# Requirements and Objectives for Secure Traffic Information Systems

Falko Dressler, Christoph Sommer
Dept. of Computer Science 7,
University of Erlangen, Germany
{dressler, christoph.sommer}@cs.fau.de

Tobias Gansen, Lars Wischhof
Audi Electronics Venture GmbH,
Gaimersheim, Germany
{tobias.gansen, lars.wischhof}@audi.de

## Abstract

*Early approaches for Traffic Information Systems (TISs) primarily focused on centralized systems using unidirectional downlink communication and employing wireless broadcast or similar techniques. In general, these centralized TISs were operated by public radio stations, thus there were almost no security issues related to this approach. The situation changes when new Inter Vehicle Communication (IVC) techniques are investigated. The advantages of improved timeliness and accuracy of available traffic information come with a number of security concerns. This paper reviews the requirements and objectives for secure TISs. We outline possible solutions to face the security concerns and clearly depict open issues. In conclusion, we advocate more secure TISs that benefit from recent IVC technologies in a more secure and privacy protecting way.*

## 1. Introduction

Communication among cars on the road has become one of the major research domains of the mobile networking community. This domain covers "Car-to-Car", i.e. scenarios of direct inter-vehicle communication, "Car-to-Infrastructure", i.e. the intelligent information exchange between the car and Roadside Units (RSUs) or the private car port, and any further "Car-to-X" communications. In literature, all these efforts are summarized as Inter Vehicle Communication (IVC) [2, 16]. A subset of such communication techniques are investigated in the Vehicular Ad Hoc Network (VANET) community [11]. IVC functions can be classified into the following categories [22]:

- Road traffic information: distribution of current road and traffic status (including emergencies and congestion) to vehicles that are still far away from the specific road under observation.
- Communication-based control along the road: exploitation of IVC capabilities to look ahead on the street for possible emergencies or congestion without centralized Traffic Information System (TIS) systems.
- Cooperative assistance systems: coordination of cars in critical situations such as crossings without signals or highway exits.

In this paper, we concentrate on a subset of the IVC functions, which are Traffic Information Systems. These systems rely on general information exchange for more effective and accurate dynamic route planning. An important issue for TISs is the security of the information exchange. Recently, a number of efficient TIS variants have been described in the literature. Unfortunately, the security aspects are still underestimated. A first study in 2002 outlined that almost no confidentiality issues need to be addressed in the context of IVC [27]. Similarly, privacy issues have been neglected. However, a later study clearly stated privacy concerns for localization of cars [14]. Furthermore, first attack models have been analyzed [20]. In the VANET community, the main focus is on secure routing [2, 21], for which solutions have been proposed in the last years [1, 13]. In addition, a number of challenges are being discussed in the domain of lightweight authentication [12, 19].

More recently, the demand for IVC based TISs has increased. This trend was supported by the development of fully distributed self-organizing TIS applications [24]. First field tests are about to be started[1]. It has become clear that security must be inherently included in such applications for two reasons. The commercial exploitation will not be feasible if information cannot be kept confidential and public acceptance can hardly be achieved without privacy protecting solutions [12, 23].

This paper contributes to this domain in two dimensions. First, a general review of security objectives in the field of Traffic Information Systems is provided that builds the basis for further security analyzes of particular systems. Secondly, we summarize possible security solutions and their inherent problems for providing the main security measures for IVC based TISs.

[1] SIM-TD http://www.cvisproject.org/en/links/sim-td.htm

978-1-4244-2575-4/08/$20.00 ©2008 IEEE

# 2. Traffic Information Systems

The primary objective of Traffic Information Systems is to provide traffic relevant information to the driver of a vehicle in various situations. Complementing the information available from pre-installed systems (e.g. the navigation system including maps, and local sensors such as GPS, current speed and others) communication systems are used to acquire additional data from remote systems. The TIS is responsible for processing all available data in order to extract relevant information. Basically, two application classes can be distinguished [24]:

*Comfort applications* – This type of application improves the passenger comfort and traffic efficiency and/or optimizes the route to the destination. This includes traffic information, weather, road conditions, and others.

*Safety applications* – Applications of this category improve the safety of passengers. This goal is achieved by exchanging emergency warnings or providing intersection coordination and collision avoidance.

