The Security of Vehicular Ad Hoc Networks

Maxim Raya and Jean-Pierre Hubaux

Laboratory for computer Communications and Applications (LCA)
School of Computer and Communication Sciences
EPFL, Switzerland
{maxim.raya, jean-pierre.hubaux}@epfl.ch

ABSTRACT

Vehicular networks are likely to become the most relevant form of mobile ad hoc networks. In this paper, we address the security of these networks. We provide a detailed threat analysis and devise an appropriate security architecture. We also describe some major design decisions still to be made, which in some cases have more than mere technical implications. We provide a set of security protocols, we show that they protect privacy and we analyze their robustness, and we carry out a quantitative assessment of the proposed solution.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—Security and protection

General Terms

Design, Security

Keywords

vehicular ad hoc networks, security

1. INTRODUCTION

Until recently, road vehicles were the realm of mechanical engineers. But with the plummeting costs of electronic components and the permanent willingness of the manufacturers to increase road safety and to differentiate themselves from their competitors, vehicles are becoming "computers on wheels", or rather "computer networks on wheels". For example, a modern car typically contains several tens of interconnected processors; it usually has a central computer as well as an Event Data Recorder, reminiscent of the "black boxes" used in avionics. Optionally, it also has a GPS receiver, a navigation system, and one or several radars.

Manufacturers are about to make a quantum step in terms of vehicular IT, by letting vehicles communicate with each other and with roadside infrastructure; in this way, vehicles will dramatically increase their *awareness* of their environment, thereby increasing safety and optimizing traffic. Researchers have investigated many aspects of vehicular communications [7, 10, 13, 15, 16, 18, 22, 29, 32, 33, 34]. In the US, the FCC has allocated a bandwidth of 75MHz for these applications, usually referred to as DSRC (Dedicated Short Range Communications) [3]; similar initiatives are expected in other parts of the world. Significant progress has been made on the definition of the MAC and physical layer protocols; consensus is emerging around a customized version of IEEE 802.11.

Considering the tremendous benefits expected from vehicular communications and the huge number of vehicles (hundreds of millions worldwide), it is clear that vehicular communications are likely to become the most relevant realization of mobile ad hoc networks. The appropriate integration of on-board computers and positioning devices, such as GPS receivers along with communication capabilities, open tremendous business opportunities, but also raise formidable research challenges.

One of these challenges is security; very little attention [7, 15, 18, 34] has been devoted so far to the security of vehicular networks. Yet, security is crucial. For example, it is essential to make sure that life-critical information cannot be inserted or modified by an attacker; likewise, the system should be able to help establish the liability of drivers; but at the same time, it should protect as far as possible the privacy of the drivers and passengers.

These concerns may look similar to those encountered in other communication networks, but they are not. Indeed, the size of the network, the speed of the vehicles, the relevance of their geographic position, the very sporadic connectivity between them, and the unavoidably slow deployment make the problem very novel and challenging. The purpose of this paper is to bring a first response to this challenge.

The paper is organized in the following way. In Section 2, we present the state of the art. In Section 3 we describe the system model that we subsequently use to provide a threat analysis in Section 4 and the corresponding solutions in Section 5. In Section 6 we analyze the security of the proposed protocols and in Section 7 we address implementation issues. Finally, in Section 8 we discuss related issues and Section 9 concludes the paper.

2. STATE OF THE ART

VANETs (Vehicular Ad-hoc NETworks) are an emerging research area. Currently, most of the research is focused on

SASN'05, November 7, 2005, Alexandria, Virginia, USA.

the development of a suitable MAC layer, as well as potential applications ranging from collision avoidance to onboard infotainment services. But both academics and the industry have so far largely overlooked the subject of security in VANETs, postponing it to later phases of research and development.

In fact, there are very few academic publications describing the security architecture of VANETs [7, 18, 34]; none of them proposes specific protocols or considers practical issues such as key sizes and authentication delays. The use of digital signatures in the vehicular environment is discussed in [15]. Software frameworks for telematics are proposed in [10, 11]. Some recent papers [16] focus on particular subjects in vehicular security without defining the big picture where the proposed solutions would fit. Very related to VANET security is the security of the electronic systems in a vehicle that are actually responsible for transporting or generating the data before it is sent. A security architecture based on a PKI for digital tachograph[1] systems is proposed in [14]. The security problems of automotive bus systems are pinpointed in [31].

The most prominent industrial effort in this domain is carried out by the Car 2 Car Communication Consortium [1] and several projects such as NOW [2] in Europe, and the DSRC [3] consortium, especially the IEEE P1556 Working Group (Security and Privacy of Vehicle and Roadside Communications including Smart Card Communications), in the USA.

Some commercial products already make use of vehicular communication without taking the security aspect into account. For example, insurance companies install black boxes (similar to the Event Data Recorders in this paper) in cars to collect their usage data (e.g., travelled distance) and to calculate insurance costs accordingly. Another related application is GPS car tracking (discussed in Section 8).

3. SYSTEM MODEL

In this section, we present the distinguishing properties of VANETs (Fig. 1) in order to shape later the problem statement. Further, we describe a basic safety messaging protocol to be used as a reference in later sections.

3.1 System assumptions

To be future-compatible, the following assumptions are based mainly on specifications of upcoming products.

3.1.1 Network model

The communicating nodes in VANETs are either vehicles or base stations. Vehicles can be private (belonging to individuals or private companies) or public (i.e., public transportation means, e.g., buses, and public services such as police cars). Base stations can belong to the government or to private service providers. We assume a communication channel supported by an IEEE 802.11-like technology.

Given that the majority of the network nodes will consist of vehicles, the network dynamics will be characterized by quasi-permanent mobility, high speeds, and (in most cases) very short connection times between neighbors (e.g., in the case of crossing vehicles). For example, on highways vehicle speeds are usually higher than 80km/h (with relative speeds

[1]A tachograph is a device used to record the speed and duration of trips in a motor vehicle.

