisms [28], [22], [9]; the effectiveness of changing pseudonyms to provide location privacy in vehicular networks is analyzed in [6].

The Berkeley PATH project in the USA and the German project Fleetnet. did not considered security aspects. The IEEE P1609.2 standard [1] is part of the DSRC standards for VC supported by the US Vehicle Safety Communication Consortium (VSCC). The project "NoW - Network on Wheels" is a follow-up to the Fleetnet project and is based on wireless multi-hop communication. The working group "Adhoc Data Security" focuses on security issues. Security is also among the topics addressed by the Car2Car Communication Consortium (C2C-CC), a non-profit organization initiated by European vehicle manufacturers (Audi, BMW, DaimlerChrysler, Fiat, Renault, Volkswagen).

X. Conclusions

We present the basic ideas of a security architecture for vehicular communication systems, with the focus on communication. The basic objectives of the proposed architecture, in the context of the Sevecom project, are: identity and cryptographic key management, privacy protection, secure communication, and in-car protection and tamper-resistance. At the same time, identification of nodes, which are otherwise protected by privacy-enhancing mechanisms, is possible when necessary, e.g., for liability attribution. Our design approach seeks to produce a "baseline" architecture and solution. On the one hand, our baseline architecture combines well-accepted building blocks (e.g., cryptographic primitives) and concepts (e.g., anonymized certificates/pseudonyms) adopted. The use of well-established security mechanisms facilitates deployment. On the other hand, our baseline architecture is adaptable, so that mechanisms or other changes aiming at higher protection levels can be introduced transparently in the future.

References

[1] IEEE P1609.2 - Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages. *In development*, 2006.

[2] A. Aijaz, B. Bochow, F. Dtzer, A. Festag, M. Gerlach, R. Kroh and T. Leinmuller, "Attacks on Inter-Vehicle Communication Systems - An Analysis" *in Proceedings of the 3rd International Workshop on Intelligent Transportation (WIT 2006)*, March 2006

[3] F. Armknecht, A. Festag, D. Westhoff, and K. Zeng, "Cross-Layer Privacy Enhancement and Non-Repudiation in Vehicular Communication," *4th Workshop on Mobile Ad-Hoc Networks (WMAN)*, March 2007

[4] M. Blum and A. Eskandarian, "The Threat of Intelligent Collisions," *IT Professional,* January 2004

[5] M. Bond and R. Anderson, "API level attacks on embedded systems," IEEE Computer Magazine, Oct. 2001

[6] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," In *Proceedings of the Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks* (ESAS 2007), Springer LNCS 4572, Cambridge, 2007

[7] D. Chaum "Security without identification: Transactions to make big brother obsolete," Communications of the ACM, 1985

[8] D. Choffnes and F. Bustamante, "An Integrated Mobility and Traffic Model for Vehicular Wireless networks," *In Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks (VANET'05)*, 2005

[9] E. Fonseca, A. Festag, R. Baldessari and R. Aguiar, "Support of Anonymity in VANETs - Putting Pseudonymity into Practice," *IEEE Wireless Communications and Networking Conference (WCNC)*, March 2007

[10] M. Gerlach, "VaneSe - An approach to VANET security," *in Proceedings of the V2VCOM*, 2005

[11] M. Gerlach, A. Festag, T. Leinmller, G. Goldacker, and C. Harsch, "Security Architecture for Vehicular Communication," *5th International Workshop on Intelligent Transportation (WIT)*, March 2007

[12] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," *in Proceedings of the 2004 Workshop on Vehicular Ad hoc Networks (VANET)*, 2004

[13] C. Harsch, A. Festag, and P. Papadimitratos, "Secure Position-Based Routing for VANETs," *in Proceedings of the IEEE 66th Vehicular Technology Conference VTC2007-Fall, Baltimore, Oct. 2007* (to appear)

[14] R. Hauser, T. Przygienda and G. Tsudik, "Reducing The Cost Of Security In Link-State Routing," *In Proceedings of the Symposium on Network and Distributed System Security*, 1997

[15] http://sumo.sourceforge.net/

[16] http://www.isi.edu/nsnam/ns/

[17] http://wiki.epfl.ch/trans

[18] F. Kargl, S.Schlott and M. Weber, "Identification in Ad hoc Networks," *Hawaiian International Conference on System Sciences (HICSS 39)*, January 2006

[19] F. Kargl, Z. Ma, E. Schoch, "Security Engineering for VANETs," *4th Workshop on Embedded Security in Cars (escar 2006)*, November 2006

[20] K. Laberteaux and Y.-C. Hu, "Strong VANET Security on a Budget," In *Workshop on Embedded Security in Cars (ESCAR)*, 2006

[21] T. Leinmller, E. Schoch, and F. Kargl "Position Verification Approaches for Vehicular Ad Hoc Networks," *IEEE Wireless Comm. Magazine*, October 2006

[22] M. Li, R. Poovendran, K. Sampigethaya, and L. Huang, "CARAVAN: Providing Location Privacy for VANET," *in Proceedings of the Embedded Security in Cars (ESCAR) Workshop*, Cologne, Germany, November 2005

[23] C. Lochert, A. Barthels, A. Cervantes, M. Mauve and M. Caliskan "Multiple simulator interlinking environment for IVC," *In Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks (VANET'05), Poster session*, 2005

[24] S. Micali, "Efficient certificate revocation," MIT Laboratory for Computer Science, Tech. Rep. TM-542b, Mar. 1996

[25] P. Papadimitratos, A. Kung, J-P. Hubaux, and F. Kargl, "Privacy and Identity Management for Vehicular Communication Systems: a Position Paper," *Workshop on Standards for Privacy in User-Centric Identity Management*, Zurich, Switzerland, July 2006

[26] P. Papadimitratos, V. Gligor, and J.-P. Hubaux. "Securing vehicular communications - assumptions, requirements, and principles," In *in Proceedings of the Workshop on Embedded Security in Cars (ESCAR)*.

[27] B. Parno and A. Perrig. "Challenges in securing vehicular networks," In *Proceedings of HotNets-IV*, 2005.

[28] M. Raya and J-P. Hubaux, "The security of vehicular ad hoc networks," *in Proceedings of the Workshop on Security in Ad hoc and Sensor Networks (SASN)*, 2005

[29] M. Raya, P. Papadimitratos, and J-P. Hubaux, "Securing Vehicular Networks," *IEEE Wireless Communications*, Volume 13, Issue 5, October 2006

[30] R. Mangharam, and D. Weller, D. Stancil, R. Rajkumar and J. Parikh, "GrooveSim: a topography-accurate simulator for geographic routing in vehicular networks," *In Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks (VANET'05)*, 2005

[31] A. Saha and D. Johnson, "Modeling mobility for vehicular ad-hoc networks," *In Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks (VANET'04), Poster session*, 2004

[32] C. Tchepnda, H. Moustafa, H. Labiod and G. Bourdon "Securing Vehicular Communications: An Architectural Solution Providing a Trust Infrastructure, Authentication, Access Control and Secure Data Transfer," *In Proceedings of the 1st IEEE Workshop on Automotive Networking and Applications (AutoNet'06)*, 2006

[33] M. El Zarki, S. Mehrotra, G. Tsudik, and N, Venkatasubramanian, "Security Issues in a Future Vehicular Network," *in Proceedings of European Wireless*, 2002