Open access • Proceedings Article • DOI:10.1109/WONS.2007.340489

# Security requirements and solution concepts in vehicular ad hoc networks



Tim Leinmüller, Elmar Schoch, C. Maihofer

**Institutions:** Daimler AG, University of Ulm

**Published on:** 02 Apr 2007 - Wireless on Demand Network Systems and Service

**Topics:** Vehicular ad hoc network, Wireless ad hoc network and Wireless sensor network

# Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks

Tim Leinmüller[+], Elmar Schoch[*] and Christian Maihöfer[+]
[+]DaimlerChrysler AG, Group Research and Advanced Engineering,
{Tim.Leinmueller|Christian.Maihoefer}@DaimlerChrysler.com
[*]University of Ulm, Institute of Media Informatics, Elmar.Schoch@uni-ulm.de

***Abstract*— Inter-vehicle communication is one of the most challenging research areas for communication in wireless ad hoc and sensor networks. The main benefit of this kind of communication is seen in active safety systems, which aim at increasing passengers' safety by exchanging warning messages between vehicles. In the past few years, considerable effort has been spent in research on networking protocols and applications, however research on security threats and solutions only started recently.**

**In this paper, we elaborate on security issues in vehicular ad-hoc networks (VANETs) regarding active safety applications. We provide an overview on solution concepts and evaluate requirements of corresponding mechanisms. One conclusion is that although some concepts can be viewed as strong solutions from a network point of view, they do not fit into the design constraints of VANETs. Therefore, less secure mechanisms will probably have to suffice.**

## I. Introduction

The common goal of projects on vehicular ad hoc networks (VANETs) is to improve vehicle passengers' safety by means of inter-vehicle communication. So, for instance in the case of an accident active safety applications could use inter-vehicle communication to warn approaching cars. Research projects (e.g. Fleetnet [1]) have already produced fundamental results in the domains of routing and applications. Ongoing work is concentrating on further evaluation of these results (e.g. in the Network on Wheels project [2]) as well as on the definition of common standards amongst car manufacturers (like in the C2C-CC [3], the VSCC [4] or the VII consortium [5]). Another important direction is the research on security and privacy issues of VANETs in projects like Sevecom [6].

In this paper we specifically address the security of active safety applications. We provide an overview on concepts that help to improve security in inter-vehicle communication scenarios and evaluate requirements of corresponding mechanisms. In a first step, the concepts are introduced independent of any system constraints, which are discussed afterwards. Fig. 1 shows the design space of security concepts as it is used in the remainder of this work.

The concepts are divided into two categories, based on their primary mode of operation. Proactive concepts comprise all approaches, which aim at increasing security by applying preventive mechanisms, e.g. by restricting access to the system. Reactive concepts on the other hand do not impose restrictions in advance, but detect and react on attacks and malicious or faulty behavior after it actually happened.

Along with the security concepts, which provide abstract descriptions of techniques that aim at realizing distinct security objectives, we outline selected security mechanisms realizing the aforementioned concepts. For every security concept, we look into requirements of the respective potential mechanisms, and on the benefits and security improvements the mechanisms provide.

Then, we discuss system design constraints in VANETs and conclude which of the security concepts and mechanisms currently appear to result in the most suitable security solution.

The remainder of this paper is organized as follows. The next section will give a brief overview on related work regarding security in VANETs. Section III summarizes the primary security and system requirements. In section IV and section V we introduce and evaluate security concepts and corresponding mechanisms. Then, we present constraints that have to be respected and propose a reasonable security design in section VI. Finally, section VII concludes the paper.

## II. Related Work

With progressing work on VANETs, it has become clear that security and privacy will be integral elements of the system. Without suitable security mechanisms and without respecting privacy, expectations on dependability will not be met and customers won't accept the system if it cuts their privacy. Hubaux et al. have been working as one of the first in the area, describing the challenges and solution approaches in several articles. For instance, in [7], the authors give an overview of key security topics in VANETs and in [8], Raya and Hubaux present a general description of problems and a framework for security in VANETs.

Besides, also Parno and Perrig have discussed security challenges in vehicular networks. In [9], they elaborate on contradicting goals like liability and privacy, they give an analysis of attackers, attacks and potential solutions for several problems.

Another work concentrates on correctness of data in VANETs. In their work, Golle et al. present a framework for detection and correction of such malicious data [10].