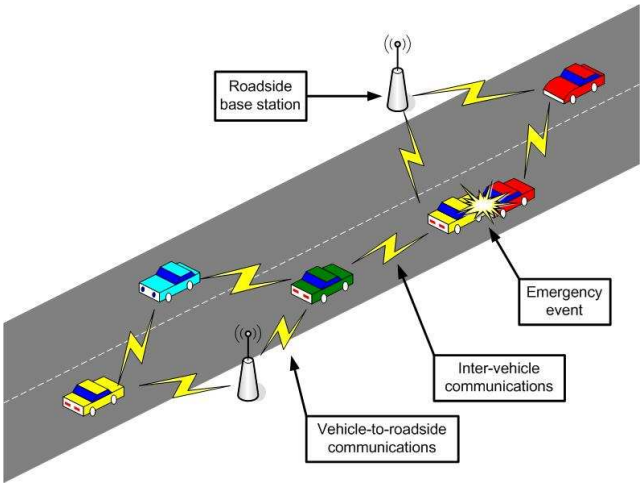


Figure 1: A VANET consists of vehicles and roadside base stations that exchange primarily safety messages to give the drivers the time to react to life-endangering events.

equal to twice these values), and in some countries (e.g., Germany) are not even upper bounded. Another aspect of network dynamics is that vehicle trajectories are mostly well defined by the roads, which incurs some advantages (for message dissemination) and disadvantages (for privacy).

The scale of VANETs is another feature that sets them apart. With hundreds of millions of nodes distributed everywhere, VANETs are likely to be the largest real-world mobile ad hoc network. But communication in this network will be mainly local, thus partitioning the network and making it scalable.

An advantage of VANETs over "usual" ad hoc networks is that vehicles provide relatively sufficient computational and power resources, especially taking into account Moore's law and the related improvement of computing platforms in the next few years. As mentioned in the Introduction, a typical vehicle in a VANET will host several tens or even hundreds of microprocessors, an EDR (*Event Data Recorder*) that can be used for crash reconstruction, and a GPS (*Global Positioning System*) receiver (or a similar system, such as Differential GPS or Galileo) that will provide position and a clock. It should be noted that the existence of a GPS-like device is not mandatory for supporting security in VANETs; we will describe alternative options.

VANETs are expected to be deployed over the next decade to achieve considerable penetration only around 2014 [23, 25]. Nevertheless, the network should become partially operational with the release of the first products, i.e., in the next couple of years. This means that the basic functions of VANETs and the related security mechanisms should be available even with low market penetration, and especially without relying on the existence of an infrastructure (which will take a longer time to deploy due to administrative and installation costs).

3.1.2 Application categories

There are many applications envisioned for VANETs, most of which are proposed by the vehicle manufacturers. Al-

Table 1: Message classes and properties

Class\Property	Legitimacy	Privacy protection		Real-time constraints
		Against other individuals	Against the police	
Traffic information	✓	✓	✓	
General safety messages	✓	✓	✓	✓
Liability-related messages	✓	✓		✓

though the spectrum of these applications is very wide ranging (from the realistic to the futuristic) [3], we have divided the applications into two major categories:

1. Safety-related applications, such as collision avoidance, cooperative driving, and traffic optimization. The common characteristic of this category is the relevance to life-critical situations where the existence or lack of a service may affect life-endangering accidents. Hence the security of this category is mandatory, since the proper operation of any of these applications should be guaranteed regardless of the presence of security threats.

2. Other applications, including payment services (e.g., toll collection), location-based services (e.g., finding the closest fuel station), infotainment (e.g., Internet access). Obviously, security is also required in this application category, especially in the case of payment services. But in this paper we address the security aspects of safety-related applications because they are the most specific to the automotive domain and because they raise the most challenging problems.

3.1.3 Safety messages

As explained in the previous section, we consider only public safety applications. In this context, we can classify the safety messages into three classes, based on their properties related to privacy and real-time constraints, as shown in Table 1. *Traffic information* messages are used to disseminate traffic conditions in a given region and thus affect public safety only indirectly (by preventing potential accidents due to congestion); hence they are not time-critical. *General safety-related* messages are used by public safety applications such as cooperative driving and collision avoidance and hence should satisfy stringent constraints such as an upper bound on the delivery delay. *Liability-related* messages are distinguished from the previous class because they are exchanged in liability-related situations such as accidents. Therefore, the liability of the message originator should be determined by revealing his identity to the law enforcement authorities. This classification of messages will be useful later in describing the attacks on VANETs.

A common property of all the message classes is that they are broadcast and mainly standalone (i.e., there is no content dependency among them like in media streams). The content of a typical safety message includes position, speed, direction, and acceleration of the vehicle, in addition to data specific to traffic events (e.g., congestion notification or accident). If the sender faces an abnormal situation (e.g., an accident), these data help receivers compute their positions with respect to the sender and determine if they are in danger. The message does not necessarily contain explicit ID information.

An important feature of ad hoc networks is multihopping. But according to the DSRC specifications and because of their broadcast nature, safety messages are transmitted over a single-hop with a sufficient power to warn vehicles in a range of 10 seconds travel time, thus eliminating the need for multihop. Nevertheless, some form of multihop still exists: vehicles that receive warning messages estimate whether the reported problems can also affect their followers; in this case, they forward the message to them.

3.1.4 Trust

A key element in a security system is trust. This is particularly emphasized in vehicular networks because of the high liability required from safety applications and consequently the nodes running these applications. Due to the large number of independent network members (i.e., they do not belong to the same organization) and the presence of the human factor, it is highly probable that misbehavior will arise. In addition, consumers are becoming increasingly concerned about their privacy. Drivers do not make an exception, especially because the lack of privacy and the related potential of tracking may result in high financial charges on the drivers (e.g., due to occasional overspeeding). As a result, we assume a low level of trust in vehicles, as well as service provider base stations. Beside drivers and service providers, there will be a considerable presence of governmental authorities in VANETs. But due to the reasons stated above, trust in any of these authorities will be only partial (e.g., a given police officer may abuse his authority if given full trust). To gain full trust, several authorities will have to cooperate as will be sketched in Section 5.

3.2 Basic safety messaging protocol

Because the research on VANETs and their applications is still in its beginnings, there are few papers in the literature that describe protocols for safety messaging [32, 33]. To better describe the security solutions introduced in this paper, we describe in the following a simple protocol inspired from [33] for safety messaging to use as an example reference in later sections.

- In compliance with the DSRC specifications [3], we assume that each vehicle V periodically sends messages over a single hop every 300 ms within a range of 10 s travel time (the minimum range is 110 m and the maximum is 300 m).

- The inter-message interval drops to 100 ms and the range to 15 m if the vehicles are very slow or stopped (i.e., their speed is less than 10 miles/h or $\approx$ 16 km/h).