Independent of the particular architecture of the TIS, a number of features in terms of installed systems in a car are usually assumed. This includes the availability of GPS localization and a local navigation system including up-to-date maps. The GPS also provides synchronized clocks. Current navigation systems have sufficient processing and storage capacities. The main difference between the different TIS approaches lies in the way in which information dissemination is achieved. In the following, we quickly outline the major classes of traffic information systems and the used communication approaches.

## 2.1. Centralized TIS

Conventional TIS are organized in a centralistic way as illustrated in Figure 1: Sensor-based traffic monitoring systems deployed directly at the roadside collect information about current traffic conditions. This data is transferred to a central Traffic Information Center (TIC), where the current road situation is analyzed. The result of this situation analysis is packed into messages for the Traffic Messaging Channel (TMC), forwarded to the FM radio broadcast station and transmitted via Radio Data System (RDS) to the driver. Alternatively, the traffic messages can be transferred on demand via cellular mobile phone network, e.g. GPRS.

Characteristic of a centralized TIS is that the traffic information is processed in one or more dedicated (centralized) traffic processing entities, e.g. a TIC as shown in Figure 1 or an Internet database server.

There are a number of limitations of the centralized solution as depicted in [24]. Basically, the argumentation is that the pre-installed road sensors are expensive and only available on major roads such as highways. Additionally, there is a non-negligible delay from obtaining the sensor measurements until the pre-processed data is delivered to the cars. Furthermore, the resolution of traffic information is limited by the capacity of the central processing systems and the bandwidth of the wireless link to the vehicle. Due to the high delay, emergency applications such as collision avoidance are not possible with the centralized approach. Last but not least, centralized services require an operator – in case of a private operator, this often results in a service charge for the end user.

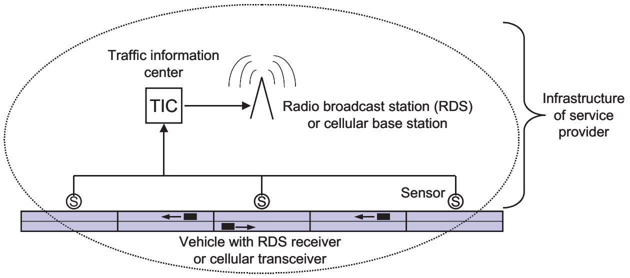
Traffic information center
TIC
Radio broadcast station (RDS) or cellular base station
Infrastructure of service provider
Sensor
S
S
S
Vehicle with RDS receiver or cellular transceiver

**Figure 1. Centralized TIS**

## 2.2. Floating Car Data (FCD)

To overcome the limitations of pre-installed infrastructure components, systems using moving vehicles (called “floating cars”) as traffic sensors have been created. In these systems, cars send their traffic observations using a cellular mobile phone network to a TIC where they are integrated with other data. TISs over 3rd Generation Mobile Networks are being actively investigated in the Cooperative Cars (CoCar) project [7]. Here, cars equipped with e.g. a UMTS radio act as floating cars and distribute information via a multi-tier aggregation hierarchy. Cellular base stations act as near-field reflectors of information and warning messages, passing on to the TIC only aggregated data. The TIC disseminates traffic information in the form of TPEG messages, both directly via the mobile network and via uplinks to traditional TICs broadcasting RDS and voice bulletins. Depending on the method of information distribution, this approach improves accuracy both in time and position.

## 2.3. Distributed or self-organizing TIS

An alternative and completely different approach for monitoring the traffic situation and distributing the traffic messages to vehicle drivers has been proposed in various VANET based research projects, e.g. FleetNet [10]. A decentralized self-organizing traffic information system is established by combining a digital map, a positioning system (e.g. GPS) and wireless ad hoc communication among the vehicles. Since the first two components are already avail-

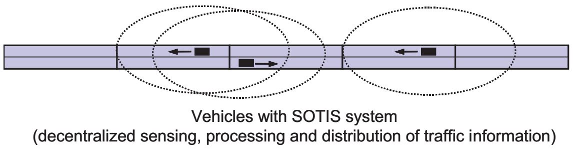
Vehicles with SOTIS system
(decentralized sensing, processing and distribution of traffic information)

**Figure 2. Decentralized self-organizing TIS**

able in modern vehicles equipped with navigation systems, the only additional requirement is a wireless interface for IVC. In this decentralized Self-Organizing Traffic Information System (SOTIS) [25], vehicles inform each other of the local traffic situation by IVC as illustrated in Figure 2. The traffic situation analysis is performed locally in each car. No communication/sensor infrastructure is required. For a global route optimization, the SOTIS information for the local area (e.g. for a radius 50–100 km) can additionally be combined with traffic information provided by roadside access points or conventional centralized systems.

