A Privacy Aware and Efficient Security Infrastructure for Vehicular Ad Hoc Networks

Klaus Plößl and Hannes Federrath

University of Regensburg, 93040 Regensburg, Germany

Abstract. VANETs have the potential to dramatically increase road safety by giving drivers more time to react adequately to dangerous situations. To prevent abuse of VANETs, a security infrastructure is needed that ensures security requirements like message integrity, confidentiality, and availability. After giving more details on the requirements we propose a security infrastructure that uses asymmetric as well as symmetric cryptography and tamper resistant hardware. While fulfilling the requirements, our proposal is especially designed to protect privacy of the VANET users and proves to be very efficient in terms of computational needs and bandwidth overhead.

1 Introduction

The term vehicular ad hoc network (VANET) is used for a subgroup of mobile ad hoc networks (MANETs, defined in [1]). The distinguishing property of the VANET is that it is formed mainly by vehicles. This implies that node movement is restricted by factors like road course, encompassing traffic and traffic regulations. Because of the restricted node movement it is a feasible assumption that the VANET will be supported by some fixed infrastructure that assists with some services and can provide access to stationary networks [2]. The fixed infrastructure will be deployed at critical locations like slip roads, service stations, dangerous intersections or places well-known for hazardous weather conditions.

Nodes are expected to communicate by means of North American DSRC standard [3] that employs the IEEE 802.11p standard for wireless communication. To allow communication with participants out of radio range, messages have to be forwarded by other nodes (multi-hop communication). Vehicles are not subject to the strict energy, space and computing capabilities restrictions normally adopted for MANETs [4]. More challenging is the potentially very high speed of the nodes (up to 250 km/h) and the large dimensions of the VANET.

The primary VANET's goal is to increase road safety. To achieve this, the vehicles act as sensors and exchange warnings or – more generally – telematics information (like current speed, location or ESP activity) that enables the drivers to react early to abnormal and potentially dangerous situations like accidents, traffic jams or glaze. In addition, authorized entities like police or firefighters should be able to send alarm signals and instructions e.g. to clear their way or stop other road users. Besides that, the VANET should increase comfort by means of value-added services like location based services or Internet on the road [5].

Plößl K. and Federrath H. (2007).
A Privacy Aware and Efficient Security Infrastructure for Vehicular Ad Hoc Networks.
In *Proceedings of the 5th International Workshop on Security in Information Systems*, pages 145-154
DOI: 10.5220/0002419901450154

These three application categories (“warnings and telematics information” (W), “alarm signals and instructions” (A), and “value-added services” (V)) imply different security and privacy requirements with respect to the protection goals integrity, confidentiality and availability. Nevertheless, there is a common need for a security infrastructure establishing mutual trust and enabling cryptography. The security infrastructure therefore includes all technical and organizational measures and facilities needed. After defining the requirements for any such security infrastructure (section 2) we present a new proposal (section 3) that particularly aims to protect privacy of the participants and is designed to be very efficient in terms of computing capabilities and communication bandwidth. Our system is evaluated in section 4. Section 5 outlines our conclusion and future work.

2 Security Requirements

In this section we explain the requirements for a VANET security infrastructure. If necessary, we distinguish between the three application categories W, A, and V as defined in section 1. The requirements are summarized in table 1.

2.1 Integrity

The security infrastructure has to provide mechanisms that prevent or at least detect message modification (I1). This hinders malicious nodes from modifying forwarded messages and protects message integrity for all application categories.

Alarm signals and instructions sent from authorized nodes like police cars, fire engines or ambulances have to be obeyed by the addressees. Therefore, the authenticity and integrity of the message as well as the authorization of the sender must be provable instantly without further information (I2a). In contrast, for warnings and telematics messages plausibility checks can be conducted by means of in car sensors or messages received from other VANET nodes. Hence no unchangeable and unique identity would be necessary in this case. Moreover, to hamper movement profile creation it would be preferable to cloak sender identity especially in periodically sent messages (P1). Nevertheless, ex post accountability and non-repudiation is necessary to be able to prosecute misuse of the VANET like injection of bogus information (I2b). Therefore anonymous participation should not be allowed, pseudonymous participation is desirable.