- Vehicles take decisions based on the received messages and may transmit new ones. For example, if V receives an emergency warning from another vehicle W and,

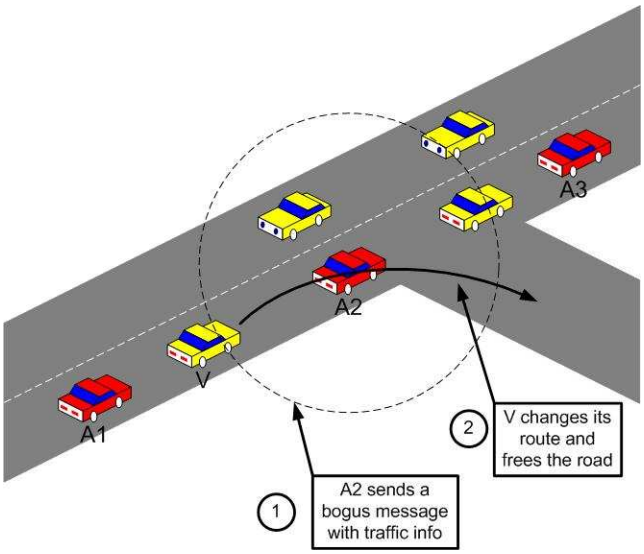


Figure 2: In this example *bogus information* attack, colluding attackers (A2 and A3) disseminate false information to affect the decisions of other vehicles (V) and thus clear the way of attacker A1.

based on their mutual positions, estimates that it is also in danger, it sends out its own warning messages.

4. ATTACKS ON VEHICULAR NETWORKS

In this section we describe the security threats facing vehicular networks. Since we cannot envision all the possible attacks that will be mounted in the future on VANETs, we will provide a general classification of attacks substantiated by a list of attacks that we have identified so far. But before describing the attacks, it is important to define the attacker, which we do in the following section.

4.1 Attacker's model

To classify the capacities of an attacker, we have defined three dimensions:

1. *Insider* vs. *Outsider*. The insider is an authenticated member of the network that can communicate with other members. As will be explained later, this means that he possesses a certified public key. The outsider is considered by the network members as an intruder and hence is limited in the diversity of attacks he can mount (especially by misusing network-specific protocols).

2. *Malicious* vs. *Rational*. A malicious attacker seeks no personal benefits from the attacks and aims to harm the members or the functionality of the network. Hence, he may employ any means disregarding corresponding costs and consequences. On the contrary, a rational attacker seeks personal profit and hence is more predictable in terms of the attack means and the attack target.

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

Inspired by the model in [17] we characterize an attacker by the tuple *Membership.Motivation.Method* where *Membership* stands for *Insider* (I_m) or *Outsider* (O_n), *Motivation* for *Malicious* (M) or *Rational* (R), and *Method* for *Active* (A) or *Passive* (P); m and n indicate the numbers of I and O nodes that the attacker controls, respectively. These two numbers also cover the notion of collusion. For example, an attacker $I_2.R.A$ controls two networks members, behaves rationally, and mounts active attacks. A star ("*") indicates that the corresponding field can take any value.

4.2 Specific attacks

As this paper is concerned with vehicular *networks*, we consider only the attacks perpetrated against messages rather than the vehicles, as the physical security of vehicle electronics (e.g., against hardware tampering) is out of the scope of this paper.

1. *Bogus information* (Fig. 2): Attackers are $I_m.R.A$ (m indicates any positive integer) and diffuse wrong information in the network to affect the behavior of other drivers (e.g., to divert traffic from a given road and thus free it for themselves).

2. *Cheating with positioning information*: Attackers in this case are also $I_m.R.A$, and use this attack to alter their perceived position, speed, direction, etc. in order to escape liability, notably in the case of an accident. In the worst case, colluding attackers can clone each other, but this would require retrieving the security material (which should be stored in tamper-proof hardware as discussed in Section 5.3) and having full trust between the attackers.

3. *ID disclosure* of other vehicles in order to track their location. This is the Big Brother scenario, where a global observer can monitor trajectories of targeted vehicles and use this data for a range of purposes (e.g., the way some car rental companies track their own cars). To monitor, the global observer can leverage on the roadside infrastructure or the vehicles around its target (e.g., by using a virus that infects neighbors of the target and collects the required data). The attacker is passive. We assume that the attacker does not make use of cameras, physical pursuit, or onboard tracking devices to uncover the identity of his target; otherwise, the tracking problem becomes simpler but also more expensive and tied to few specific targets, and it can be done anyhow based on existing license plates. In addition, we assume that physical-layer attacks (e.g., using radio fingerprinting [27]) are solved by appropriate physical layer techniques such as radio transmitters that randomize fingerprints.

4. *Denial of Service*: The attacker is $*.M.A$ and may want to bring down the VANET or even cause an accident. Example attacks include channel jamming and aggressive injection of dummy messages.

5. *Masquerade*: The attacker actively pretends to be another vehicle by using false identities and can be motivated by malicious or rational objectives.

5. HOW TO SECURE VANETS

In the next sections, we propose a set of security solutions to be deployed in vehicular networks. We attempt to consider all the possible options but take into account both the current state of the art and the long-term viability of these networks.

5.1 Requirements

A security system for safety messaging in a VANET should satisfy the following requirements:

- *Authentication*: Vehicle reactions to events should be based on legitimate messages (i.e., generated by legitimate senders). Therefore we need to authenticate the senders of these messages.

- *Verification of data consistency*: The legitimacy of messages also encompasses their consistency with similar ones (those generated in close space and time), because the sender can be legitimate while the message contains false data.

- *Availability*: Even assuming a robust communication channel, some attacks (e.g., DoS by jamming) can bring down the network. Therefore, availability should be also supported by alternative means.

- *Non-repudiation*: Drivers causing accidents should be reliably identified; a sender should not be able to deny the transmission of a message (it may be crucial for investigation to determine the correct sequence and content of messages exchanged before the accident).

- *Privacy*: People are increasingly wary of Big Brother enabling technologies. Hence, the privacy of drivers against unauthorized observers should be guaranteed.

- *Real-time constraints*: At the very high speeds typical in VANETs, strict time constraints should be respected.

5.2 Digital signatures as a building block

As emphasized in Section 5.1, message legitimacy is mandatory to protect VANETs from outsiders, as well as misbehaving insiders. But since safety messages will not contain any sensitive information (Section 3.1.3 describes the contents of a typical message), confidentiality is not required. As a result, the exchange of safety messages in a VANET needs authentication but not encryption.

Symmetric authentication mechanisms usually induce less overhead per message (not counting the handshake needed to establish a shared key) than their asymmetric counterparts. But digital signatures are a better choice in the VANET setting, because safety messages are typically standalone, as mentioned in Section 3.1.3 and should be sent to receivers as fast as possible. In fact, a preliminary handshake is not acceptable and actually creates more overhead. In addition, given the huge amount of network members and the sporadic connectivity to authentication servers, a PKI (Public Key Infrastructure) is the most suitable way for implementing authentication.