For SOTIS as investigated in [24], the objective is to acquire state information for all road segments within the local area. The state of a road segment is described by an average velocity value and a flag indicating if an emergency occurred. Additionally, a time stamp is included that specifies when this information was measured. The information on the traffic state can, e.g., be used in the navigation system of the vehicle to calculate a dynamic route update and inform the driver of hazardous situations ahead. By applying a segment-based store-and-forward communication, state information is available even if only a low number of vehicles are equipped with IVC.

### 2.4. Communication and Information Dissemination

The approaches used for information dissemination in centralized and self-organizing traffic information systems can be classified in push oriented and in pull oriented techniques. For centralized TIS, the RDS TMC is a commonly used push oriented approach: traffic information is broadcasted as part of the FM radio channel to the vehicles. Since the available data rate is low, locations are transmitted in form of *location codes* which identify a specific location in the road network. However, centralized systems can also apply pull oriented communication. A typical example is a vehicle navigation system which requests traffic information via a cellular communication system such as GPRS/UMTS from a centralized server.

Self-organizing traffic information systems are based on a direct communication between individual vehicles in a local area. This is achieved by local wireless communication – typically by Wireless LAN (WLAN) using the IEEE 802.11 *ad hoc* mode or via the automotive WLAN variant IEEE 802.11p. Due to the limited transmission range (typically 50–1000 m) of these standards, pull oriented communication over large distances is only feasible if a larger ratio of all vehicles is equipped with the communication system. Therefore, a store-and-forward based push communication is often preferred, such as Segment-Oriented Data Abstraction and Dissemination (SODAD) [24]. In this case, vehicles continuously record the traffic information for the current location and periodically transmit the available data via broadcast to all other vehicles in communication range. Additionally, the information is transported on board the vehicle which allows closing gaps in the network where no communication is feasible. It has been shown that this technique allows covering an area exceeding the individual transmission range by far, even if only 1–2 % of all vehicles are equipped with the system [24].

## 3. Security Challenges

The primary objective of this paper is to analyze the security challenges and to review possible solutions for the different TIS variants. In the following, we outline some prerequisites and perform a security analysis. Based on this analysis, specific challenges and solutions are discussed.

### 3.1. Prerequisites

Figure 3 shows the relevant communication and trust relations of the typical players and components in a TIS. Depending on the particular source of traffic information, the quality and trustworthiness can be severely impaired. We define a "closed system" as a closed user group that is well-controlled either by a single authority or in a loosely-coupled way. In such a closed system, the authenticity of individual messages is much easier to be verified compared to an "open system", which represents an uncontrolled group of entities that have free access to the system. From a single system's point of view, it might be essential to identify the origin of the information or just to trust the whole system. Similarly, the location and time of measured data is of high importance. GPS provides exact data; however, it must be ensured that this data is not falsified within the car *before* transmitting the information to a TIC or to neighboring cars. Obviously, all communication channels have to be analyzed for possible security flaws. In this sense, dedicated procedures are necessary if third party traffic information should be included into the system. Examples are information about free parking lots or active traffic signs that (dynamically) broadcast their current status. Traffic signs will be usually managed by trusted government agencies whereas parking lots are provided by companies with a possibly less secure trust relation. One critical component of the entire system is the (necessary) possibility of system

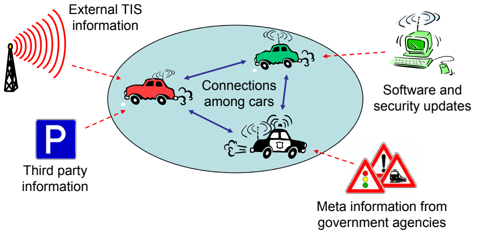
External TIS information
Connections among cars
Software and security updates
P
Third party information
Meta information from government agencies

**Figure 3. Communication and trust relations**

and security updates. Such updates have much higher security requirements as any other communication link. Therefore, the security of the global TIS essentially relies on the security of the update mechanism.

### 3.2. Security objectives

The literature on network security lists five general security objectives. Depending on the specific communication principles and the general architecture of the TIS, the relevance of each objective may vary. Table 1 summarizes the discussion of security issues in typical TIS solutions.