This ex post identification must only be allowed in severe cases like accidents with death results or sending bogus warnings. Automated traffic surveillance or automated prosecution – e.g. based on the sent telematics data – must not be allowed with regard to multilateral security (P2). Multilateral security means taking the interests of all parties involved into account. In this case, interests of law enforcement (to prosecute each violation of law with as few effort as possible) have to be balanced with interests of citizens (not to be monitored regardless of whether a suspicion exists). It is an interesting question how to define what such severe cases of VANET abuse are. Nevertheless, it will not be answered here because we focus on the technical details of the security infrastructure. We assume that in-car sensor data is correct. Additionally, we expect integration of

Table 1. Requirements.

I1	Data integrity
I2a	Immediate sender authentication
I2b	Ex post accountability
C1	Different levels of confidentiality
C2	Protection of the security infrastructure
P1	Protection against profile generation
P2	Protection against surveillance
A1	Computational and bandwidth efficiency

correct time and position information in all messages to protect against replay and position spoofing attacks. This information is available from an infrastructure like Galileo [6].

2.2 Confidentiality

Confidentiality requirements vary heavily between the three application categories. While confidentiality of alarm signals is negligible in most cases, it can e.g. be crucial for services subject to costs. The security infrastructure therefore has to provide mechanisms that support different levels of confidentiality (C1). For example these levels could be no confidentiality, confidentiality against outsiders and confidentiality against all except direct communication partners.

Besides application data administrative messages like routing protocol information or messages containing cryptographic material have to be protected against eavesdropping. Also, the cryptographic information held by participants or centralized instances has to be protected against unauthorized access. More generally, the security infrastructure has to be protected against attacks (C2).

2.3 Availability

Because most VANET messages are related to driving conditions and road safety, real-time processing of these messages is crucial. To be able to fulfill the above integrity and confidentiality requirements VANET nodes have to carry out additional cryptographic operations that extend message processing. Mechanisms to protect message integrity increase the message length. To satisfy the given real-time constraints the mechanisms of the security infrastructure must be as efficient as possible in terms of computational and bandwidth needs (A1). Despite the fact that there is no feasible protection against jamming attacks [7] actions must be taken that complicate denial-of-service attacks and therefore increase availability.

3 Proposal

In this section we present our proposal for a VANET security infrastructure that is designed to be very efficient in terms of computing capabilities and communication bandwidth while fulfilling all security and privacy requirements. After a once-only initialization it employs asymmetric cryptography within a public key infrastructure (PKI) for messages influencing road safety. All other messages (especially the periodically sent telematics messages) are protected by a system employing symmetric cryptography that is much faster and protects privacy of the participants better than the asymmetric part. After outlining our proposal in section 3.1 we give some more details on the once-only initialization (3.2) and the symmetric system part (3.3). Figure 1 shows a VANET with the different message types.

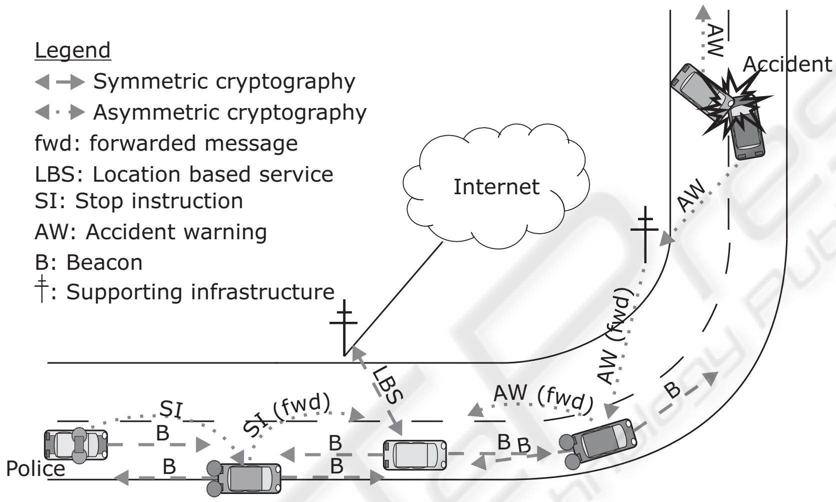

Fig. 1. VANET with different message types.