5.2.1 Securing messages

Under the PKI solution, each vehicle will be assigned a public/private key pair (we will elaborate more on the nature of these keys in the next section). Before a vehicle sends a safety message, it signs it[2] with its private key and includes the CA's (Certification Authority, discussed in 5.4.3) certificate as follows:

$$V \rightarrow * : M, Sig_{PrK_V}[M|T], Cert_V$$

where V designates the sending vehicle, $*$ represents all the message receivers, M is the message, $|$ is the concatenation operator, and T is the timestamp to ensure message freshness (it can be obtained from the security device introduced in Section 5.3). It should be noted that using nonces instead of timestamps is not desirable because of the burden of the inherent preliminary handshake where the communicating parties exchange the nonces; using sequence numbers also incurs overhead as they need to be maintained. $Cert_V$ is the public key certificate of V and will be described later.

The receivers of the message have to extract and verify the public key of V using the certificate and then verify V's signature using its certified public key. In order to do this, the receiver should have the public key of the CA, which can be preloaded as described below.

If the message is sent in an emergency context, which means that it belongs to the *liability-related* class, this message should be stored (including the signature and the certificate) in the EDR for further potential investigations in the emergency.

5.3 Tamper-proof device

The use of secret information such as private keys incurs the need for a tamper-proof device in each vehicle. In addition to storing the secret information, this device will be also responsible for signing outgoing messages. To reduce the risk of its compromise by attackers, the device should have its own battery, which can be recharged from the vehicle, and clock, which can be securely resynchronized, when passing by a trusted roadside base station. The access to this device should be restricted to authorized people. For example, cryptographic keys can be renewed at the periodic technical checkup of the vehicle. Several commercial products have these features, e.g., [6].

5.4 Key management

We will address below the issues of cryptographic key distribution, certification, and revocation.

5.4.1 Cryptographic information types

To be part of a VANET, each vehicle has to store the following cryptographic information:

1. An electronic identity called an *Electronic License Plate* (*ELP*) [18] issued by a government, or alternatively an *Electronic Chassis Number* (*ECN*) issued by the vehicle manufacturer. These identities (further referred to simply by ELP) should be unique and cryptographically verifiable (this can be achieved by attaching a certificate issued by the CA to the identity) in order to identify vehicles to the police in case this is required (usually, identities are hidden from the police). Similarly to the physical license plates, the ELP should be

[2]The message is actually hashed before being signed.

changed (i.e., reloaded in the vehicle) when the owner changes or moves, e.g., to a different region or country.

2. *Anonymous key pairs* that are used to preserve privacy. An *anonymous key pair* is a public/private key pair that is authenticated by the CA but contains neither information about nor public relationship with (i.e., this relationship cannot be discovered by an observer without a special authorization) the actual identity of the vehicle (i.e., its ELP). Yet this anonymity is conditional for liability purposes as will be explained later. Normally, a vehicle will possess a set of anonymous keys to prevent tracking.

5.4.2 Key bootstrapping and rekeying

Since the ELP is the electronic equivalent of the physical license plate, it should be "installed" in the vehicle using a similar procedure, which means that the governmental transportation authority will preload the ELP at the time of vehicle registration (in the case of the ECN, the manufacturer is responsible for its installation at production time).

Anonymous keys are preloaded by the transportation authority or the manufacturer, but with different consequences as discussed in the next section. Moreover, while ELPs are fixed and should accompany the vehicle for a long duration (potentially its life cycle), anonymous key sets have to be periodically renewed after all the keys have been used or their lifetimes have expired. This renewal can be done during the periodic vehicle checkup (typically yearly) or by similar procedures.

In addition to the ELP and anonymous keys, each vehicle should be preloaded with the CA's public key.

5.4.3 Key certification

Certification Authorities (CA) will be responsible for issuing key certificates to vehicles. Two solutions can be envisioned:

1. *Governmental transportation authorities*: Vehicles will be registered in different countries by the corresponding transportation authorities (which are usually regional). The advantage of this option is that the certification procedure will be under the direct control of the concerned authority. Although the ELP and keys of each vehicle are certified by a regional authority in a given country, vehicles from different regions or countries should be able to authenticate each other. This problem is usually solved by including the certificate chain leading to a common authority, but in the case of VANETs this would tremendously increase the message overhead. This certificate chain can be replaced by a single certificate by making the CA of the travelling vehicle's transit or destination region re-certify the ELP and the anonymous keys of the vehicle after verifying them with the public key of the CA that registered the vehicle. This requires the installation of base stations at the region borders.

2. *Vehicle manufacturers*: Certificates can also be issued by vehicle manufacturers, given their limited number and the trust already endowed in them. The advantage of this approach is reduced overhead. In fact, each vehicle will need to store a small number of manufacturer public keys in order to be able to verify any other vehicle it encounters, which is not the case if the CA is a local authority. The disadvantage is that non-governmental institutions will be involved in law-enforcement mechanisms.

For example, assuming keys are certified by a certain CA, a certificate $Cert_V[PuK_i]$ of the i^{th} anonymous key PuK_i of a vehicle V should include at least the following:

$$Cert_V[PuK_i] = PuK_i | Sig_{PrK_{CA}}[PuK_i | ID_{CA}]$$

where PrK_{CA} is CA's private key and ID_{CA} is the unique ID of CA.

5.4.4 Key revocation

We consider two key revocation scenarios, depending on the information compromised by the attacker:

1. All the cryptographic material belonging to a vehicle is compromised. To avoid the overhead of revoking all the keys of this vehicle, the CA will revoke them by sending secure revocation messages to the tamper-proof device.

2. A particular key of a vehicle's key set is compromised. In this case, sending a revocation message to the tamper-proof device for each revoked key would cause a large overhead. There are many other key revocation options in the literature [35], but they either require permanent online connectivity to the CA or are not suitable for the vehicular environment. Therefore, we opt for using *short key certificate lifetimes* that will make key certificates expire, thus revoking the keys. Using this approach requires large storage space on the vehicles, because keys should be frequently replaced by new ones. Although this would be a problem for resource constrained scenarios, vehicles are resourceful enough to satisfy this requirement. We will illustrate this with numerical examples in Section 7.1.

5.5 Anonymous public keys

There are several types of privacy. As safety messages will not contain any secret data about their senders, vehicle owners will be only concerned about identity and location privacy. To respond to these concerns, we propose the use of anonymous public keys that we detail in this section.

5.5.1 Identity and location privacy

Even though anonymous keys do not contain any publicly known relationship to the true identity of the key holders, privacy can still be hijacked by logging the messages containing a given key and thus tracking the sender until discovering his identity (e.g., by associating him with his place of living).

