Journal of Computer Security 15 (2007) 39–68
IOS Press

Securing 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
E-mail: {maxim.raya, jean-pierre.hubaux}@epfl.ch

Vehicular networks are very likely to be deployed in the coming years and thus 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 efficiency.

Keywords: Vehicular ad hoc networks, wireless, 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 EDR (*Event Data Recorder*), reminiscent of the "black boxes" used in avionics. Optionally, it also has a GPS (*Global Positioning System*) 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 [7,9,12,15,16,21,26,40–42]. In the US, the FCC has allocated a bandwidth of 75 MHz 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, namely IEEE 802.11p.

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, opens tremendous business opportunities, but also raises formidable research challenges.

One of these challenges is security; limited attention [7,15,21,33,42] 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 establishing 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. It is an extension of our previous work on the subject [33].

It should be noted that the first applications of vehicular networks will probably be commercial, such as infotainment services provided by the infrastructure. Yet, it is very important to establish the foundations of security for the next steps (vehicle-to-vehicle communications) because industrial consortia are already working on the standards.

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 go into the details of authentication mechanisms. Section 7 presents the security analysis of the proposed protocols and Section 8 addresses implementation issues. In Section 9 we discuss open problems. Finally, Section 10 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 the development of a suitable MAC layer, as well as potential applications ranging from collision avoidance to onboard infotainment services. But both academia and the industry have so far largely overlooked the subject of security in VANETs, postponing it to later phases of research and development.

The research on VANET security is just starting, with few pioneer papers so far. In [7], Blum and Eskandarian describe a security architecture for VANETs intended

mainly to counter the so-called "intelligent collisions" (meaning that they are intentionally caused). But this is only one type of attacks and building the security architecture requires awareness of as many potential threats as possible. They propose the use of a PKI and a virtual infrastructure where cluster-heads are responsible for reliably disseminating messages (by a sequential unicast instead of broadcast) after digitally signing them; this approach creates bottlenecks at cluster-heads in addition to high security overhead. Gerlach [14] describes the security concepts for vehicular networks. Hubaux et al. [21] take a different perspective of VANET security and focus on privacy and secure positioning issues. They point the importance of the tradeoff between liability and anonymity and also introduce Electronic License Plates (ELP) that are unique electronic identities for vehicles. Parno and Perrig [29] discuss the challenges, adversary types and some attacks encountered in vehicular networks; they also describe several security mechanisms that can be useful in securing these networks. El Zarki et al. [42] describe an infrastructure for VANETs and briefly mention some related security issues and possible solutions. The use of digital signatures in the vehicular environment is discussed in [15]. Software frameworks for telematics are proposed in [9,10]. Some recent papers [16,32] focus on particular VANET security subjects that can easily fit in the architecture presented in this paper. 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 [13]. The security problems of automotive bus systems are pinpointed in [39].

In the case of non-safety related applications in which vehicles communicate with the infrastructure, the CARAVAN scheme [34] allows vehicles to preserve their privacy by forming groups in which the group leader acts as a proxy on behalf of all group members that access the infrastructure. When the vehicles do not have to access the infrastructure, they remain silent thus preventing eavesdroppers from tracking their pseudonyms.

The most prominent industrial effort in this domain in Europe is carried out by the Car 2 Car Communication Consortium [1] and several projects such as SEVECOM [2], while in the USA it is addressed by the DSRC [3] consortium, especially the IEEE P1609.2 Working Group [6].

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 9).

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

3. System model

In this section, we present the distinguishing properties of VANETs (Fig. 1) in order to express 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 make the system future-compatible, the following assumptions are based mainly on specifications of future 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 [3].