*Confidentiality* – depending on the status of the TIS, this may be one of the most important issues; for a closed user group, confidentiality is essential to keep the exchanged information private. This is the case if the information shall be commercially used and sold.

*Data integrity* – the integrity of messages is highly important to prevent any (intentional) falsification of traffic information. In order to prevent forged data, explicit message authentication is necessary. However, this does not address forging of data within the car by manipulating sensors.

*Accountability* – in the context of TISs, accountability can be achieved by means of message authentication. Depending on the TIS variant, accountability to a group of systems or to a single system might be demanded. Since accountability is contrary to anonymity, the principle of commensurability suggests not to put accountability on top of the objectives as long as driver generated traffic information is regarded.

*Availability* – even though this would be a major issue for any safety application, we explicitly exclude this issue as (with some efforts) the radio channel used for all the IVC channels can be disturbed (jammed).

| Security objective |
|---|
| Prevention of unauthorized usage of available TIS data |
| Protection of the privacy of participating users |
| Prevention of manipulated or falsified TIS messages |
| Protection against forged TIS messages |
| Identification of single message sources or user groups |
| Effective control for software and security updates |

**Table 1. TIS-relevant security objectives**

*Access control* – for a closed system, access control is required, which is usually performed by means of identification of a user or a group of users. The same mechanisms as used to provide confidentiality and message authentication can be employed.

### 3.3. Attacker models

Raya et al. [20] developed appropriate attacker models for VANETs and IVC. We cite these models here as they must be appropriately considered during the development of secure Traffic Information Systems.

*Insider vs. Outsider* – The insider is an authenticated member of the network that can communicate with other members. The outsider is considered by the network members as an intruder and hence is limited in the diversity of attacks he can mount (especially by misusing network-specific protocols).

*Malicious vs. Rational* – A malicious attacker seeks no personal benefits from the attack and aims to harm the functionality of the network. In contrast, a rational attacker seeks personal profit and hence is more predictable.

*Active vs. Passive* – An active attacker can generate packets or signals, whereas a passive attacker contents himself with eavesdropping on the wireless channel.

Considering privacy threats, another distinction into *global* and *local* adversaries becomes necessary. A global attacker has complete knowledge of the whereabouts of the vehicles employing IVC. This enables the tracing of vehicles regardless of any pseudonymization applied. Since IVC communication ranges are relatively short, a global attacker might technically not be feasible compared to a local attacker. The latter kind of adversary is able to install several probes within an area of interest to record messages. The combination of the distributed observations may yield knowledge of vehicle's traces [4].

Since an IVC based TIS are highly cooperative systems, they have not only to cope with *malicious* attackers, but also consider *selfish* nodes which overuse shared resources (e.g. bandwidth) or do not forward crucial information (e.g. because of privacy concerns) [5, pages 77-80].

## 4. Solution Space for Secure TIS

As discussed in the previous section, the solution space for secure TIS applications must incorporate the following objectives: confidentiality of transmitted TIS messages from a TIC to the cars as well as between cars; message authentication on the same communication channels; key management and security updates supporting frequent re-keying and providing forward and backward security. Additionally, privacy issues must be addressed that finally increase the public acceptance of the entire system.

### 4.1. Confidentiality

Confidentiality of exchanged TIS data is especially relevant if the overall TIS is managed and maintained as a "closed system". In contrast to an open system, where every node may participate equally, a closed system has to distinguish between legitimate members, i.e. paying users, and outsiders. The market introduction of IVC based TISs is still an open issue [17]. The problem is that customers of car manufacturers would have to be charged for a system which will start to function properly with growing penetration rates over the lifetime of a car. Since the success of this model seems unlikely, the car manufacturers may have to equip the first cars with such functionality free of charge. In order to not let this capital expenditure be exploited by competitors, the TIS will be maintained as a closed system. As the information that is broadcasted within the system must be accessible to authenticated nodes, encryption techniques need to be employed to enable confidential communication.

Encryption can be applied on different network layers. Depending on the selected approach, specific challenges in the key management procedures are required, i.e. frequent key updates might be necessary.

### 4.2. Message integrity and authentication

Message authentication is required for two main reasons. Messages need to be protected against forgery and falsification. Encryption or key-based message authentication provide the required authentication level. Another problem to be solved is the possible replay of messages. This can be addressed by means of synchronized clocks. All communication messages should include both sequence numbers as well as timestamps. Clock synchronization is a non-issue, for the time being, as all vehicles and fixed infrastructure components are (per our assumption) equipped with GPS receivers and GPS is also a time service.