Therefore, anonymous keys should be changed in such a way that a pervasive observer cannot track the owner of the keys. The downside of this approach is that a vehicle will have to store a large key and certificate set (depending on the key changing frequency). In Section 6.2 we will propose a variable-frequency key changing algorithm that can preserve privacy and minimizes the key storage space.

5.5.2 Conditional anonymity

Privacy preservation is a requirement for deploying vehicular safety applications. But safety and the implied liability

requirement have higher priority. Hence, anonymity should be conditional on the scenario (e.g., if there are issues of law enforcement or national security, anonymity should be overriden). But if police (or other law enforcement entities) are given full control over the ID disclosure process, abuse can occur. Hence, the ID disclosure capability should be distributed among multiple authorities (in the same way it is done with other legal issues, such as bank account disclosure). For example, police should not be able to retrieve the identity corresponding to an anonymous key without the permission of a judge. Secret sharing [26] can be used to technically reinforce the distribution of authorizing material among authorities, whereby authorities share the secret needed to access the database that matches true vehicle identities (ELPs) with the set of their anonymous public keys. The subject of anonymity revocation is also explored in [19].

5.6 Authenticated session establishment

It is common practice in networks that two nodes establish a shared session key if they need to securely communicate for a long time. In fact, symmetric cryptographic primitives are more efficient (in terms of time and space overhead) than the asymmetric ones. In the context of vehicular networks, as the trust level is equal for all legitimate certificate-holding vehicles (because the certificate verifier actually trusts the CA that issued this certificate), the creation of secure groups (with a secret group key) in the network is not justified. In addition, these groups would lose the non-repudiation property (which means that in the case of a platoon[3], an example of VANET groups, the author of an accident would not be identifiable). In the case of broadcast messages, a set of approaches to improve the efficiency of authentication were proposed in [24], but none of these protocols can simultaneously satisfy the non-repudiation and upper delay bound constraints for standalone messages. As a result, safety message authentication is better done by digitally signing each message.

5.7 DoS resilience

DoS attacks are the nightmare of security experts, since they are mounted with no rational purpose and hence are very difficult to prevent, especially in a wireless medium.

To mitigate these attacks, we propose switching between different channels or even communication technologies (e.g., DSRC, UTRA-TDD, or even Bluetooth for very short ranges), if they are available, when one of them (typically DSRC) is brought down. In the worst-case scenario (i.e., when no means of communication between vehicles exist), the VANET enhanced features (e.g., collision avoidance) should automatically turn off to avoid problems until the network is reestablished. In fact, this is likely to be the default option in the early days of VANETs, when only a few vehicles will have the necessary technology.

5.8 Verification by correlation

In the *bogus information* attack, one or several legitimate members of the network send out false information to misguide other vehicles about traffic conditions. To cope with such misbehavior, data received from a given source should be verified by correlating them with those received from other sources. This is typically done by reputation-based systems, although it is important to stress here that what matters is the rating of the correctness of the data rather than its source (due to high mobility, neighborhood membership will change too fast to allow for the building of the reputation of each member), e.g., using an approach similar to [16].

[3]A group of vehicles that allows many cars to accelerate or brake simultaneously to increase road capacity without building additional traffic lanes.

6. SECURITY ANALYSIS

In the following we analyze how the previously proposed solutions address the requirements stated in Section 5.1.

6.1 Compliance with the security requirements

Authentication of message legitimacy is provided by the digital signature of the sender and the corresponding CA certificate. The only guarantee that this provides is that the message comes from a vehicle that was trusted, at least when the keys were issued. Nevertheless, these mechanisms ensure that outsiders are not able to send messages to network members. Verification by correlation (Section 5.8) and fast key revocation increase this guarantee, even though it cannot be complete because of the specific functionality of a given correlation algorithm and the vulnerability window of lifetime-based key revocation schemes.

Availability can never be totally guaranteed. Yet, the ways in which an attacker can disrupt the network service are limited: outsiders can only mount jamming attacks. Even in this case, channel or communication technology switching (Section 5.7) can reduce the impact of such attacks.

Non-repudiation is achieved as follows:

- Vehicles cannot claim to be other vehicles (*masquerade* attack) since they interact only with their anonymous public keys. ELPs cannot be forged because they are unique and verifiable.
- Vehicles cannot cheat about their position and related parameters if a secure positioning solution is used (Section 8).
- A vehicle cannot deny having sent a message because it is signed by an anonymous key that belongs exclusively to the sender; likewise, the vehicle cannot claim that the message was replayed because a timestamp is included in each message.

The satisfaction of the privacy requirement is addressed in the next section and the real-time constraints are analyzed in Section 7.

6.2 Anonymity

In order to preserve the driver's anonymity and minimize the storage costs of public keys, we propose a key changing algorithm that adapts to the vehicle speed and takes into account key correlation by the attacker as described below.

Let us consider the typical tracking scenario where the attacker controls stationary base stations separated by a distance d_{att} and captures all the received safety messages; he can later use these data (including the public keys) to illegally track vehicles. In addition, we assume that the attacker can correlate two keys if the sender moves at a constant speed in the same direction and on the same lane

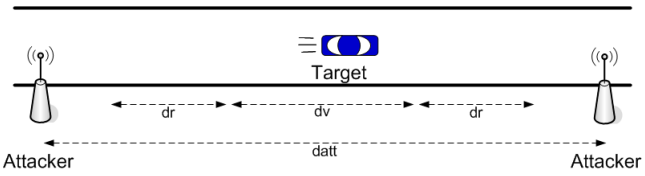


Figure 3: To uncover the identity of its targets, the attacker leverages on key correlation and the target's transmission range.

between two observation points (e.g., given the initial position of the target the attacker can predict its position in the future and confirm this prediction if a message is received at the next observation point with correct predicted speed and position). It should be noted that the following algorithm and analysis apply when there are at least two neighboring targets under observation; otherwise, the tracking of a single target becomes trivial despite the usage of any anonymity measures.

