Towards a Security Architecture for Vehicular Ad Hoc Networks

Klaus Plößl, Thomas Nowey, Christian Mletzko
University of Regensburg, 93040 Regensburg, Germany
Klaus.Ploessl@wiwi.uni-regensburg.de

Abstract

Vehicular ad hoc networks (VANETs) have the potential to increase road safety and comfort. Especially because of the road safety functions, there is a strong demand for security in VANETs. After defining three application categories the paper outlines main security and privacy requirements in VANETs. Next, a security architecture for VANETs (SAV) is proposed that strives to satisfy the requirements. To find mechanisms applicable in the architecture a survey of existing mechanisms is given.

1 Introduction

In 2001 the European Union committed to reduce traffic victims until 2010 to the half of the victims in the year 2000 [9]. One component to reach this goal is active road safety (prevention of accidents). Common methods in this area are ABS (Anti-lock Braking System) or ESP (Electronic Stability Program). Another method is ADAS (Advanced Driver-Assistance Systems) where vehicular ad hoc networks (VANETs) are subordinated to.

More technically VANETs are a subgroup of mobile ad hoc networks (MANETs, defined in [22]). The main difference is that the mobile routers building the network are vehicles like cars or trucks and their movement is restricted by factors like road course, encompassing traffic and traffic regulations. It is a feasible assumption that the members of VANETs can connect to fixed networks like the Internet occasionally, at least at regular service intervals. A main goal of VANETs is to increase road safety. To achieve this goal the vehicles act as sensors and inform each other about abnormal and potentially hazardous traffic conditions like accidents, traffic jams or glaze.

The messages exchanged in the VANET influence the behavior of the drivers. Depending on the information they get they will e.g. drive very carefully and slowly in the case of a glaze warning or choose an alternate route in the case they are informed about a traffic jam on their desired route. Adversaries could exploit this by injecting wrong messages and slowing down traffic or getting a vehicle-free road. To prevent this kind of misuse security is very important in VANETs.

After defining three application categories and deriving security and privacy requirements in section 2 this paper outlines a security architecture for VANETs (SAV) which strives to prevent attacks and enables the participants to communicate in a secure manner while also protecting their privacy. In section 4 a survey on existing approaches is done to find suitable mechanisms to use in the architecture.

2 Application Categories and Requirements

2.1 Application Categories

In this section we define three main categories of applications in VANETs. The categorization is done with respect to security and privacy issues as well as communication requirements.

Telematics Messages and Warnings: The vehicles exchange messages to inform each other about events and dangers on the road. The messages include information derived from the car sensors (ABS, ESP, etc.), like a recognized full stop or aquaplaning, the usage of an airbag, current speed and acceleration or deceleration as well as sending time and position. Even traffic jams or congestions can be identified by aggregating and interpreting these messages. Besides information exchange between vehicles, stationary transmitters (e.g. SOS-telephones) can be used to extend range or provide access to other networks.

According to [30] there are two technical possibilities for such a telematics system:

1. Passive: All vehicles periodically broadcast messages with their current status (*beacons*) and forward such messages if necessary. Based on rules each vehicle decides independently how to react to the information. The quality of these rules defines the effectiveness of the system.

2. Active: A vehicle only sends messages if it recognizes a problem or has to forward a message. The effectiveness of the system depends mainly on the problem recognition.

The main drawbacks of the passive approach are the need for more bandwidth and computing power and the fact that creation of movement profiles is easier. The big advantages are that more situations can be recognized and anomaly detection is easier because the data of all surrounding vehicles is available.

In this category the security requirements are high because the data sent in beacons and warnings influences the behavior of the drivers. It should for example be impossible to replay or modify messages. In addition, privacy is an issue because the data sent could – especially in the case of periodically sent beacons – easily be used for movement profile creation. The addressees are unknown – all vehicles in a given region (e.g. all vehicles not more than 20 km behind the scene of an accident) are addressed. Sending a message to addressees in a given geographic area is known as *geocasting* [20].