## III. Security and System Requirements

*1) Timely Delivery:* One of the primary system requirements is that the system should display all valid warning messages to the driver, respecting time constraints. For example,

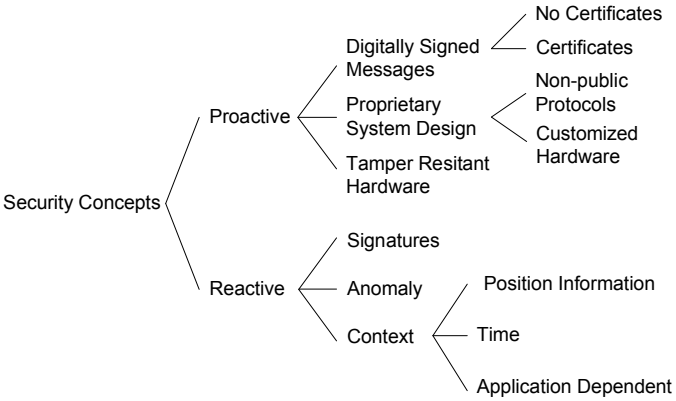


Fig. 1. Security Concepts Design Space

this means a warning message has to be displayed to the driver before it is too late to react on the warning.

*2) Location Accuracy:* Strongly related to the previous requirement, location accuracy means, that the system has to display warning messages at the right location. Combining both requirements, one can say a warning message has to be displayed to the driver before he passed the geographic position of the warning.

*3) Correctness of Messages:* From the security point of view, the system should prevent wrong warnings to enter the system. In case a wrong message has already entered the system or been created within the system, it should detect the wrong warning message before it has been displayed to the driver. On the other hand, correct warning messages should not be discarded as being invalid.

However, since it is impossible to realize a $100\%$ correctly working driver assistance system using wireless communication, as one can see from other examples in the vehicular environment, such as radar based adaptive cruise control, the requirements for the system have to be softened. This means, if possible, the system should display a technically achievable minimum of false warnings, while discarding virtually no correct messages at the same time.

*4) Privacy:* Due to the nature of wireless communication, information is sent via broadcast that anybody can receive. In fact, this information contains privacy sensitive data such as vehicle location, time, speed, and internal car sensor data. Thus it is a key prerequisite that this data cannot be linked to the driver's identity by other network participants. Amongst others, this means that a driver's location must not be traceable nor must it be possible to track vehicle movements.

*5) Liability:* Often, liability is regarded as another key requirement to communication based active safety systems. This means, e.g. in case of an accident, data recorded from the communication system will be used as evidence against involved drivers. However, this work argues to rate privacy and anonymity of communication data in VANETs higher than the benefit of using communication data for jurisdiction. In particular, collected evidence would not be complete until all vehicles get equipped with such a communication system, which might never happen. Also when thinking of tracking down criminals' vehicles, these might use cars not equipped with the communication system.

## IV. Proactive Security Concepts

This section introduces the three proactive security concepts that are currently the most promising candidates to increase security for warning applications in VANETs. Digitally signed messages primarily aim at providing message authenticity, yet, in combination with certified public keys, they provide network access restriction in addition. Proprietary system design and customized hardware aim at access restriction. In order to complement the aforementioned concepts, tamper resistant hardware is meant to provide secure input to the communication system, by securing the in-vehicle communication system and protecting it from manipulation.

### A. Digitally Signed Messages

*1) Without Certificates:* Digitally signed messages are a concept that is based on applying cryptographic digital signatures to messages or hashes over messages.

The use of digitally signed messages can provide three security improvements to communication, namely message authenticity, message integrity protection and non-repudiation. This means, with messages being signed, it is guaranteed that the messages originate from nodes holding the required cryptographic key material and the messages have not been altered by intermediate forwarding nodes.

Digital message signatures are commonly realized using asymmetric cryptography, i.e. by using public-private key cryptography. Messages (or hashes over the respective messages) are signed with the message originators' private keys. Later, the message receiver is able to verify the integrity and authenticity of the messages, by using the corresponding public keys. Assuming that the private key of a node is only known to itself, the node can not be impersonated. In addition, message receivers can securely correlate several messages to a single sender, in case the sender uses the same key for signing the message.

The requirements for digitally signed messages without certification are rather small, i.e. the nodes need a possibility to receive or create and store cryptographic key pairs as well as they necessitate the processing power for creating and verifying message signatures.

In VANETs, the concept of digitally signed messages can be applied to any message sent by a vehicle. In the context of active safety messages, it is of particular interest to apply it to the warning messages itself. Furthermore, messages that serve as input or triggers to the safety system could also be signed.

The advantage of this concept is that it is simple to realize with small requirements. Respective mechanisms are widely deployed and well known. However on the disadvantages side, what is not prevented by using digitally signed messages are attacks like message forging and and denial of service attacks (DoS). Malicious nodes are still able to replicate and pretend to

be more than one node at a given time (sybil attack). Also, the digitally signed messages concept does not prevent attackers to create fake warning messages.