Assume the speed of target V is v_t, its transmission range is d_r, and d_v is the distance over which a vehicle does not change its speed and lane (the vulnerability window with respect to the correlation of keys). As Fig. 3 illustrates, the vehicle's anonymity is vulnerable over a distance equal to $d_v + 2d_r$. This means that it is not worth changing the key over smaller distances because an observer can correlate keys with high probability. This defines the lower bound on the key changing interval T_{key}:

$$min(T_{key}) = \frac{d_v + 2d_r}{v_t} \text{seconds} \quad (1)$$

But if $d_{att} > d_v + 2d_r$, V can avoid being tracked (by changing its key) as long as it does not use the same key for a distance equal to or longer than d_{att}. This in turn defines the upper bound on the key changing interval:

$$max(T_{key}) = \frac{d_{att}}{v_t} \text{seconds} \quad (2)$$

Since V does not know d_{att}, but knows d_r and d_v, it can choose a value of T_{key} that is a little larger than $min(T_{key})$. If we denote by r_m the message rate, one key should be used for at most:

$$N_{msg} = \lceil r_m \times T_{key} \rceil \text{messages} \quad (3)$$

For example, assume $d_{att} = 2$ km, $r_m = 3.33$ msg/sec (1 message every 300 ms), $d_v = 30$ sec $\times v_t$ (i.e., V does not change its lane and speed over 30 sec), $d_r = 10$ sec $\times v_t$ (according to DSRC, the transmission range is equal to the distance travelled in 10sec at the current speed), and $v_t = 100$ km/h. Then $min(T_{key}) = 50$ seconds and $max(T_{key}) = 72$ seconds. V can choose T_{key} to be 55 seconds; as a result, $N_{msg} = 184$ messages.

7. IMPLEMENTATION ISSUES

7.1 Certificate lifetime and key set size

On one hand, the *anonymous key set size* should be small to reduce storage space on vehicles. On the other hand, the *certificate lifetime* should be short to reduce the vulnerability window of the system if an anonymous public/private key pair is compromised. Hence a tradeoff must be made between the two.

7.1.1 Certificate lifetime

Each anonymous key should be used only with a sequence of consecutive messages as described in Section 6.2, otherwise a global attacker can extract information if a key is reused, even on different days. The lifetime of certificates should be short, around one day, to limit in time the effects of key compromise. But the driving duration changes from day to day (e.g., a long trip on vacation compared to daily home-work-home trajectory), hence on some days a larger number of keys may be required. To account for this, the lifetime of a key certificate should be stretched over several days (this is distinct from the usage duration of a key, which is only several seconds and aims at protecting the privacy of the key holder).

7.1.2 Anonymous key set size

Leveraging on the analysis in Section 6.2, a vehicle should change its anonymous key only after having used it for a certain number of messages. Reusing the example in 6.2, a vehicle should change its key within an interval of around 1 min. If we assume that an average driver uses his car 2 hours per day, the number of required keys per year is approximately 43800, which amounts to around 21 Mbytes (assuming a storage space of 500 bytes per key, including its certificate). To reduce the key storage space for governmental transportation authorities, anonymous keys can be derived from a master key shared between an authority and the vehicle corresponding to the keys. When verifying vehicle identities in liability-related situations, the keys can be regenerated using the master key.

7.2 Estimation of the signature size

As we propose using a PKI for supporting security in VANETs, it is important to choose a Public Key Cryptosystem (PKCS) with an acceptable implementation overhead in the vehicular context. According to DSRC, safety-related messages are sent with a periodicity of 100 to 300 ms. This imposes an upper bound on the processing time overhead; this overhead is given as follows:

$$T_{oh}(M) = T_{sign}(M) + T_{tx}(M|Sig_{PrK_V}[M]) + T_{verify}(M)$$

where $T_{sign}(M)$, $T_{tx}(M)$, and $T_{verify}(M)$ are the necessary durations to sign, transmit, and verify a message M, respectively; $Sig_{PrK_V}[M]$ is the signature of M by the sending vehicle V and includes the CA's certificate of the signing key. The above expression reveals the two factors that affect the choice of a particular PKCS: (1) the execution speeds of the signature generation and the verification operations, and (2) the key, signature, and certificate sizes.

Since the typical size of safety messages is between 100 and 200 bytes [32, 33], and the message is hashed before being signed, the overhead is almost constant for a given PKCS. Hence, it is possible to compare different options at least relatively to each other (because the actual performance varies with the platform, implementation, and version of the algorithm).

In fact, there are several candidate PKCS (we consider only the currently standardized systems) for implementing the PKI in a VANET. To assure the future security of the cryptographic material, and taking into account the deploy-

Table 2: Size and transmission time of PKCS

PKCS	Sig size (bytes)	$T_{tx}(Sig)$ (ms)
RSA	256	0.171
ECDSA	28	0.019
NTRU	197	0.131

Table 3: Comparison of signature generation and verification times on a memory-constrained Pentium II 400 Mhz workstation

PKCS	Generation (ms)	Verification (ms)
ECDSA	3.255	7.617
NTRU	1.587	1.488

ment schedule of VANET technology, we assume a security level at least equivalent to RSA 2048 according to the figures provided by [21] (which is supposed to survive until 2030 [5]) and we list figures for public key and signature sizes [4]:

1. RSA Sign: the key and signature sizes are large (256 bytes).
2. ECC (Elliptic Curve Cryptography): it is more compact than RSA (28 bytes), faster in signing but slower in verification.
3. NTRUSign[4] [4]: the key size is between the two above (197 bytes), but it is much faster than the others in both signing and verification.

Given that in DSRC the minimal data rate is 6 Mbps (for safety messaging it is typically 12 Mbps), the transmission overhead (at 12 Mbps) is acceptable in each of the above options, as shown in Table 2.

Table 3 gives approximative execution times of signature generation and verification for ECDSA (Elliptic Curve Digital Signature Algorithm) and NTRUSign. These figures are derived from [4] and [8] and should be taken only as indicative for the specific platform (Pentium II 400 Mhz with memory constraints).

In conclusion, we can notice that in terms of performance, ECDSA and NTRU outperform RSA. Compared to each other, the advantage of ECDSA is its compactness, whereas NTRU's is its superior speed (the gain is approximately 2 in signing and 5 in verification [4]). The conclusive decision should depend on case-specific evaluations (e.g., considering the computing platforms that will be installed on vehicles equipped with DSRC).

Recent advances in Merkle tree traversal [28] could also open the possibility of using efficient Merkle authentication.

7.3 Is public key cryptography fit?

A typical criticism of public key cryptography in wireless networks is that its overhead seriously affects the performance of the system. This is particularly true for resource-constrained devices, such as handhelds and sensors. But the advantage of VANETs is that nodes are not anemic devices but energy-rich nodes. As VANETs are still in the development phase with a deployment schedule spanned over at least a decade, it is reasonable and necessary to consider the future compatibility of the system. Next we provide performance figures based on typical VANET scenarios and taking the technology timeline into account.