Alarm Signals: This application category mainly addresses electronic alarm signals from emergency vehicles (police cars, fire engines, ambulances, etc.) in action. By sending its current position, time and destination or desired route, the other vehicles can (and must) clear the way for the emergency vehicle. By forwarding the alarm signals the time to react for the other vehicles further increases. In addition, it is possible to influence the behavior of infrastructure like traffic lights to grant the emergency vehicle free drive. [6] suggests a secure communication protocol for the special case of influencing the state of a traffic light.

In this category the security requirements are very high because the data sent directly influences the behavior of the drivers and infrastructure. It should for example be impossible to replay or modify messages because then adversaries could clear their way like emergency vehicles. Privacy is normally not an issue here but the addresses have to know for sure that the message originates from an authorized source. Again addressees are unknown and geocasting is used.

Value-added Services: There are numerous services to think of in a VANET. These services mainly depend on unicast messages to an already known communication partner and include location based services like finding an alternative route, the next hotel or restaurant as well as other services like providing Internet access. The security and privacy requirements range from low to high depending on the service. In contrast to the other categories this is end-to-end communication (in most cases over multiple hops) and the user has no obligation to use the service. The priority is comparatively low.

2.2 Requirements

The following enumeration of security and privacy requirements is based on a more detailed analysis of the application categories that is omitted here due to space limitations.

Integrity

1. Integrity for all messages should be protected to prevent adversaries from altering them.
2. Authentication is needed to keep outsiders[1] from injecting messages.
3. A reliable time source is needed to guard against replay-attacks and a reliable positioning system is needed to prevent position spoofing.

Confidentiality

4. The privacy of users should be protected to prevent creation of movement and usage profiles and to protect users' identity.
5. The messages should be encrypted to prevent outsiders from gaining information from the value-added services.

Availability

6. To reach all necessary recipients that may even be unknown to the sender an adequate routing protocol is needed. Also some messages (e.g. an ice warning) have to be kept in a specified location for a specified time.
7. Because of the urgency of traffic information low latency is a must for the communication.
8. Scalability is also an issue given some 50 million vehicles only in Germany [25].

To be able to prosecute misuse non-repudiation is necessary but this bears (besides others) the danger of automated traffic surveillance. Therefore, when designing a security mechanism there should be the possibility to identify the sender of a message but this identification should not be allowed in an automated and easy fashion.

[1] Outsiders are entities that are not valid participants of the VANET, e.g. residents that profit by or are at a disadvantage by certain road courses.

3 Security Architecture

After introducing our communication model this section outlines a security architecture for VANETs (SAV).

Communication model. We suggest a *hybrid telematics system* where each vehicle periodically sends beacons (passive). If it recognizes a potentially dangerous traffic event by combining and interpreting the beacons of other vehicles and in-car sensor data, explicit warnings are sent (active). I.e. the two approaches mentioned on page 1 are combined and there is no need to forward beacons because of the explicit warning messages. Beacons are just sent single hop. The warning messages are spread over multiple hops in a specified region depending on the type of the traffic event.

To lower network traffic the beacons of the hybrid telematics system should be combined with messages needed by the routing algorithm. Therefore a beacon contains all information needed by the routing algorithm as well as enough information for the hybrid telematics system to decide if there is a dangerous situation. More concretely it has to contain the pseudonym, position, current time and movement (direction, speed and acceleration or deceleration) of the sending vehicle at a minimum. The sending interval should be variable to reduce network traffic or to be able to comply with conditions like speed, communication range, etc. as suggested in [28] and [27].

SAV consists of three layers shown in Fig. 1. The bottom layer includes basic security elements that are used in the other layers. The second layer (single-hop-security) shows how the beacons are secured that are in most cases the first contact between vehicles and therefore build the basis for further communication. The multi-hop layer includes all other applications, services, etc. used in the VANET.