Depending on the working behavior of the TIS, different requirements on the message integrity and authentication need to be distinguished. In particular, there are different roles of message providers and, therefore, different trust relationships:

*TIC messages* – The TIC must be considered a trusted central entity that provides accurate traffic information. Nevertheless, it must be ensured that no third party can modify or forge TIC messages. Depending on the used communication channel, i.e. whether a global broadcast scheme such as RDS or a completely self-organized distribution channel such as SOTIS / SODAD is used, the complexity of message authentication greatly varies.

*3rd party messages* – Intelligent traffic signs or dynamic Point of Interest (POI) information may be incorporated from 3rd party information providers. It may be necessary to clearly identify the source of such messages to evaluate the trust level of the messages. For example, traffic signs are managed by government agencies that should usually be trustworthy.

*Self-generated messages* – This message class refers to all TIS messages generated by individual vehicles that participate on a common TIS. Such messages may include congestion and emergency information but also generic status information. As messages are generated by individuals, the overall system must implement validation techniques to check the messages against malicious reports.

*VANET-internal messages* – Basically, all previously discussed messages may be forwarded through the VANET using ad hoc communication. Thus, messages must be clearly protected against any manipulation or forgery.

Zarki et al. [27] suggest the use of digital signatures: since each vehicle (and the roadside infrastructure) will receive many more messages than it will send, the cost of signature verification is of more importance than that of signature generation. Therefore, RSA-based digital signatures should be used. Similarly, current proposals for standardized wireless communication in vehicular networks such as IEEE 1609.2 suggest employing Elliptic Curve Digital Signature Algorithm (ECDSA) schemes. However, due to the high computational cost, lightweight broadcast authentication is being discussed as an alternative [19].

### 4.3. Key management and security updates

The following approaches for key management are described in the literature: Key pre-distribution, dynamic key generation, and key management by a trusted third party. Key management in ad hoc networks has been extensively investigated [6, 26]. Unfortunately, the developed approaches cannot simply be used in IVC based TIS approaches because bidirectional communication between the communicating parties is required – most current TIS approaches do not provide a back-channel, i.e. no possibility for dynamic key generation.

Therefore, only two candidate solutions remain for application in TISs: key pre-distribution, e.g. installed on a CD, or public-key techniques using a PKI. Both techniques can be operated in two ways: based on single key solutions, i.e. either a single key for the entire system or pre-installed keys for each participating node; and based on group keys, i.e. supporting the identification of specific user groups such as government-maintained entities.

According to [27], public key digital signatures are not particularly useful without a certification infrastructure. Designing a nimble, scalable and secure Public Key

Infrastructure (PKI) has been a major challenge in the last decade. We must take into account the unique aspects of the IVC based network environment in designing such a PKI. Finally, there are some recent and promising results in cryptography that obviate the need for public key certificates. For example, the Boneh/Franklin identity-based encryption system [3] is an elegant method of obtaining public key cryptography without any certificates: an entity's public key is derived from a unique identity string, e.g. a vehicle identification number.

Depending on the security of the selected key distribution scheme and the employed cryptographic primitives, the key management requires periodic replacement of all keys in order to cope with possibility of broken or discovered keys. Such key updates can be subsumed under general security update requirements that also focus on possible commercial issues such as contract updates. The distribution path of the security update must be clearly secured, i.e. an anonymous Internet update will not be possible.

### 4.4. Secure positioning

Traffic information is closely related to positioning, since status reports transmitted within a TIS are bound to distinct locations. Today, basically only GPS is used for positioning within cars. An attacker who is able to locally forge GPS signals can deceive on-board hardware, resulting in the transmission of falsified position data while leaving the actual message sent within the TIS untouched. One solution to this problem is to calculate relative positions to certain trusted network entities [15]. In a TIS, this could be provided by RSUs. Besides managing certificates, signing and validating messages, an additional task is to provide tamper evident crypto-hardware to consolidate received location information and to adequately set positions of traffic reports within transmitted messages.