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

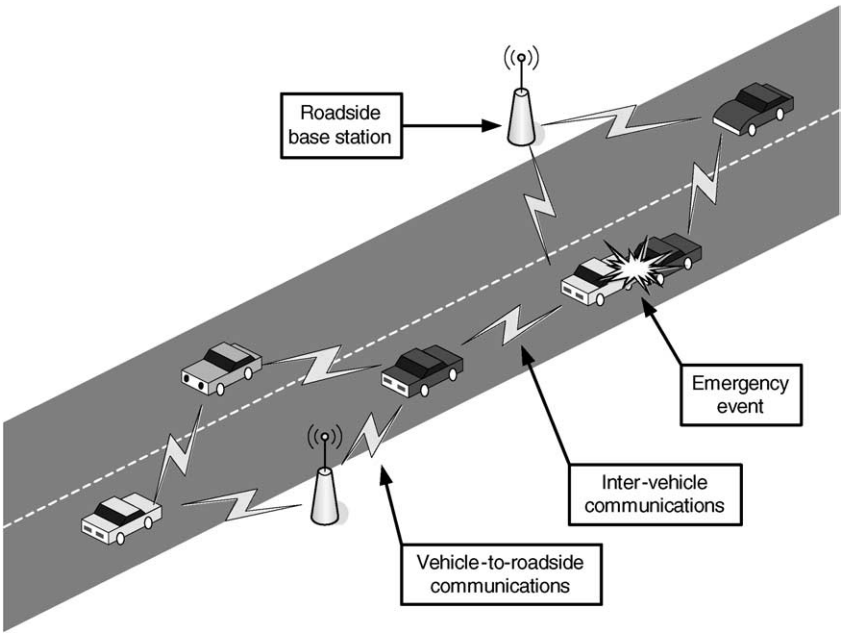

Fig. 1. A VANET consists of vehicles and roadside base stations that exchange primarily safety messages to give the drivers the time to react to life-endangering events.

crossing vehicles). For example, on highways vehicle speeds are usually higher than 80 km/h (with relative speeds 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 substantial 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 that can be used for crash reconstruction, and a GPS 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; in Section 9.4 we will describe alternative options.

VANETs are expected to be deployed over the next decade to achieve considerable penetration only around 2014 [27,35]. Nevertheless, the network should become partially operational with the release of first products in the next few 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 omnipresent infrastructure supporting safety features (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. Although 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 and cooperative driving (e.g., for lane merging). The common characteristic of this category is the relevance to life-critical situations where the existence of a service may prevent life-endangering accidents. Hence the security of this category is mandatory, since the proper operation of any of these applications should be guaranteed even in the presence of attackers.
2. Other applications, including traffic optimization, 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 focus on 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.

Table 1
Message classes and properties

Class/Property	Legitimacy	Privacy protection		Real-time
		Against others	Against police	constraints
Traffic information	*yes*	*yes*	*yes*	
General safety messages	*yes*	*yes*	*yes*	*yes*
Liability-related messages	*yes*	*yes*		*yes*

3.1.3. Safety messages

As explained in the previous section, we consider only 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 geocast 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 fines 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 limited (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 [40,41]. To better describe the security solutions introduced in this paper, we describe in the following a simple protocol inspired from [41] 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 a vehicle V receives an emergency warning from another vehicle W and, 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 define four 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.
4. *Local* vs. *Extended*. An attacker can be limited in scope, even if he controls several entities (vehicles or base stations), which makes him local. An extended attacker controls several entities that are scattered across the network, thus extending his scope. This distinction is especially important in privacy-violating and wormhole attacks that we will describe shortly.

Inspired by [19], we characterize an attacker by *Membership.Motivation.Method. Scope* where *Membership* stands for *Insider* (I_m) or *Outsider* (O_n), *Motivation* for *Malicious* (*M*) or *Rational* (*R*), *Method* for *Active* (*A*) or *Passive* (*P*), and *Scope* for *Local* (*L*) or *Extended* (*E*); 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 $I_2.R.A.L$ controls two networks members, behaves rationally, and mounts active attacks in restricted areas. A star ("*") indicates that the corresponding field can take any value.

4.2. Basic attacks

As this paper is concerned with vehicular *networks*, we consider only the attacks perpetrated against messages rather than 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 sensor information*: Attackers in this case are also $I_m.R.A.L$, 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