Basic security elements. As fundamental security mechanism we suggest to employ a centralized public key infrastructure (PKI) with a trusted third party (TTP) what is motivated in more detail in section 4.3. All vehicles get – preferably at production time – the root certificate of the TTP and pseudonym certificates with corresponding key pairs that are stored in tamper proof hardware. We assume that there are enough pseudonyms to be able to protect the privacy of the participants. Emergency vehicles get certificates with an additional attribute that certifies their special role. The question if the certificates should be bound to persons, vehicles or both is not yet answered but does not affect the overall functionality. Additionally, each vehicle needs the ability to determine its current time and position in a reliable manner.

Single-Hop-Security. As stated above the beacons are the basis for routing and the hybrid telematics system. To be able to implement security mechanisms at a higher level it has to be ensured that the receiver of a beacon has the ability to verify the integrity of the beacon as well as to identify the sender as a valid participant of the VANET.

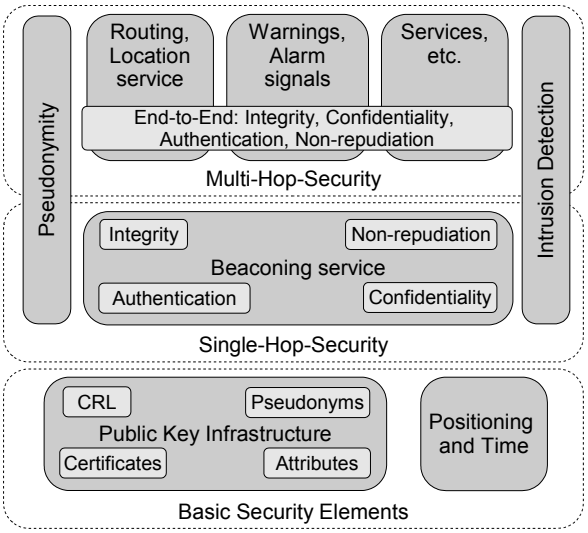

Figure 1. Security Architecture

To be able to do so, we employ the PKI of the basic security layer. Each sending vehicle S digitally signs its beacons and sends them in conjunction with its certificate $Cert_S$ that is used for the digital signature. The receiving vehicle R uses $Cert_S$ (and the root certificate of the TTP) to test if S is a valid participant of the VANET[2]. Then the signature in conjunction with $Cert_S$ is used to verify that the given beacon is really from S (authentication and non-repudiation) and has not been changed (integrity). The freshness of the beacon is proved by the time included in the beacon. After this R can be sure that he communicates with S. For performance reasons he should add $Cert_S$ to a neighborhood table for a specific time[3]. After S has checked R's beacons in the same way S and R can communicate in a secure manner. If confidentiality is an issue they can encrypt messages with the public key included in the certificate of the communication partner. For performance reasons the validity of the certificate just needs to be checked if it is not already in the neighborhood table.

Because asymmetric cryptography is very costly in terms of computing time and beacons are sent relatively often, we propose a hybrid variation of the above protocol: After the certificate exchange the two neighbors can securely exchange a secret symmetric key that is saved in the neighborhood table, too. This secret key is used together with a

[2]We assume that anybody with a valid certificate is allowed to participate in the VANET.

[3]The time depends on traffic conditions (like current speed, vehicle density, etc.).

message authentication code (MAC) to provide integrity of the beacons. The asymmetric digital signature is not necessary any more. This hybrid variation also has some drawbacks: The integrity check can only be done after a secret key is exchanged with each neighbor. A unique MAC has to be computed for each neighbor what needs additional time and bandwidth. The possible optimization to use the same symmetric key for all neighbors results in completely loosing non-repudiation what is not desirable. If the pure asymmetric or the hybrid variant is more efficient depends on the frequency of neighbor changes, the absolute amount of neighbors and the cryptography algorithms used.

Periodically sent beacons with position and time information enable external eavesdroppers to create movement profiles. To protect against this, the beacons could be encrypted and should not give away information about the sender or receiver. To encrypt the messages one could use the public keys or the secret symmetric keys of the hybrid variant, respectively. A problem is that the eavesdropper would still get to know any new neighbors, because these have to send their certificates in plain text before being able to encrypt communication with the existing neighbors.