### 4.5. Privacy issues

In conventional TISs, privacy is a non-issue, since a road operator or public authorities are responsible for collecting, aggregating and broadcasting the traffic related information. There is neither the need to hide the communication itself nor exists the requirement to hide the identity of the sender. The receivers are hidden because of the broadcast nature of the communication applied. This situation changes if more recent techniques like FCD or fully distributed TISs shall be used. Since the users of the TIS also contribute by sending traffic information, they expect a certain level of privacy. One objective is "location privacy" which means that a sender of a message cannot be localized or tracked. This is often referred to as the question about liability vs. privacy: how to avoid the Big Brother syndrome [14].

Since the very nature of a TIS is concerned with traffic events being bound to locations, one is only able to disguise the sender's identity. This can be achieved using pseudonyms, where the senders do not reveal their real identity but use a (random) pseudonym instead. To avoid tracking of a node, pseudonyms do have to change frequently over time [4]. It is obvious that changing a pseudonym at application or network layer is not enough to avert tracking. Identifiers at all communication layers have to change accordingly, including used cryptographic primitives [9].

This is what makes efficient key distribution techniques an important issue in VANET research. One approach to enable pseudonymity while preserving accountability is to equip nodes with a long term identifier. Using this long term identifier nodes can apply for a set of pseudonyms distributed by a Trusted Third Party (TTP). Then, only the supplying TTP is able to resolve the identity of a node in case of misbehavior or a legal dispute [18]. Fischer et. al. extended the model of the pseudonym supplying TTP to a secret sharing scheme among multiple TTPs [8]. Therefore, no single TTP can resolve a node's identity.

The drawback of having a central instance being able to track the users may turn out to be a opportunity, since it is relatively easy to apply organizational means of data protection in such an instance. A distributed TIS lacks such a central instance. Violation of a sender's privacy is relatively easy by eavesdropping broadcasted messages. This implies that the communication protocol applied, together with the communicating nodes, are responsible for supporting privacy.

## 5. Conclusion

We analyzed the security requirements for typical Traffic Information System (TIS) architectures. Based on this discussion, we identified a number of security issues that need further consideration in the context of IVC and VANET research. These objectives can be met by means of cryptography. Therefore, it can be concluded that the most important aspect is the key management. This can be provided for example by a certificate-based PKI. Comparing the possible security solutions that address the demands of centralized and fully distributed TIS alternatives, we see further research required for solving the following open issues:

*Key management* – For developing and deploying any effective TIS, it is necessary to securely maintain trust relationships in terms of an adequate key management. The efficiency and security of the key management is in direct conflict with the ease of use from a user's perspective. Regular key updates or even permanent connectivity might not be feasible for all TIS solutions. On the other hand, the probability of forgery increases with limited possibilities of keeping the key material up-to-date.

*Security vs. privacy* – Best security results can be achieved if all the participants of the entire TIS can be clearly identified, i.e. if all traffic information messages can be secured against forgery and falsification. Unfortunately, this solution leads to severe privacy problems as individual cars would become traceable. Typically, such traceability can only be prevented by using frequently changing pseudonyms, which, in turn, makes key management even more complicated.

## References

[1] F. Almenarez and C. Campo. SPDP: A Secure Service Discovery Protocol for Ad-Hoc Networks. In *9th Open European Summer School and IFIP Workshop on Next Generation Networks*, Budapest, Hungary, 2003.

[2] J. J. Blum, A. Eskandarian, and L. J. Hoffman. Challenges of Intervehicle Ad Hoc Networks. *IEEE Transactions on Intelligent Transportation Systems*, 5(4):347–351, December 2004.

[3] D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. *SIAM Journal of Computing*, 32(3):586–615, 2003.

[4] L. Buttyán, T. Holczer, and I. Vajda. On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs. In *4th European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS2007)*, Cambridge, UK, July 2007. Springer.

[5] L. Buttyán and J.-P. Hubaux. *Security and Cooperation in Wireless Networks*. Cambridge University Press, 2008.

[6] S. Capkun, L. Buttyán, and J.-P. Hubaux. Self-Organized Public-Key Management for Mobile Ad Hoc Networks. *IEEE Transactions on Mobile Computing*, 2(1):52–64, January 2003.

[7] Y. Chen, G. Gehlen, G. Jodlauk, C. Sommer, and C. Görg. A Flexible Application Layer Protocol for Automotive Communications in Cellular Networks. In *15th World Congress on Intelligent Transportation Systems (ITS 2008)*, New York City, NY, November 2008. to appear.