Each message will contain a digital signature and a corresponding certificate. ECC and NTRU are the most reasonable PKCS candidates so far, hence we assume a signature size between 28 bytes (ECDSA) and 197 bytes (NTRU). We assume the safety message size (not considering cryptographic material) to be around 200 bytes, including all overheads. The resulting total message size (safety message plus a digital signature plus a certificate, which contains a public key and a signature) is between 284 and 791 bytes. The second figure may be surprising at first, as the security overhead is almost 3 times the message size. But it represents the upper bound on the total message overhead; below we will show that even this overhead is acceptable. In fact, if we compare the values in Tables 2 and 3, we can deduce that the critical overhead of a given PKCS is the signature verification time, since each vehicle will periodically receive *several* messages that it needs to verify while it has to sign and send only one message during the same period. The use of smaller signature sizes (e.g., ECDSA) is also possible with hardware accelerators.

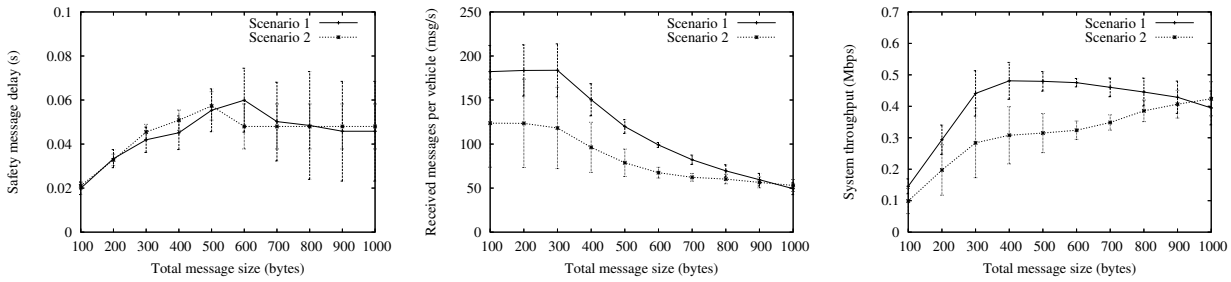
7.3.1 Numerical upper bounds

We consider two scenarios (we assume upper bounds on all values) with the basic protocol introduced in 3.2. The channel capacity is typically 12 Mbps for safety messages with a minimum of 6 Mbps.

1. A highway with 6 lanes (3 in each direction) of 3 m each. We assume a uniform presence of vehicles, with an inter-vehicle space of 30 m. Vehicles are mobile and transmit DSRC messages every 300 ms over a 300 m communication range. We consider a vehicle V located in the middle of the highway, which corresponds to a maximum of received messages; V can hear 120 vehicles per 300 ms. In the worst-case, where all vehicles contend for the channel, the system throughput is 2.53 Mbps (120 veh $\times$ 3.33 msg$\times$sec/veh $\times$ 791 bytes/msg), to be compared with the minimum nominal capacity of DSRC, which is 6 Mbps. Before V can send a new message, it should be able to process all incoming messages within 300 ms. Assuming V receives all the 120 messages (although the average reception rate has recently been evaluated to be significantly smaller than 1 [29]), the maximum tolerable processing delay per message is 300 ms/120 = 2.5 ms, a figure already achievable (Table 3).

2. We consider the same highway as in the previous case but this time vehicles are very slow or stopped (congestion scenario) and spaced by 5 m (including the vehicle length). Each vehicle transmits a safety message over a range of 15 m every 100 ms. In this case, a vehicle V can hear at most 36 other vehicles per 100 ms, which amounts to a throughput of 2.28 Mbps (36 veh $\times$ 10 msg$\times$sec/veh $\times$ 791 bytes/msg), which is also smaller than the minimum 6 Mbps. The upper bound on the processing delay per message, assuming V receives all the messages, is 100 ms/36 = 2.78 ms, which is already achievable.

[4]The NTRU cryptosystem is recent and has so far undergone considerable scrutiny. It is being standardized by the IEEE P1363 Working Group (Standard Specifications For Public-Key Cryptography).



(a) Message delay (b) Received packets (c) System throughput

Figure 4: The effect of packet size on the VANET performance. All curves include a confidence interval of 95%

7.3.2 Simulations

To support the above numerical results, we have simulated the above scenarios on the ns-2 simulator. We have used the MAC (Medium Access Control) and PHY parameters of IEEE 802.11a on which DSRC is based. Figure 4 shows the message delay, the number of received messages per vehicle, and the system throughput (total number of bits received per vehicle) as functions of the total message size (including the security overhead).

In Fig. 4(a), we can see that the average message delay does not vary considerably when the message size increases because the low contention on the medium and the high transmission rate minimize the effect of the message size. It is important to note that in Scenario 1, the maximum message delay is smaller than 300 ms, which is the interval between consecutive messages. In Scenario 2, the maximum is smaller than 100 ms, the inter-message interval in this case. Hence, the introduction of the cryptographic material does not critically affect the message delay.

Fig. 4(b) shows the number of received messages per vehicle as a function of the message size. We can see that the maximum numbers of received messages are smaller than the upper bounds provided in 7.3.1. The average actual processing delays for a message of size 800 bytes are around 1s/75msg = 13.33 ms in Scenario 1 and 1s/60msg = 16.67 ms in Scenario 2, which are acceptable values. We can also notice that large message sizes heavily increase message loss.

Finally, Fig. 4(c) shows that the system throughput in both cases is smaller than the minimum available capacity of 6Mbps. This is due to the message reception rate, which is smaller than 1.

In practice, this overhead can be further reduced by using the following optimizations:

1. V verifies a message only if its content is relevant (a message can be read before verification since it is not encrypted).

2. If V receives a message signed using a public key that it had already verified (this is possible because anonymous keys are used for several messages before being discarded), it has to verify only one signature. This is a typical case in a congestion scenario.

To conclude, we believe that public key cryptography is fit for vehicular networks. Given the above results, a PKCS can be already used relying on current technology, but there is ample space for optimization. Further advances in algorithms, software, and hardware will increase the performance and efficiency of the security functions.

8. DISCUSSION

A related topic that is worth considering is secure positioning. The most common approach to positioning vehicles is by GPS. But this has several drawbacks, because the precision of GPS is to the order of several meters and degrades in urban environments because of constructions such as buildings and tunnels that weaken GPS signals. The recently introduced DGPS solves the precision problem by reducing the error to several centimeters [12]. GPS can also be subject to a series of attacks such as signal jamming and spoofing [30]. Some attempts have been made to correct this problem [20], although no definitive solution is available yet. A solution for secure positioning without GPS was proposed in [9], but it is not adapted to VANETs.