*2) With Certificates:* In order to enhance the digitally signed messages concept, the signatures can be combined with digital certificates provided by a trusted third party. The basic assumption with certificates is that nodes, which include certificates in their messages, are trusted by other nodes that are able to verify the certificates.

Certificates in combination with digital signatures can be used to provide the following security improvements. In case the certificate issuer keeps track on issued certificates, he can trace back every signed message that includes a certificate to the senders real identity. Certificates can also be used as access control mechanism. This can be realized in a way, that only messages with valid certificates are considered by receivers. Message with invalid or no certificates are ignored. Another benefit from the usage of certificates is that, depending on the deployed usage restrictions, they can prevent or at least limit node replication (sybil) attacks. Of course, this requires a mechanism that guarantees that a node can use only one certificate at a given time and not multiple.

Certificates and digitally signed messages are usually combined as follows. The signed messages include a certificate that is cryptographically linked to the public key that belongs to the private key the message issuer uses to sign messages. Using certificates provided by a trusted third party makes it possible to realize a system where only messages from nodes that possess valid certificates are trusted and messages from other nodes are ignored. In addition, with the trusted third party storing information on issued certificates linked to key holders, it is possible to realize track back mechanisms. Using such a mechanism, the message originator can be determined using the corresponding certificate, for any message that is signed with the corresponding key pair. Once determined, the issuer can for example be excluded from further participation in the network, or even be legally pursued.

In order to be able to issue certificates, there is a need for a certificate management and distribution system with a certification authority (trusted third party). Furthermore, vehicles in the VANET need access to such a system, either permanently (”online” available), only from time to time, or even only once, e.g. during production of the unit/vehicle. The required access frequency depends on the system design. The higher it is, the more flexible the system. However, more detailed discussion of this is beyond the scope of this document, for additional details please refer to [11] for example.

In VANETs, requiring messages to be signed with a certified cryptographic key aims at preventing external attackers (e.g. notebook users at the road-side) from being able to inject wrong warning messages. The distribution of certificates is limited to valid VANET nodes, e.g. communication systems inside vehicles or roadside equipment. Since new valid active safety messages can only be created by nodes having obtained a valid certificate, this excludes outside attackers. Obviously, this statement holds only, if we can assume that those attackers have no certified keys and if they are unable to extract any from valid nodes. In addition, keys from maliciously behaving nodes or defective nodes can be identified and then revoked, or they expire after a certain time and are not renewed. Furthermore, owners of those nodes could be held responsible for any damage caused by the distribution of fake warning messages. Owner identification might also be used for other legal aspects, not directly linked to active safety application, which is out of scope for this document.

The advantage of the certificate concept lies in the possibility to exclude external attackers from the system, as well as in the ability to remove malicious or defective nodes. With appropriate mechanisms in place, it can also prevent sybil attacks. The downside is, that it suffers from the similar open issues as the concept without certificates, but to the costs of the need for a certification infrastructure. Furthermore and most important, these mechanisms will not prevent wrong active safety messages to be created by nodes that hold valid (certified) key material for message signing. In other words, every legitimate node in the VANET is still capable of creating fake warnings.

For example, fake warnings with valid signatures and certificates could result from one of the following actions. An attacker is able to extract or copy the cryptographic (private) key(s) from a vehicle. Or, someone is able to manipulate sensor values that serve as input to the in-vehicle safety system that creates warning messages. The same holds for any other information source that serves as input to the warning message creation system, e.g. the GPS receiver that supplies position and time information. In addition, resulting in the same effect as the previous two examples, an attacker could manipulate messages on in-vehicle communication buses.

### *B. Proprietary System Design*

*1) Non-public Protocols:* An alternative to the access restrictions as realized with the usage of digitally signed messages with certificates, is the usage of non-public communication protocols.

In case the protocols remain undisclosed, like the certificate approach, this concept prevents non-authorized nodes from participating in the network.

The security concept of non-public communication protocols, and of proprietary system design in general, is based on the assumption that it is rather difficult and not worth the effort to reverse engineer a complex system, which might even be designed with additional mechanisms in place to complicate reverse engineering.

In VANETs, the concept’s realization could mean communication protocols are kept secret amongst vehicle manufacturers and selected suppliers, but not made available to the public. Of course, this requires close cooperation between all parties concerned. With non-public communication protocols, for an external attacker (e.g. roadside attacker) it is more difficult to introduce and modify messages, since the protocols are not known to the attacker.