To overcome this problem, each new neighbor N could send a couple – say x – of other certificates in addition to his own certificate. The existing neighbors then would have to encrypt all messages with all public keys (or in the hybrid variant have to encrypt at least the new symmetric keys with all public keys). The attacker then only knows that one of the x+1 vehicles has joined. The x+1 certificates build the anonymity group for N.

In summary, digitally signing each message greatly improves security and prevents outsiders from injecting bogus information. Encryption imposes a lot of overhead and increases the time to react to a dangerous situation because before being able to read a beacon, the certificates (and probably keys) have to be exchanged and the message has to be decrypted. We think road safety is more important here than the additional protection against the creation of movement profiles by non-participants and therefore discourage encryption at this level. Instead, the privacy of the users is protected by complicating the creation of movement profiles by regularly changing pseudonyms (see 4.4 for more details).

Multi-Hop-Security. This layer is applicable for alarm signals, warnings and value-added services. There are the following options for end-to-end security:

- In the case of uni- or multicast, certificates can be exchanged with the communication partners. These can be used for asymmetric cryptography or the exchange of symmetric keys. A problem may be pseudonym changes because messages may get lost after the change.
- In the case of geocast, asymmetric cryptography is a must. Because the recipients of the message are unknown, there is no way to exchange certificates or keys with them. Therefore encryption is not possible here. The digital signature provides at least authentication, non-repudiation and integrity.

A possibility to protect the exact position of the sender of a geocast message relevant for vehicles further away (like a traffic jam warning) is spatial cloaking – the obfuscation of the exact position information. Addressees very near to the traffic jam need the exact position (e.g. "behind the next curve"), whereas addressees 50 km away just need to know between which exits of the highway the traffic jam is located to be able to choose an alternative route (example from [29]). The cloaking can be done in various ways, one of the simplest is adding a random distance to the exact position information in dependence of the addressed geographical region. I.e. vehicles further away get less reliable position information. More on cloaking can be found in [14]. This method is not suitable for all geocast messages. E.g. alarm signals must contain the exact position information to enable the other vehicles to prepare for the arrival of the emergency vehicle in time.

Further Aspects. The aggregation and interpretation of beacons can lead to a warning message in case of a potentially dangerous situation. Therefore the hybrid telematics system depends on the cooperation and trustworthiness of the participants. The same is true for the routing protocol. Insiders (entities that are valid participants of the VANET) trying to actively interfere the protocols are very dangerous adversaries. To defend against these we suggest using tamper proof hardware as platform for the telematics and routing algorithms. As for the telematics system beacons that triggered a warning message should be saved by the sender of the warning message to be able to prosecute the injection of bogus information.

An intrusion detection system (IDS) should check if messages are forwarded on the technical layer. In addition, it should check if the information received is feasible. This check can be done by employing data delivered from sensors inside the vehicle or information received from other participants of the VANET. If an adversary inside the VANET is detected who does not forward messages or injects bogus information, this information (including evidence like the in-car sensor data) should be forwarded to the TTP. Then the TTP can decide if the adversary's certificate should be revoked with the consequence that the adversary is no longer able to participate in the VANET. This mechanism requires that the participants regularly update the certificate revocation list (CRL) from the TTP or have other means to check the validity of a certificate.

To reduce latency for important messages (like beacons, warning messages and alarm signals) a priority scheme that prefers this type of message could easily be added. To be able to protect against the creation of movement profiles by insiders and outsiders we suggest to use changing pseudonyms. One must not forget that identifiers on all communication layers must be changed when pseudonyms are changed. An example of such an identifier could be the medium access control address of the wireless protocol or even a typical packet size or RF-fingerprint caused by the hardware [5].