[8] L. Fischer, A. Aijaz, C. Eckert, and D. Vogt. Secure Revocable Anonymous Authenticated Inter-Vehicle Communication (SRAAC). In *4th Conference on Embedded Security in Cars (ESCAR 2006)*, Berlin, Germany, November 2006.

[9] E. Fonseca, A. Festag, R. Baldessari, and R. Aguiar. Support of Anonymity in VANETs - Putting Pseudonymity into Practice. In *IEEE Wireless Communications and Networking Conference (WCNC 2007)*, pages 3400–3405, Hong Kong, March 2007.

[10] W. Franz, H. Hartenstein, and M. Mauve, editors. *Inter-Vehicle Communications Based on Ad Hoc Networking Principles - The FleetNet Project*. Universitätsverlag Karlsruhe, June 2005.

[11] H. Hartenstein and K. P. Laberteaux. A Tutorial Survey on Vehicular Ad Hoc Networks. *IEEE Communications Magazine*, 46(6):164–171, June 2008.

[12] Y.-C. Hu and K. P. Laberteaux. Strong VANET Security on a Budget. In *4th Conference on Embedded Security in Cars (ESCAR 2006)*, Berlin, Germany, November 2006.

[13] J.-P. Hubaux, L. Buttyán, and S. Capkun. The Quest for Security in Mobile Ad Hoc Networks. In *2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing (ACM Mobihoc 2001)*, pages 146–155, Long Beach, CA, USA, October 2001. ACM.

[14] J.-P. Hubaux, S. Capkun, and J. Luo. The Security and Privacy of Smart Vehicles. *IEEE Security and Privacy*, 2(3):49–55, May 2004.

[15] L. Lazos and R. Poovendran. SeRLoc: Robust localization for wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 1(1):73–100, August 2005.

[16] J. Luo and J.-P. Hubaux. A Survey of Inter-Vehicle Communication. Technical Report IC/2004/24, School of Computer and Communication Sciences, EPFL, 2004.

[17] C. Menig, L. Wischhof, A. Ebner, T. Gansen, V. Seemann, R. Hildebrandt, and R. Braun. Increasing Mobility by Car-2-X Communication: Applications for Market Introduction. In *FISITA World Automotive Congress)*, Munich, Germany, September 2008.

[18] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya. Architecture for Secure and Private Vehicular Communications. In *7th International Conference on ITS Telecommunications (ITST 2007)*, Sophia Antiplolis, France, June 2007.

[19] A. Perrig, R. Canetti, D. Tygar, and D. Song. The TESLA Broadcast Authentication Protocol. *Cryptobytes*, 5(2):2–13, 2002.

[20] M. Raya and J.-P. Hubaux. The Security of Vehicular Ad Hoc Networks. In *3rd ACM Workshop on Security of ad hoc and Sensor Networks*, pages 11–21, Alexandria, VA, USA, November 2005.

[21] M. Raya, P. Papadimitratos, and J.-P. Hubaux. Securing Vehicular Communication. *IEEE Wireless Communication, Special Issue on Inter-Vehicular Communication*, 13(5):8–15, October 2006.

[22] D. Reichardt, M. Miglietta, L. Moretti, P. Morsink, and W. Schulz. CarTALK 2000 - Safe and Comfortable Driving Based Upon Inter-Vehicle-Communication. In *IEEE Intelligent Vehicle Symposium*, volume 2, pages 545–550, Versailles, June 2002.

[23] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran. AMOEBA: Robust Location Privacy Scheme for VANET. *IEEE Journal on Selected Areas in Communications (JSAC)*, 25(8):1569–1589, October 2007.

[24] L. Wischhof, A. Ebner, and H. Rohling. Information dissemination in self-organizing intervehicle networks. *IEEE Transactions on Intelligent Transportation Systems*, 6(1):90–101, March 2005.

[25] L. Wischhof, A. Ebner, H. Rohling, M. Lott, and R. Halfmann. SOTIS - A Self-Organizing Traffic Information System. In *57th IEEE Vehicular Technology Conference (VTC2003-Spring)*, Jeju, South Korea, April 2003.

[26] B. Wu, J. Wu, E. B. Fernandez, and S. Magliveras. Secure and Efficient Key Management in Mobile Ad Hoc Networks. In *1st International Workshop on Systems and Network Security (SNS 2005)*, April 2005.

[27] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian. Security Issues in a Future Vehicular Network. In *European Wireless 2002*, Florence, Italy, February 2002.