The concept realizes the restriction of network participation to selected vehicles with a rather low cost solution. The reduction in costs can be seen best, when comparing the concept to the certification approach as introduced previously. Certification results in higher setup costs and especially additional operational costs.

However, the main disadvantage of such a so called "security by obscurity" approach is, anyone that is capable and willing to spend enough money, research and time, will be able to acquire at least the basic protocol specifications by means of reverse engineering. And once the protocols are disclosed, anyone who is able to build or purchase the corresponding hardware, will be able to participate in the previously closed system. So, in order to represent an acceptable level of security, reverse engineering must come with a requirement of money to be spent, being unattractive for average users or the system needs to be protected by law. Another disadvantage is that the realization of the concept could result in a sub-optimal communication protocol design, due to the deployed mechanisms that aim at complicating reverse engineering.

Regarding the use in VANETs, this approach seems not promising. On the one hand this is due to the fact that vehicle manufacturers are aiming at the development of a common and open standard for the communication system. On the other hand VANETs are going to be large scale systems that will have to operate in a secure way for quite a long time, according to vehicle and vehicle equipment production cycles.

*2) Customized Hardware:* An alternative based on the same principles is the concept of customized hardware. Here the assumption is that communication protocols are publicly available but instead the required communication hardware is not.

This approach enables the same security as the one previously mentioned (closed communication system), but with the difference that the access restriction is based on non-available hardware instead of an undisclosed communication protocol. Likewise to the previous approach, building the required hardware for communication, must be expensive enough to be unattractive. There are a variety of possible realizations of the non-available hardware concept. One possibility would be communication devices based entirely on custom chips. Another realization might consist in a proprietary device design with standard chips, which can not be connected to a PC.

The application of this concept in VANETs suffers from the general problem of customized hardware design. Development and production costs increase drastically in case the hardware is not produced for the mass market (i.e. in large margins). Therefore the original idea to go for an 802.11 based physical layer in order to be able to use comparatively inexpensive hardware would not make sense any more. To resolve this issue a convenient solution could be to use standard ICs as planned, but with a customized HAL (hardware abstraction layer), which is not available to the public. This is done today for a couple of wireless network cards and open source Linux drivers.

So, in case the required hardware is not easily available for hackers and even if the attacker would be able to get hand on the required hardware, he wouldn't be able to use it with standard computers, like for instance a laptop.

The advantage of this approach is that it is better applicable in VANETs than the closed protocol concept, since the developing consortia aim at a publicly available standard. On the downside, customized hardware is more expensive, depending on if the customization is realized entirely in hardware, or as also proposed only with non-public hardware abstraction layer. Furthermore, again, the other disadvantage is that once there is a cheap solution available to access the communication system, for instance a software modification for another existing hardware (e.g. a standard WLAN card), the access restriction is gone.

Summarizing both approaches for proprietary system design, the concepts aim at rising the required effort an attacker has to spent in order to enter into the system. They do not prevent him from doing so, nor do they prevent any attack from an insider. For example, an attacker is still able to distribute fake warning messages using a vehicle's safety communication system.

### C. Tamper Resistant Hardware

As explained in the previous subsection, even when securing the external communication part of an active safety communication system, there is no guarantee that the system will be free from maliciously introduced fake warnings. An approach that aims a preventing such attacks over in-vehicle communication systems and in-vehicle devices is the usage of tamper-resistant hardware.

Tamper resistant in general means that something is resistant against tampering, independent of the type of access a person might have to the system. With respect to hardware, it means the device in question is difficult to be manipulated or exchanged by another device, without the system would take notice. The implementation of tamper resistance ranges from complicating access to device internals up to self-destruction of the device upon the detection of tampering attempts. Closely related are the following two terms, tamper proof and tamper evident. Tamper-proof is a more strict definition of tamper resistant, which claims to be $100\%$ secure against tampering, whereas tamper evident means that one is able to detect that a device has been tampered with.

For secure in-vehicle communication (e.g. reporting of sensor data to the warning system) tamper resistance means on the one hand, that the sensors and in-vehicle devices have to be secured, on the other hand also in-vehicle communication buses have to be protected. Furthermore, tamper resistant devices can provide secure storage for keys and certificates, and maybe even for a history of recent messages sent over the external communication system, like an event data recorder (EDR) for the VANET communication system, which could be used for legal purposes.

When properly applied, tamper-proof and tamper-resistant hardware enable secured in-vehicle communication and will

prevent most attacks on the active safety communication system from inside of the vehicle.