3.1 Outline and Asymmetric Part

In the asymmetric part of the VANET we employ a PKI with vehicle-related identities (VRI) in form of a private key and a corresponding certificate. The certificates are issued by a certification authority (CA) in each country that should be operated by the governmental transportation authority (GTA). We suggest a VRI issued by the GTA because of the following reasons:

- A VRI is the digital equivalent of the current situation: The license plate is a fixed pseudonym for the owner of the vehicle and only GTA can link the pseudonym with the real world identity of the owner. The driver is not known for sure but this is consistent with current legislation in most countries.
- The GTA is already known and somewhat trusted by the citizens.
- Employing GTA as CA would – at least in the EU – be cost efficient because the digital tachograph system demands that each member country has a CA issuing certificates used in the digital tachograph hardware [8]. In other words most European GTAs already operate a CA.

Each vehicle stores its VRI and at least the root certificate of the country CA in tamper resistant hardware (TRH). For warnings integrity and authenticity is ensured (req. I1, I2a/b) by adding a digital signature and the sending node's certificate (see fig. 2). The recipient can check the signature and the identity of the sender included in the certificate[1]. Because warnings are sent very seldom and only distributed to a small geographical region they can not be used to generate movement profiles. Therefore digitally signing warnings does not harm privacy of the driver in an unacceptable manner.

Data with address information	Digital Signature	$CERT_{Sender}$

Fig. 2. Message with asymmetric protection.

People with special privileges like police officers additionally get individual-related identities (IRI), in form of a private key and a corresponding certificate stored on a smart card. To be able to use their special privileges the certificate of the sending vehicle and the certificate of the driver have to be submitted to the CA. After checking the two certificates, the CA issues a certificate (and corresponding key pair) that includes attributes that grant authorization to send a defined set of alarm signals and/or instructions. This certificate is valid e.g. for eight hours (one shift) and used to add a digital signature to alarm signals and instructions. Recipients can check message integrity and authorization of the sender instantly and do not have to check revocation information due to the short validity of the certificate (req. I1, I2a).

Taking into account performance (req. A1) and privacy requirements (req. P1, P2) it is not desirable to digitally sign all messages[2] with the vehicles certificate. Therefore geographically distributed trusted third parties (GTTPs) are employed which enable pseudonymous participation in the VANET as well as message encryption and authentication within their assigned geographical regions by means of symmetric cryptography. The participation in the symmetric protected part of the VANET requires communication with a GTTP from time to time. If a VANET node is not able to contact his GTTP he has to use asymmetric cryptography and cannot decrypt or verify messages protected with symmetric cryptography. We want to point out that any VANET participant is able to participate in the asymmetric part of the VANET after the once-only initialization. This means he can understand and send safety critical VANET messages even if he is never able to communicate with a GTTP. We give more details on the symmetric part after explaining the once-only initialization phase.

[1] If the sending vehicle's certificate was issued by another country CA, cross-certificates are needed.

[2] Especially the periodically sent telematics information including current position and speed could easily be abused to create movement profiles. In addition, these so-called beacons are sent very often (approximately every 10 to 300 ms [9, 2]) what results in a lot of computational and bandwidth overhead.

3.2 Initialization

At production time each vehicle is equipped with TRH that cannot be removed without being destroyed. Then the car manufacturer installs the root certificate ($CERT_{Root}$) of the GTA the vehicle is sold to – e.g. $CERT_{Root_{DE}}$ for Germany – and a symmetric key. The symmetric key is also saved on a smart card. This pre-shared key is used to encrypt communication between TRH and the smart card (req. C2).

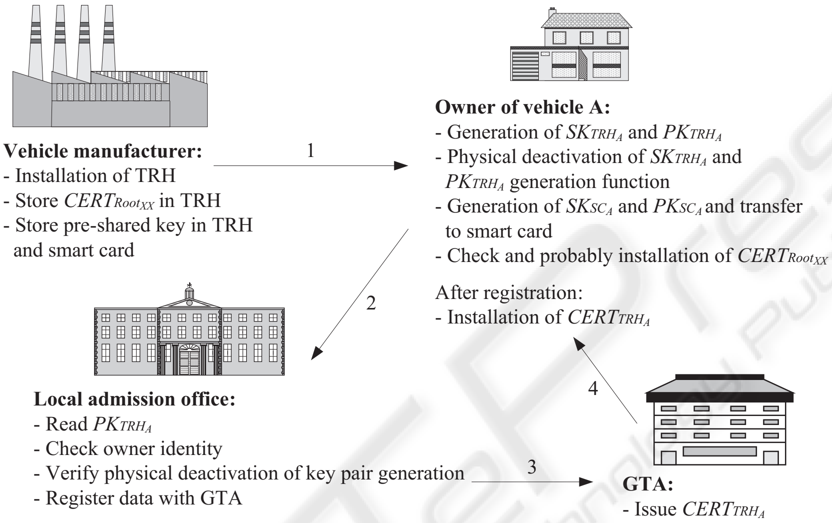
Vehicle manufacturer:
- Installation of TRH
- Store $CERT_{Root_{XX}}$ in TRH
- Store pre-shared key in TRH and smart card
1
Owner of vehicle A:
- Generation of SK_{TRH_A} and PK_{TRH_A}
- Physical deactivation of SK_{TRH_A} and PK_{TRH_A} generation function
- Generation of SK_{SC_A} and PK_{SC_A} and transfer to smart card
- Check and probably installation of $CERT_{Root_{XX}}$
After registration:
- Installation of $CERT_{TRH_A}$
2
Local admission office:
- Read PK_{TRH_A}
- Check owner identity
- Verify physical deactivation of key pair generation
- Register data with GTA
3
4
GTA:
- Issue $CERT_{TRH_A}$