Evaluation. Integrity is ensured in single-hop as well as multi-hop messages. Also, all messages are authenticated and there is the possibility to encrypt messages (req. 1, 2 and 5). In addition, non-repudiation is guaranteed by employing a digital signature. It is not possible for outsiders to inject bogus information or to reuse old messages for a replay attack. If the algorithms are implemented in tamper proof hardware even valid participants cannot actively manipulate the communication. Pseudonyms protect the identities of the participants. By creating appropriate policies at the TTP even law enforcement could not easily get to know the identity of a given VANET participant. If pseudonym changes are done in an appropriate manner creation of movement and usage profiles is prevented (req. 4). Scalability (req. 8) was considered when suggesting a PKI. Requirements 3, 6 and 7 can not be fulfilled solely by the security architecture. We will address this issue after the survey on existing mechanisms.

4 Existing Mechanisms

Zarki et al. [31] probably published the first paper dealing with security in VANETs. Other existing publications on security in VANETs cover single aspects like PKI [7, 24] or secure position sensing and privacy [16]. [23] gives an overview on security flaws and solutions. This section briefly evaluates existing mechanisms that could be employed in the proposed security architecture.

4.1 Assumptions

No special wireless technology is needed underlining the independence of the security architecture. Nevertheless dedicated short range communications (DSRC) is expected because it is explicitly designed for VANETs, supported by US and European car manufacturer consortia and standardized as IEEE 802.11p WAVE (wireless access for vehicular environments).

Vehicles are cars and trucks. Motorbikes or other road users like pedestrians are not taken into consideration to prevent restrictions on hardware. The VANET will not operate in a standalone fashion but be supplemented by some infrastructure like traffic lights or dedicated hardware like S0S-telephones that play the role of message repeaters. Access to a stationary network is – at least temporarily – possible. It is expected that data inside vehicles is reliable. Especially the sensor data is expected to be correct.

Requirement 6 cannot be satisfied by the security architecture. Therefore we assume that there exists a secure routing protocol and a mechanism to keep messages in a specified geographic region. Nevertheless we briefly examine these issues in the following.

Routing. Routing protocols can be categorized in topology-based and position-based routing algorithms. A main advantage of position-based routing is that it supports geocasting. [12, 11, 18] found that position-based routing is also superior to topology-based routing in VANETs in terms of delivery rate, additional network load and latency.

Now we want to outline the requirements for a good VANET routing protocol:

- Functional requirements
  1. Has low latency.
  2. Is capable of uni-, broad-, multi- and especially geocasting.
  3. Guarantees delivery or at least a high delivery rate.
  4. Considers the specific VANET topology (streets, node destination, etc.).
  5. Causes low additional network load.
- Security and privacy requirements
  6. Protects from active attacks like the injection of wrong routing information.
  7. Protects from passive attacks like black hole attacks.
  8. Protects the position information of the nodes.
  9. Allows anonymity or pseudonymity.
  10. Protects from or at least complicates the creation of movement profiles and traffic analysis.

In our analysis we could not find a routing protocol that fulfills all requirements. There are routing protocols that fully satisfy the security requirements (e.g. ASR [33]) but these lack functional requirements or make assumptions that are impractical in VANETs (e.g. there must be a shared secret between source and destination in the case of ASR). Some protocols try to find a compromise between security and functional requirements (e.g. AODV-SEC [8] or

SPAAR [4]) but these don't support geocasting what is essential in a VANET. Spatially aware routing (SAR, [27]) from the CarTalk2000 project fully satisfies the functional requirements but does not fulfill any security requirements. There seems to be no good routing protocol to use at the moment.

Regional Alerts. There are mainly two approaches to keep regional alert messages in a specified geographic region for a specified time: Stationary transmitters that periodically repeat the message and BiPP (Bidirectional Perimeter-based Propagation, [26]) that just needs the cooperation of the VANET participants.

Stationary transmitters are more reliable than BiPP but we don't expect the necessary infrastructure in the near future because of high costs. Therefore we suggest using BiPP that can be used without additional costs. Nevertheless BiPP should be modified in a way that it is able to use stationary transmitters when available. Then the reliability and efficiency of the regional alert system could be increased by deploying stationary transmitters at positions that are potentially highly dangerous.

4.2 Positioning and Time

Each participant should be able to determine his current position and the current time correctly and provable. Nobody should be able to forge a position and nobody should get to know the position and identity of a participant unless the participant tells him. The time needed to determine the position should be very short because of the real time constraints of the VANET.