However, tamper proof hardware on its own will not be able to secure the external communication, so a combination, for example with signed and certified messages is still required in order to secure external communication. Additionally, manipulation of sensor input, e.g. putting a lighter in close proximity to a temperature sensor, will not be prevented nor detected. Likewise, attacks with GPS simulators (position and timing information) are still possible.

## V. Reactive Security Concepts

Due to the shortcomings of all proactive concepts as outlined in the previous section, there will be in any case a need for complementary reactive mechanisms to compensate for the open issues.

Reactive concepts comprise what is commonly known under the term intrusion detection. They have in common that they correlate information which is either already available from normal system operation, or which is introduced additionally. For intrusion detection systems in mobile ad hoc networks (MANETs), there are basically two methods this information is created and used for correlation. One possibility is signature based detection, the other anomaly based detection (see [12] and [13] for more details). Intrusion detection systems or similar systems for VANETs are still rarely explored (initial publications are [10] and [14]). These system comprise what is sometimes referred to as plausibility checks, information verification, use of side-channel information or context verification.

In VANETs, or more specifically for active safety systems in VANETs, reactive security mechanisms have to aim at detecting wrong information in warning messages and inconsistencies in the inter-vehicle communication system. In order to do so, upon the reception of warning messages, nodes evaluate the validity of the warnings and then process the messages accordingly. If the message content is found to be invalid, the nodes ignore the message (some systems even try to correct the invalid data) and may in addition communicate their estimation of validity of the warning in question to neighboring nodes. The following subsections discuss the applicability of the three mentioned concepts to this goal.

### A. Signature Based Detection

Signature based intrusion detection detects attacks on a system by comparing network traffic to known signatures of attacks. As soon as an attack is detected appropriate countermeasures can be initiated.

The primary interest of signature based detection is to realize a mechanism that is capable to detect known attacks on a communication system.

Signature based intrusion detection introduces a couple of requirements on the detection system. First, there is the requirement to be able to define attack signatures. Then, there has to be the ability to store and update attack signatures.

For VANETs, the idea is to describe simple attacks or misbehavior by signatures. Then, network traffic or received messages are compared to those signatures and malicious behavior is reported to a security system within the safety system. This security system would then have to decide how to react on the reported event.

Obviously, in VANETs this kind of detection is limited. The approach is restricted to information from the communication protocols, information from applications and especially their meaning can not be considered. Another aspect to consider are dynamics and unpredictable situations occurring in VANETs, making it hard to define attack signatures.

The advantages of signature based detection are that it can be realized with simple mechanism and that it normally provides reliable detection of known attacks. The disadvantages are the requirement for frequent updates of the attack signature database, the slow reaction on new attacks and of course the difficulty to define attack signatures.

### B. Anomaly Detection

Statistical anomaly detection is based on the assumption that there is a definition normal communication system behavior. Deviations from that behavior are statistically analyzed and as soon as they reach a defined level, the security system concludes that there is an attack ongoing.

Like signature based detection, the applicability of anomaly detection for active safety applications in VANETs is rather limited. Definition of normal system behavior based on network traffic does not allow to detect attacks on an active safety system.

The advantage of anomaly detection is that it enables the detection of previously unknown attacks without requiring an attack database to be updated. But, there are also several disadvantages. The definition of normal system behavior is rather complex and anomaly detection is known to produce many false positives.

### C. Context Verification

Context verification is an approach that specifically addresses the properties of VANETs and active safety applications in VANETs.

The idea is to collect as much information from any information source available. The collected data is used by every vehicle to create an independent view of its current status, its current surrounding (physical) environment and current or previous neighboring vehicles. The information sources are for example the warning system, data that is available from telemetric monitoring and data extracted from other VANET communication. Then, upon the reception of a warning message, the message (its content, origin, etc. ) is evaluated and compared to the vehicle's own estimation of the current situation, which results from the previously collected data.

In order to enable this comparison, there is a requirement for the definition of rule-sets that determine, what is to be expected with which probability in which situation. It is important to

note that obviously due to the time critical nature of a warning system, this comparison has to be done in near-real-time, otherwise the warning information would be useless.

Even data that is not specifically bound to warning messages or other applications can be used to execute plausibility verifications for the creation of the vehicle's own perception on its surroundings. An example would be the verification of position information in beacon messages, which is an application independent service provided by the network layer. Thus, the evaluation mechanisms are either application independent or application dependent. Furthermore there are mechanisms that work individually on every node and there are mechanisms that require cooperation with other nodes.

Application independent verification mechanisms comprise mainly mechanisms that evaluate data transmitted regularly, e.g. in beacons. Basically, this means position information and timing information (and derivable data such as speed or heading). The information learned through the beaconing process is compared to data received from other information sources (from the communication system point of view sometimes referred to as side-channel information) such as the vehicles positioning system (GPS) or other vehicle sensors.