Fig. 3. Once-only initialization process.

After receiving his new vehicle (and the smart card) the customer connects the smart card to the TRH and starts the initialization process. TRH checks connection to the smart card and generates two asymmetric key pairs. One is used as VRI and is saved in TRH (e.g. PK_{TRH_A} and SK_{TRH_A} for vehicle A). TRH ensures that only one key pair can be saved and the secret key (SK_{TRH_A}) never leaves TRH (req. C2). The second key pair is digitally signed with the first one and saved on the smart card. This key pair (PK_{SC_A} and SK_{SC_A}) is used to authenticate the owner. Configuration changes like saving new or deleting old root certificates in TRH are allowed only after authentication with the smart card. This ensures that only the owner is authorized to change the TRH configuration. If the vehicle is sold the new owner can generate a new key pair and delete the old one.

If there are no errors in the initialization process the possibility to generate a TRH key pair (PK_{TRH_A} and SK_{TRH_A}) has to be physically destroyed (e.g. by melting a fuse after key-pair generation). This ensures that VRI cannot be changed any more (at least until TRH is removed; partly req. I2a/b). Demanding that the owner generates the key pair ensures that vehicle manufacturers do not know VRIs of their vehicles (partly req. P1).

The VRI then is registered with the GTA in the normal registration process of a new vehicle at the local admission office. This means the local admission office has to read PK_{TRH_A} and must check that key pair generation is deactivated. Then it saves VRI within the existing GTA registers and therefore is able to link VRI to owner identity. Then GTA issues a certificate ($CERT_{TRH_A}$) that is saved in vehicle's TRH. TRH can check validity by means of the stored root certificate ($CERT_{Root_{DE}}$). Communication between the local admission office and GTA has to be protected by the usual means of network security like firewalls, VPNs, etc. (req. C2) and shall not be discussed here.

The fact that the owner can check and store root certificates in TRH ensures that vehicle manufacturers or maintenance personal is not able to operate their own certificate hierarchy by installing own root certificates in TRH (req. C2). On the other hand, the owner has to be made responsible for correct configuration of root certificates. Fig. 3 shows the initialization process.

3.3 Symmetric Part

As already mentioned, beacons and messages of the value-added services are protected by means of symmetric cryptography. To be able to participate, node A uses a challenge response protocol and $CERT_{TRH_A}$ to authenticate to the local GTTP. To increase availability, GTTP should be reachable via the VANET as well as via other communication infrastructures like GSM. GTTP has to be independent from law enforcement and GTA (see later). After authenticating itself GTTP issues a pseudonym PA and an associated symmetric key $k_{MAC_{PA}}$ that is unique to the VRI for a certain period of time and stores the relation between VRI and PA. It also issues the symmetric keys $k_{MAC_{ALL}}$ and k_c. These are the same for all VANET users in a certain geographic region and a certain time period. TRH ensures that the symmetric keys are kept secret (req. C2). The exchange of the symmetric keys has to be encrypted. The necessary encryption keys can for example be generated by a Diffie-Hellman key exchange after mutual authentication. Varying levels of confidentiality can easily be achieved by additionally encrypting the sent data with keys based on VRI or other service specific certificates (req. C1).