9. CONCLUSION

In this paper, we have explained why vehicular networks need to be secured, and why this problem requires a specific approach. We have proposed a model that identifies the most relevant communication aspects; we have also identified the major threats. We have then proposed a security architecture along with the related protocols; we have shown how and to what extent it protects privacy. Finally, we have analyzed the robustness of our proposal, and we have assessed its performance. We have shown that public key cryptography is fit for the considered problem.

To our best knowledge, this is the first paper addressing the security of vehicular networks in a systematic and quantified way.

In terms of future work, we intend to further develop this proposal. In particular, we intend to explore in more detail the respective merits of key distribution by the manufacturers or by governmental bodies; we will also perform additional numerical evaluations of the solutions.

Acknowledgements

We would like to thank Imad Aad, Levente Buttyan, Mario Cagalj, Markus Jakobsson, Daniel Jungels, Tim Leinmueller, and Christof Paar for their helpful feedback on earlier versions of this work.

10. REFERENCES

[1] http://www.car-2-car.org/.

[2] http://www.network-on-wheels.de/.

[3] 5.9 GHz DSRC. http://grouper.ieee.org/groups/scc32/dsrc/.

[4] http://grouper.ieee.org/groups/1363/working group/presentations/ntrusignparams-1363-0411.pdf.

[5] http://www.rsasecurity.com.

[6] Wave Systems Corp. EMBASSY 2100 cryptographic controller. http://www.wave.com/about/datasheets/03-000139_EMBASSY2100.pdf.

[7] Jeremy Blum and Azim Eskandarian. The threat of intelligent collisions. *IT Professional*, 6(1):24–29, Jan.-Feb. 2004.

[8] Michael Brown, Darrel Hankerson, Julio López, and Alfred Menezes. Software implementation of the NIST elliptic curves over prime fields. *Lecture Notes in Computer Science*, 2020:250–265, 2001.

[9] S. Capkun and J.P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *IEEE INFOCOM*, 2005.

[10] Sastry Duri, Marco Gruteser, Xuan Liu, Paul Moskowitz, Ronald Perez, Moninder Singh, and Jung-Mu Tang. Framework for security and privacy in automotive telematics. In *Proceedings of the 2nd international workshop on Mobile commerce*, pages 25–32. ACM Press, 2002.

[11] Stephan Eichler, Jerome Billion, Robert Maier, Hans-Jrg Vgel, and Rainer Kroh. On providing security for an open telematics platform. In *5th International Conference on ITS Telecommunications*, 2005.

[12] Per Enge. Retooling the Global Positioning System. *Scientific American*, May 2004.

[13] Wilfried Enkelmann. FleetNet - applications for inter-vehicle communication. In *IEEE Intelligent Vehicles Symposium*, pages 162–167, June 2003.

[14] Igor Furgel and Kerstin Lemke. A review of the digital tachograph system. In *Workshop on Embedded IT-Security in Cars (escar)*, 2004.

[15] Lutz Gollan and Christoph Meinel. Digital signatures for automobiles. In *Systemics, Cybernetics and Informatics (SCI)*, 2002.

[16] Philippe Golle, Dan Greene, and Jessica Staddon. Detecting and correcting malicious data in VANETs. In *Proceedings of the first ACM workshop on Vehicular ad hoc networks*, pages 29–37. ACM Press, 2004.

[17] Yih-Chun Hu, Adrian Perrig, and David Johnson. Ariadne: a secure on-demand routing protocol for ad hoc networks. In *Proceedings of the 8th annual international conference on Mobile computing and networking*, pages 12–23. ACM Press, 2002.

[18] Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo. The security and privacy of smart vehicles. *IEEE Security and Privacy Magazine*, 2(3):49–55, May-June 2004.

[19] Markus Jakobsson. *Privacy vs. Authenticity.* PhD thesis, University of California at San Diego, 1997.

[20] Markus G. Kuhn. An asymmetric security mechanism for navigation signals. In *Sixth Information Hiding Workshop*, 2004.

[21] A. K. Lenstra and E. R. Verheul. Selecting cryptographic key sizes. *Journal of Cryptology*, 14(4):255293, 2001.

[22] Matthias Lott, Rudiger Halfmann, Egon Schultz, and Markus Radimirsch. Medium access and radio resource management for ad hoc networks based on UTRA TDD. In *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, pages 76–86. ACM Press, 2001.

[23] Kirsten Matheus, Rolf Morich, Ingrid Paulus, Cornelius Menig, Andreas Lbke, Bernd Rech, and Will Specks. Car-to-car communication - market introduction and success factors. In *ITS 2005: 5th European Congress and Exhibition on Intelligent Transport Systems and Services*, 2005.

[24] Adrian Perrig and J.D. Tygar. *Secure Broadcast Communication in Wired and Wireless Networks.* Kluwer Academic Publishers, 2003.

[25] Peter Samuel. Of sticker tags and 5.9GHz. *ITS International*, 2004.

[26] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[27] D. Shaw and W. Kinsner. Multifractal modelling of radio transmitter transients for classification. In *WESCANEX 97: Communications, Power and Computing*, 1997.

[28] Michael Szydlo. Merkle tree traversal in log space and time. In *Eurocrypt*, 2004.

[29] Marc Torrent-Moreno, Daniel Jiang, and Hannes Hartenstein. Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks. In *VANET '04: Proceedings of the first ACM workshop on Vehicular ad hoc networks*, pages 10–18. ACM Press, 2004.

[30] Jon S. Warner and Roger G. Johnston. Think GPS cargo tracking = high security? Think again. Technical report, Los Alamos National Laboratory, 2003.

[31] Marko Wolf, André Weimerskirch, and Christof Paar. Security in automotive bus systems. In *Workshop on Embedded IT-Security in Cars (escar)*, 2004.

[32] Qing Xu, Tony Mak, Jeff Ko, and Raja Sengupta. Vehicle-to-vehicle safety messaging in DSRC. In *Proceedings of the first ACM workshop on Vehicular ad hoc networks*, pages 19–28. ACM Press, 2004.

[33] Xue Yang, Jie Liu, Feng Zhao, and Nitin Vaidya. A vehicle-to-vehicle communication protocol for cooperative collision warning. In *First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 2004)*, August 2004.

[34] Magda El Zarki, Sharad Mehrotra, Gene Tsudik, and Nalini Venkatasubramanian. Security issues in a future vehicular network. In *European Wireless*, 2002.

[35] Peifang Zheng. Tradeoffs in certificate revocation schemes. *SIGCOMM Comput. Commun. Rev.*, 33(2):103–112, 2003.