Accordingly, application dependent plausibility evaluation relies on similar verifications but with respect to additional information from application message format fields and general knowledge on the respective applications. Here an example would be, that traffic jam warnings would normally be expected to originate from a node in direction towards the traffic jam, not from a position further away than the receiving node's own position.

*1) Position Information Verification:* Position verification in general aims at preventing malicious or defective nodes to pretend to be at arbitrary positions and triggering wrong safety messages or justifying to have "the right" to send a valid warning message for a certain region. Also malicious actions regarding position dependent routing should be detected, e.g. packet interception and packet dropping.

Greedy routing and most safety relevant applications for VANETs depend on reliable neighbor positions. Yet, the term "reliability" implies that a node cannot influence the position information given in beacons of neighboring nodes. Assuming all nodes working properly and no nodes trying to act maliciously, there is no reason for intervention. But effectively, neighbors may claim falsified positions and thereby can carry out several attacks, network operation related like node isolation or packet interception, but even more important also safety messaging related.

Position information verification is meant to contribute to what we refer to as neighborhood monitoring, i.e. mechanisms to detect any abnormal events or behavior in a node's direct neighborhood. This includes unusual increase in traffic density, two nodes being at the same position the same time, comparing consecutive position informations to maximum node velocity (in dependence from the current road scenario, highway vs city, if available for instance from a digital map), correlating node speed and node density (the higher the node speeds, the higher their distance normally should be).

*2) Time Verification:* Timing information based verification correlates the time data fields in beacon messages and other packets against the vehicle's internal clock (synchronized and updated using information provided by the GPS system).

The primary objective of time verification is to detect previously recorded and then replayed messages (replay protection).

Verifications with single packets in order to detect malicious or faulty behavior are possible with regard to the following aspects. A first step consists in comparing the message reception time to the message creation time stamp. This can give estimations if the message creation time is plausible or not, e.g. warning messages with time stamps considerably in the future should not occur. Likewise, messages that have been created a year ago, should not be circulated any more.

Time verification with several packets originating from a single node can provide additional insight on the nodes behavior (or on the fact another node is trying to impersonate this node). One approach is to compare time stamps in subsequent beacons, determining if the beacons are received in the right order. In combination with position information, time based plausibility checks for single nodes also leads towards vehicle speed related plausibility checking.

*3) Application Context Dependent Verification:* Application context dependent verification is based on the assumption that for every application, there is a set of constraints in the "real world", where the application is expected to deliver warning messages. If that assumption does not hold, at least the contents of a warning message that should be accepted as being valid, can be restricted by these constraints. Compared to application independent verification, the constraints are more precise, what in return makes verification more complex, more dependent on traffic situations and obviously more specific to message formats.

Furthermore, application dependent plausibility evaluation can benefit from information gathered by the application independent communication system. For instance, for most warning messages it is of crucial relevance where the message originates from, since normally this region should correlate with the position of the sending node and intermediate forwarding nodes. So if the verification system is able to detect that the sending node's (real) position significantly differs from this region, there is a high probability that there is something wrong in the system or with the warning message.

Additional information sources that could serve as input for application dependent verification could be the TMC system (for traffic jam warnings) or also records of previous encounters with certain nodes (the vehicle that overtook me, might send me warning for something that I might encounter soon).

An example scenario would be that an icy road warning is received and the vehicle's outdoor temperature sensor indicates +20 deg C. Now, the set of constraints defines that icy road warnings require a temperature below +5 deg C in order to be plausible. So in this case, the system has to decide which input to rely on, the internal sensor's value, or the information

obtained via the active safety communication system. In such a situation, further information from other in-vehicle systems, e.g. ABS or vehicle stability increasing systems (ESP), could help with the decision. For instance, if one of the systems had to intervene recently, this could be an indication that the temperature sensor might be defective and the warning valid.

Another example would be, that some warnings are only expected on a certain kind of roads. This is the case, e.g. when a motorist drives against the traffic on motorways, which is not applicable on normal roads, whereas drivers are allowed to use an opposite lane for overtaking there.

Application dependent verification that is based on position information gathered independently from the application could help for instance in the following situation. In dense fog an attacker informs another node, that he is in front of it (while actually, he is on the side) and has detected a hazard, what could make the other node stop or at least considerably slow down, resulting in potentially dangerous situations for other follow up nodes.

## VI. System Design

### A. Constraints

*Gradual Deployment:* Probably the most important constraint is that the communication system and all related or required services won't be deployed at once. In other words, deployment of VANET communication devices is a process that will most probably take several years until the network reaches a considerable density, which in turn enables high availability of most of the active safety features.