[3] introduces SPA (self-positioning-algorithm), a semi autonomous algorithm that enables the nodes in an ad hoc network to determine their position relative to each other without the need for additional infrastructure. No statements about the security of and the time needed by the algorithm could be found in the literature. Therefore it can not be recommended here. Another approach named verifiable multilateration is introduced in [16]. This approach employs a fixed trusted infrastructure to verify positions by triangulation. This fixed infrastructure has to be very dense what makes this approach very costly. Also there is no information available about the time needed to complete the algorithm. Therefore it can not be recommended here, too.

The most practical way to fulfill the requirements is using GALILEO, the European satellite navigation system that is expected to start operation in 2008. It needs no additional stationary infrastructure and the Safety of Live Service (SoL) guarantees an availability of 99,8%, a precision of 4-6m and additional integrity information. Combined with the built-in authentication mechanism certified receivers can prove the authenticity of the information [10].

The additional information to test integrity and authenticity can not protect from all attacks. An attacker might be able to delay the satellite signals what leads to a wrong computation of the position and time. Nevertheless this attack is a lot more difficult than forging GPS information.

4.3 Public Key Infrastructure

There are different proposals how to implement a PKI in ad hoc networks. For example, [15] suggests a solution similar to PGP and [32] suggests a decentralized PKI based on threshold cryptography. Both are not applicable in VANETs. In the first proposal it is not guaranteed that a certificate can be verified. This is not acceptable especially in the case of alarm signals. In the threshold schema a lot of participants have to work together to issue new certificates. This could not be expected in a VANET with numerous participants not knowing each other.

As stated above VANETs are usually hybrid networks with the possibility to access a stationary network at least temporarily. Therefore we suggest to use an "ordinary" centralized PKI approach with a TTP that issues certificates and revokes them. Two promising proposals how to implement such a PKI are LKN-ASF (LKN Ad hoc Security Framework, [24]) and MANET-IDs in conjunction with MANET-CRS [17]. Because of the fact that LKN-ASF already has proved good performance in simulations (see [24, 7]) we prefer this approach and will do some deeper analysis on this in the near future.

4.4 Pseudonymity

To be able to prevent creation of movement or usage profiles we suggest using role based pseudonyms. By employing roles the participants can distinguish between "ordinary" participants and privileged participants like police cars or fire fighters in action. Each participant needs a couple of pseudonyms for his "ordinary" participant role that should be unlinkable. Using randomly generated transaction pseudonyms would be a possibility to ensure anonymity. But in VANETs non-repudiation is a must because otherwise insiders could inject faked messages without having to fear punishment like exclusion from the VANET. Therefore a trusted third party (TTP) has to issue pseudonyms that the participants change regularly. Now just the TTP and law enforcement (in the case of prosecution) is able to find out the identity for a given pseudonym and get to know the other pseudonyms corresponding to the identity. All other adversaries cannot create movement or usage profiles if the pseudonyms are unlinkable.

Linkability – in this context mainly depending on the question when pseudonyms should be changed and who should initiate the change – is a problem in VANETs, es-

pecially if unencrypted telematics messages are exchanged very frequently that contain exact position information. In this case an adversary could use statistical methods to link the pseudonyms. A method to complicate this attack are MIX-zones first mentioned in [1]. Problems with MIX-zones especially in the case of VANETs and some other solution possibilities to achieve unlinkability are discussed in [5]. But one should not forget that even without a VANET it is possible to physically follow a vehicle to create a movement profile. In the case of warnings and messages sent over multiple-hops the position information could be cloaked to hamper profile creation (see section on multi-hop-security).