Messages are assembled inside the TRH. First PA is added after the data to be sent. Then a message authentication code (MAC_1) computed with $k_{MAC_{PA}}$ is added, followed by MAC_2 computed with $k_{MAC_{ALL}}$. The whole message is encrypted with k_c (see fig. 4). Outsiders not participating in the VANET are not able to see any identity or data, because messages are encrypted. Profile generation and eavesdropping from outsiders therefore is prevented (req. C1, P1). To hinder profile generation by VANET participants GTTPs can assign a number of pseudonyms to a vehicle that are changed frequently. Additionally, the pseudonyms are just valid for a short time interval. After that time interval a given pseudonym could belong to another vehicle what makes linking of pseudonyms to generate a movement or service usage profile pretty hard.

VANET participants (or more precisely their TRH) are able to decipher messages with the help of k_c and check integrity using MAC_2 computed with $k_{MAC_{ALL}}$ (req. I1). Ex post accountability (req. I2b) is ensured by employing MAC_1 computed with $k_{MAC_{PA}}$. Only TRH of the sending vehicle and GTTP know $k_{MAC_{PA}}$. Therefore, (only) GTTP can confirm if a given message is really from the claimed sender by checking MAC_1. This only works if all computations are carried out in TRH and nobody is

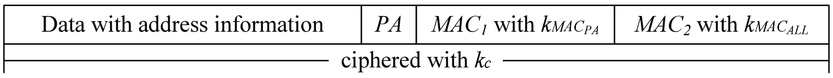
Data with address information
PA
MAC_1 with $k_{MAC_{PA}}$
MAC_2 with $k_{MAC_{ALL}}$
ciphered with k_c

Fig. 4. Message with symmetric protection.

able to get to know the symmetric keys or influence message construction. Therefore it is crucial to design TRH with a self-destruction mechanism that is activated if anybody is trying to manipulate the TRH (req. C2).

Req. P2 (protection against surveillance) is accomplished by employing independent GTTPs that have to follow strict procedures before revealing the VRI associated with a given pseudonym at a certain time. Only with this VRI law enforcement is able to find the owner of the vehicle by using the GTA register. We want to point out that while achieving non-repudiation privacy is protected. Trust is distributed between GTTPs and GTA: GTTPs do not know the real identities of the vehicle owners, GTA does not know the relationship between VRI and pseudonym.

4 Evaluation and Related Work

Our proposal ensures message integrity (I1) by means of digital signatures and MAC_2. Immediate sender authentication for alarm signals and instructions (I2a) is ensured by using short time certificates that can be linked to a specific driver and vehicle. For all other messages ex post accountability (I2b) is achieved by adding a digital signature based on VRI or MAC_1 respectively. Protection against profile generation (P1) is ensured by employing changing pseudonyms for frequently sent messages and messages of value-added services. The independent GTTPs ensure that automated surveillance is not possible (P2). Law enforcement and GTA know the VRI and the identity of the owner but cannot link this information to a pseudonym. Only in severe cases like accidents with death results GTTP has to reveal the connection between a given pseudonym and VRI. In addition, GTTP does not know the real identity corresponding to a given VRI. Different levels of confidentiality (C1) can be used by encrypting message data with VRI certificates, symmetric keys or other service specific key material. The security infrastructure is protected (C2) by means of encrypting all key management messages and employing TRH that ensures that nobody can influence message generation or get to know symmetric or private keys.

We now want to show the computational and bandwidth efficiency (A1) of our solution. We assume a message length of 300 byte what is feasible for alarm signals, warnings and beacons. For the asymmetric part we further assume the usage of RSA with SHA-256 (key length 2048 bit). The symmetric part employs HMAC SHA-256 (key length 192 bit) and AES (key length 192 bit). According to [10] this ensures adequate security till at least 2020. Pseudonyms are 48 bit in length.

If we assume the smallest possible (non standard) certificate consisting only of a public key and a digital signature we get $2048bit + 2048bit = 4096bit$. The digital signature is additional $2048bit$. Summing this up ($768byte$) and adding the message length we get $1068byte$ what translates in $768byte/1068byte = 72\%$ security overhead. For the symmetric part we get the following: $PA + 2 * HMAC = 48bit + 2 * 256bit = 70byte$. In total this is $370byte$ and a security overhead of just $70byte/370byte = 19\%$. Key management messages are negligible because they are sent very seldom (e.g. once a day). Revocation lists are not needed because of employing short time certificates for alarm signals and instructions as well as the possibility to check plausibility of warnings by means of in-car sensor data and messages received by other VANET participants. Recall that far the most messages exchanged are beacons (approximately every 10 to 300 ms). These are protected by symmetric cryptography that is very efficient in terms of additional security overhead compared to messages protected by asymmetric cryptography. Using a middle class PC-system we found that the symmetric part is faster than the asymmetric part by a factor of approximately 600.