*Deployment Costs:* For vehicle manufacturers, this means that additional deployment cost, especially in the beginning, have to be as low as possible, since selling a system is impossible that is going to work in a couple of years from now. On the other hand, spending this money in advance on their own, probably won't pay off for the vehicle manufacturers either, or at least they're not willing to take the risk. Therefore, from the manufacturers' point of view, a strategy with successive deployment is required, including a simple and cheap market introduction strategy.

*Operational Costs:* Although technically seen an important solution to many security problems in VANETs as outlined in the previous section, usage of a permanently available online certification infrastructure is not desirable, due to deployment and operational cost. Operational costs can be separated into two factors. One factor is costs for providing access of vehicle systems to the certification infrastructure, i.e. the interconnection of the VANET and the certification infrastructure. The second factor is the costs for running the certification infrastructure as such, i.e. all costs not related to access, e.g. certificate generation and revocation.

Regarding access and related costs, there are several solutions with different costs and different cost-distributions.

*Road-side Infrastructure:* One of the visions comprises area-wide deployment of road-side access points (also called road side units) with permanent access to a backbone network (e.g. a dedicated roadside network backbone or the Internet). Whereas this solution provides optimal and permanent access, it requires tremendous capital expenditures by the provider, which makes it a rather implausible solution e.g. for PKI connectivity.

*Cellular Network:* Also imaginable would be solutions with permanent network / Internet access using cellular networks such as UMTS or GPRS. But this would require the vehicles to have implemented a corresponding (additional) communication module, as well as the vehicle owner to have a contract with cellular network provider and to pay the costs for data transfer, eventually including certificates or revocation lists.

*Regular Service Checks:* More adapted to the VANET scenario and the idea of a cost-effective solution, there will be either another mechanism that will determine that a message hast been sent by a legitimate node, or maybe a possibility to preload key material during (bi-)annual service checks (offline certification infrastructure).

*Certificate Infrastructure:* Even when using an offline certificate distribution system, which obviously would drastically reduce the distribution costs, there are still other issues. Independent of the realization of access to the certificate infrastructure, the cost for providing, maintaining and operating the required infrastructure for certification as such is not included. This is, what is known for example from certificate providers in the Internet today, a complex and cost intensive service, which is highly charged. In addition, the amount of certificates and the frequency they will have to be renewed can be assumed to be much higher in VANETs than for servers in the Internet.

*Certificate Provider Business Model:* Obviously, in contrary to other systems, where network operators provide their customers with free certificates if required, in VANETs certificates won't be provided for free, due to the fact that the primary usage scenarios for VANETs provide no business opportunities for key or certificate providers. Neither will be the vehicle holders be interested in paying for certificates, since in contrast to for instance a company for selling merchandise in the Internet using a SSL secured web-shop, the vehicle owner does not run a business.

*Cross-national Issues:* In addition, when thinking of key / certificate distribution for systems that have to work across different countries, especially in Europe, cross-national administration of such a system is still an unresolved issue. This is on the one hand due to the amount of management required to coordinate a pan-European system, and on the other hand due to legal issues, i.e. national laws concerning cryptography and national laws regarding certification.

*Large Scale PKI:* Last but not least, deployment and administration of a large scale PKI, which frequently issues large numbers of certificates, is a challenging task that has not been shown to be possible at all, so far.

*Tamper Resistant Devices:* Tamper resistant devices (which increase costs for the system) might be available for devices inside the car, however, they wouldn't solve problems resulting from the insecure external communication channel. Furthermore when looking at today's in-vehicle communication

architectures, bottom line is, that the deployed bus systems are not secured. Thus, an inter-vehicle communication system that would require all or most of in-vehicle communication (i.e. transport of sensor data) to be secured against in-vehicle attackers, solely for the purpose of inter-vehicle communication, is most likely the exclusion criterion. This is especially the case for existing in-vehicle devices that are known to work reliable and thus, are unlikely to be exchanged with new devices.

### B. Reasonable System Design

Reflecting the results from the previous sections, this section will give a direction towards what can been seen as a reasonable design for a security solution for active safety applications in VANETs.

As the section on proactive concepts has shown, there is no proactive or reactive concept that fulfills all of the security and system requirements alone. Neglecting the system design constraints, there would be the possibility of building a highly secure system. However, when taking into account the constraints, it is obvious that although some concepts provide important improvements to security, they are unlikely to become realized in the near future. Therefore, a combination of less secure mechanisms will probably have to suffice.