4.5 Intrusion Detection

[17] gives a good overview on existing proposals like Watchdog and Pathrater [19], CONFIDANT [2], CORE [21] and others. In addition, it develops MobIDS (mobile intrusion detection system) an IDS architecture for mobile ad hoc networks. MobIDS is suitable for VANETs and makes some sophisticated suggestions on detecting nodes not correctly forwarding messages and informing the TTP about malicious behavior. The detection process is based on an improved version of the Watchdog approach and a probing process. A Watchdog W listens to all traffic in promiscuous mode (promiscuous overhearing) and therefore is able to check if a node N in range really forwards messages that are intended for forwarding. In the probing process the nodes on the route are explicitly probed by sending them messages to forward. This two "sensors" contribute (among some others) to a local rating of the other nodes that can lead to local reactions like avoiding certain nodes or discarding messages from them. In addition, the local rating is shared with other instances of MobIDS and combined to a global rating. If the global rating of a node becomes too poor he may be excluded from the network completely. For further information see [17].

This "technical" intrusion detection should be combined with the "semantic" detection of wrong information in beacons and warnings. [13] proposes a general approach how to validate VANET data, i.e. how to check if the information contained in beacons and warnings from other vehicles is feasible. This proposal should be integrated in MobIDS. In addition, evidence for malicious behavior has to be saved and submitted to the TTP. This evidence could be beacons and in-car sensor data that triggered a warning message, suspicious warning messages from other VANET participants or the like.

5 Discussion and Future Work

So far existing approaches focused on single aspects of VANET security. This paper defines security and privacy requirements and outlines a comprehensive security architecture that enables various applications and satisfies the key requirements. The requirements an architecture cannot fulfill seem to be satisfiable by plugging existing or modified mechanisms in the architecture.

Section 4 shows numerous existing mechanisms that fit in the proposed security architecture. For example reliable time and position information (req. 3) is achievable by employing a certified GALILEO receiver. There are some good proposals on how to implement PKI and IDS but these have to be adjusted and refined to help to fulfill all VANET requirements. The main problem seems to find a secure routing algorithm with geocasting capabilities. With BiPP there exists at least a good protocol to keep warnings in a specified region for a specified time.

We are currently evaluating existing mechanisms applicable in the security architecture and try to improve them. Thereby we focus on exactly specifying a PKI and developing a secure routing protocol with geocasting capabilities. To prevent abuse of the VANET, we try to develop a system that encourages cooperation and punishes uncooperative behavior. In summary, we try to fill the architecture with exactly specified mechanisms to be able to test scalability and latency in simulations.

References

[1] A. R. Beresford and F. Stajano. Location privacy in pervasive computing. *IEEE Pervasive Computing*, 2(1):46–55, March 2003.

[2] S. Buchegger and J.-Y. L. Boudec. Performance analysis of the CONFIDANT protocol: Cooperation of nodes - fairness in dynamic ad-hoc networks. In *Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Lausanne, CH, June 2002. IEEE.

[3] S. Čapkun, M. Hamdi, and J.-P. Hubaux. Gps-free positioning in mobile ad-hoc networks. *Cluster Computing*, 5(2):157–167, April 2002.

[4] S. Carter and A. Yasinsac. Secure position aided ad hoc routing protocol. In *Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN02)*, 2002.

[5] F. Dötzer. Privacy issues in vehicular ad hoc networks, 2005.

[6] F. Dötzer, F. Kohlmayer, T. Kosch, and M. Strassberger. Secure communication for intersection assistance, 2005.

[7] S. Eichler. Security challenges in manet-based telematics environments. In *Proceedings of the 10th Open European Summer School and IFIP WG 6.3 Workshop*, June 2004.

[8] S. Eichler, F. Dötzer, C. Schwingenschlögl, F. J. F. Caro, and J. Eberspächer. Secure routing in a vehicular ad hoc network. In *Proceedings of the 2004 IEEE 60th Vehicular Technology Conference*, 2004.

[9] European Commission. Saving 20 000 lives on our roads - A shared responsibility, 2003.

[10] European Commission. The Galilei Project - GALILEO Design Consolidation, 2003.

[11] H. Füßler, M. Mauve, H. Hartenstein, M. Käsemann, and D. Vollmer. Mobicom poster: Location-based routing for vehicular ad-hoc networks. *Mobile Computing and Communications Review (MC2R)*, 7(1):47–49, 2003.