There are only few proposals for VANET security infrastructures so far. Most researchers ([2, 11, 12]) propose a PKI solution, with anonymous or pseudonymous certificates issued by the CA. This solutions add digital signatures to each message and do not provide encryption of messages. The main drawbacks in comparison to our solution are that VANET participants have to ultimately trust the CA and computational needs and bandwidth overhead are enormous (remember the numbers above). In addition, up to date revocation information is necessary. Due to the fact that messages are not encrypted even outsiders can eavesdrop and possibly create movement profiles. [13] suggest a system based on symmetric cryptography. The main problem of this proposal is that the vehicles have to contact a base station to decrypt and verify messages what is not feasible taking into account the real-time demands and the very high mobility in the VANET. Some other authors ([14–16]) outline security and privacy issues in VANETs but do not present a security infrastructure.

5 Conclusion and Further Aspects

After motivating why some kind of security infrastructure is needed in a VANET, we discussed requirements like message integrity and non-repudiation for such infrastructures. In section 3 we made a proposal how a security infrastructure could be constructed that uses asymmetric as well as symmetric cryptography and tamper resistant hardware to fulfill the requirements. While fulfilling all requirements our proposal is especially designed to protect privacy of the VANET users and proved to be very efficient in terms of computational needs and bandwidth overhead (see sec. 4).

In our future work we will refine the proposal and discuss issues like the best schedule for changing the symmetric keys and pseudonyms. In addition, the best size of the geographic regions for the GTTPs will be determined by employing simulations.

References

1. Munoz, J., Syracuse, N.: Proc. of the 53. internet engineering task force (2002)
2. Raya, M., Hubaux, J.P.: The security of vehicular ad hoc networks. In: Proceedings of SASN 2005, ACM (2005)
3. IEEE: (Dedicated Short Range Communication Standard (DSRC)) http://grouper.ieee.org/groups/scc32/dsrc/namerica/.

4. Tian, J., Coletti, L.: Routing approach in cartalk 2000 project. In: Proceedings of the IST Mobile & Wireless Communications Summit 2003. Volume 2. (2003)
5. Plößl, K., Nowey, T., Mletzko, C.: Towards a security architecture for vehicular ad hoc networks. In: Proceedings of ARES 2006, IEEE Computer Society (2006)
6. EU: The Galilei Project - GALILEO Design Consolidation (2003)
7. Xu, W., Trappe, W., Zhang, Y., Wood, T.: The feasibility of launching and detecting jamming attacks in wireless networks. In: MobiHoc 05: Proc. of the 6th ACM internat. symposium on Mobile ad hoc networking and computing, ACM (2005)
8. Council of the EU: Council Regulation (EC) No 2135/98 (1998)
9. Tian, J., Maihoefer, C., Nelisse, M., Provera, M., Dagli, I., Tepfenhart, M., Brenzel, C.: Routing protocol implementation (2003)
10. Lenstra, A.K., Verheul, E.R.: Selecting cryptographic key sizes. Journal of Cryptology **14** (2001)
11. Parno, B., Perrig, A.: Challenges in securing vehicular networks. In: Proceedings of Workshop on Hot Topics in Networks (HotNets-IV), ACM (2005)
12. Raya, M., Papadimitratos, P., Hubaux, J.P.: Securing vehicular communications. IEEE Wireless Communications, Special Issue on Inter-Vehicular Communications (2006)
13. Choi, J.Y., Jakobsson, M., Wetzel, S.: Balancing auditability and privacy in vehicular networks. In: Q2SWinet 2005: Proc. of the 1st ACM international workshop on quality of service and security in wireless and mobile networks, ACM (2005)
14. Dötzer, F.: Privacy issues in vehicular ad hoc networks (2005)
15. Zarki, M.E., Mehrotra, S., Tsudik, G., Venkatasubramanian, N.: Security issues in a future vehicular network. In: Proc. of European Wireless 2002 Conference, Florence, Italy, February 2002. (2002)
16. Yang, H., Luo, H., Ye, F., Lu, S., Zhang, L.: Security in mobile ad hoc networks: Challenges and solutions. IEEE Wireless Communications **11** (2004)