Given the current situation regarding deployed roadside infrastructure, certification systems and pan-European legal issues with certification, we suggest to deploy a system that does not rely on certificates. The system should be build with the idea in mind that it can be extended to support certificates in the future, for instance for the authentication of nodes with special properties such as police cars. But, currently we propose to restrict access to the communication system by means of customized hardware. Furthermore, we argue that reactive concepts, especially context verification, are the key security concepts that will secure active safety applications.

## VII. Conclusions

In this paper, we have elaborated on security issues in vehicular ad-hoc networks (VANETs) with special focus on active safety applications. We have provided an overview on solution concepts and evaluated requirements of corresponding mechanisms.

The main conclusion is that although some concepts can be viewed as strong solutions from a network point of view, they do not fit into the design constraints of VANETs. Therefore, less secure mechanisms will probably have to suffice.

Overall, we advocate a solution that is capable of dynamically adapting to different security setups, i.e. a solution that is for instance capable of handling both, vehicles with communication systems being certified by a trusted third party as well as vehicles that do not possess certificates. Independent of certification, we argue that context verification is one of the key security concepts that will secure active safety applications, due to the reasons outlined in this document.

In future research we will provide more details on the aforementioned concepts as well the definition of corresponding standards.

## References


[1] W. Franz, C. Wagner, C. Maihöfer, and H. Hartenstein, "FleetNet: Platform for Inter-Vehicle Communications," in *Procedings of 1st International Workshop on Intelligent Transportatin (WIT'04)*, Hamburg, Germany, Mar. 2004.

[2] NoW, "Network on Wheels," http://www.network-on-wheels.de, 2005. [Online]. Available: http://www.network-on-wheels.de

[3] C2C-CC, "Car2Car Communication Consortium," http://www.car-to-car.org/. [Online]. Available: http://www.car-to-car.org/

[4] VSCC, "US Vehicle Safety Communication Consortium," http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/CAMP3/pages/VSCC.htm. [Online]. Available: http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/CAMP3/pages/VSCC.htm

[5] VII, "Vehicle Infrastructure Integration," http://www.its.dot.gov/vii/.

[6] T. Leinmüller, L. Buttyan, J.-P. Hubaux, F. Kargl, R. Kroh, P. Papadimitratos, M. Raya, and E. Schoch, "Sevecom - secure vehicle communication," in *Proceedings of IST Mobile Summit 2006*, 2006. [Online]. Available: http://www.leinmueller.de/publications/

[7] J.-P. Hubaux, S. Čapkun, and J. Luo, "The Security and Privacy of Smart Vehicles," *IEEE Security and Privacy*, vol. 4, no. 3, pp. 49–55, 2004. [Online]. Available: http://lcawww.epfl.ch/Publications/luo/HubauxCL04.pdf

[8] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN'05)*, 2005. [Online]. Available: http://lcawww.epfl.ch/Publications/raya/RayaH05C.pdf

[9] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks," in *Proceedings of the Fourth Workshop on Hot Topics in Networks (HotNets-IV)*, Nov. 2005. [Online]. Available: http://www.ece.cmu.edu/~bparno/

[10] P. Golle, D. Greene, and J. Staddon, "Detecting and Correcting Malicious Data in VANETs," in *Proceedings of the First ACM Workshop on Vehicular Ad Hoc Networks (VANET)*. Philadelphia, USA: ACM Press, Oct. 2004. [Online]. Available: http://crypto.stanford.edu/~pgolle/papers/vanet.html

[11] P. Zheng, "Tradeoffs in certificate revocation schemes," *SIGCOMM Comput. Commun. Rev.*, vol. 33, no. 2, pp. 103–112, 2003. [Online]. Available: http://doi.acm.org/10.1145/956981.956991

[12] P. Brutch and C. Ko, "Challenges in Intrusion Detection for Wireless Ad-hoc Networks," in *Proceedings of the IEEE Workshop on Security and Assurance in Ad hoc Networks, in conjunction with the 2003 International Symposium on Applications and the Internet(SAINT'03 Workshops)*, Orlando, Florida, United States, 2003.

[13] Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion detection techniques for mobile wireless networks," *Wirel. Netw.*, vol. 9, no. 5, pp. 545–556, 2003. [Online]. Available: http://www-static.cc.gatech.edu/~yian/Zhang_03.pdf

[14] T. Leinmüller, A. Held, G. Schäfer, and A. Wolisz, "Intrusion Detection in VANETs," in *In proceedings of 12th IEEE International Conference on Network Protocols (ICNP 2004) Student Poster Session*, Oct. 2004. [Online]. Available: http://leinmueller.de/index.php/Main/Publications