[12] H. Füßler, M. Mauve, H. Hartenstein, D. Vollmer, and M. Käsemann. A comparison of routing strategies for vehicular ad-hoc networks. Technical Report TR-02-003, Universität Mannheim, March 2002.

[13] P. Golle, D. Greene, and J. Staddon. Detecting and correcting malicious data in vanets. In *VANET '04: Proceedings of the first ACM workshop on Vehicular ad hoc networks*, pages 29–37. ACM Press, 2004.

[14] M. Gruteser and D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking, 2003.

[15] J.-P. Hubaux, L. Buttyn, and S. Čapkun. The quest for security in mobile ad hoc networks. In *Proceeding of the 2nd ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC 2001)*, 2001.

[16] J.-P. Hubaux, S. Čapkun, and J. Luo. The security and privacy of smart vehicles. *IEEE Security & Privacy*, 2(3):49–55, May-June 2004.

[17] F. Kargl. *Sicherheit in Mobilen Ad hoc Netzwerken*. PhD thesis, Universität Ulm, Ulm, 2003.

[18] C. Lochert, H. Hartenstein, J. Tian, H. Füßler, D. Hermann, and M. Mauve. A routing strategy for vehicular ad hoc networks in city environments. In *Proceedings of IEEE Intelligent Vehicles Symposium (IV2003)*, 2003.

[19] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Mobile Computing and Networking*, pages 255–265, 2000.

[20] M. Mauve, J. Widmer, and H. Hartenstein. A survey on position-based routing in mobile ad hoc networks. *IEEE Network*, 15(6):30–39, November/December 2001.

[21] P. Michiardi and R. Molva. A game theoretical approach to evaluate cooperation enforcement mechanisms in mobile ad-hoc networks, 2003.

[22] J. Munoz and N. Syracuse. Proceedings of the 53. internet engineering task force, 2002.

[23] M. Raya and J. P. Hubaux. Security aspects of inter-vehicle communications. In *Proceedings of Swiss Transport Research Conference (STRC)*, Ascona, Switzerland, March 2005.

[24] C. Schwingenschlögl and S. Eichler. Certificate-based key management for secure communications in ad hoc networks. In *Proceedings of the 5th European Wireless Conference: Mobile and Wireless Systems beyond 3G*, Februar 2004.

[25] Statistisches Bundesamt. Verkehr - Deutschland - Bestand an Verkehrsmitteln, Schienenfahrzeuge, 2005.

[26] Q. Sun and H. Garcia-Molina. Using ad-hoc inter-vehicle networks for regional alerts. Technical report, Stanford University, October 2004.

[27] J. Tian and L. Coletti. Routing approach in cartalk 2000 project. In *Proceedings of the IST Mobile & Wireless Communications Summit 2003*, volume 2, 2003.

[28] J. Tian, C. Maihoefer, M. Nelisse, M. Provera, I. Dagli, M. Tepfenhart, and C. Brenzel. Routing protocol implementation, 2003.

[29] L. Wischhof, A. Ebner, H. Rohling, M. Lott, and R. Halfmann. Sotis - a self-organizing traffic information system. In *Proceedings of the 57th IEEE Vehicular Technology Conference (VTC 03 Spring)*, 2003.

[30] X. Yang, J. Liu, F. Zhao, and N. H. Vaidya. A vehicle-to-vehicle communication protocol for cooperative collision warning. Technical report, University of Illinois at Urbana-Champaign, 2003.

[31] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian. Security issues in a future vehicular network. In *Proc. of European Wireless 2002 Conference, Florence, Italy, February 2002*, 2002.

[32] L. Zhou and Z. J. Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24–30, November/December 1999.

[33] B. Zhu, Z. Wan, M. S. Kankanhalli, F. Bao, and R. H. Deng. Anonymous secure routing in mobile ad-hoc networks. In *29th Annual IEEE International Conference on Local Computer Networks (LCN'04), November 16 - 18, 2004, Tampa, Florida, USA*, 2004.