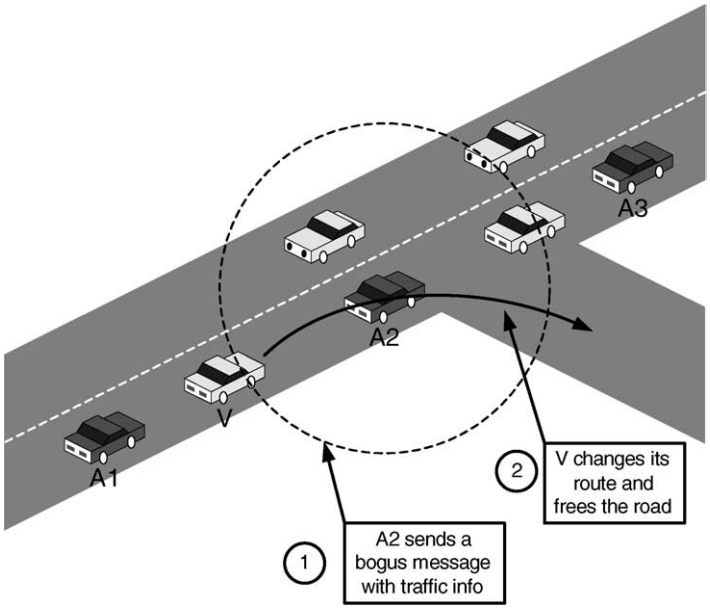

Fig. 2. In this example *bogus information* attack, colluding attackers (A2 and A3) disseminate false information to affect the decisions of other vehicles (V) and thus clear the way of attacker A1.

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 [37]) are solved by appropriate physical layer techniques such as radio transmitters that randomize fingerprints.

4. *Denial of Service*: The attacker is $*.M.A.L$ 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. *Masquerading*: The attacker actively pretends to be another vehicle by using false identities and can be motivated by malicious or rational objectives.

4.3. Sophisticated attacks

The attacks in this section are more elaborated variants or combinations of the above attacks. They are examples of what an adversary can do. In the context of VANETs, this is the first time these attacks are presented.

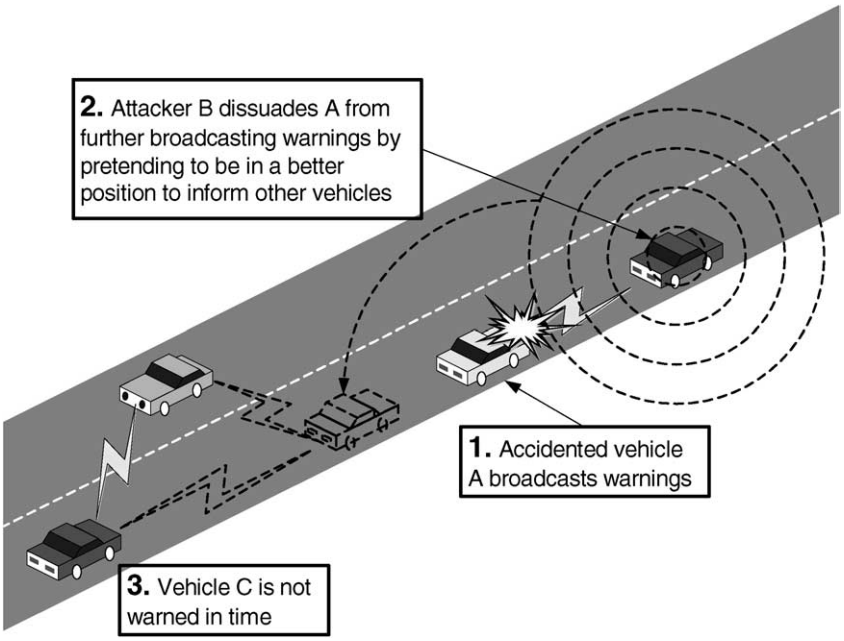

Fig. 3. Hidden vehicle attack.

1. *Hidden vehicle*: This is a concrete example of cheating with positioning information. It refers to a variation of the basic safety messaging protocol described in Section 3.2. In this version of the protocol, a vehicle broadcasting warnings will listen for feedback from its neighbors and stop its broadcasts if it realizes that at least one of these neighbors is better positioned for warning other vehicles. This reduces congestion on the wireless channel. As Fig. 3 illustrates, the hidden vehicle attack consists in deceiving vehicle A into believing that the attacker is better placed for forwarding the warning message, thus leading to silencing A and making it hidden, in DSRC terms, to other vehicles. This is equivalent to disabling the system.
2. *Tunnel*: Since GPS signals disappear in tunnels, an attacker may exploit this temporary loss of positioning information to inject false data once the vehicle leaves the tunnel and before it receives an authentic position update as Fig. 4 illustrates. The physical tunnel in this example can also be replaced by an area jammed by the attacker, which results in the same effects.
3. *Wormhole*: In wireless networking, the wormhole attack [20] consists in tunneling packets between two remote nodes. Similarly, in VANETs, an attacker that controls at least two entities remote from each other and a high speed communication link between them can tunnel packets broadcasted in one location to another, thus disseminating erroneous (but correctly signed) messages in the destination area.

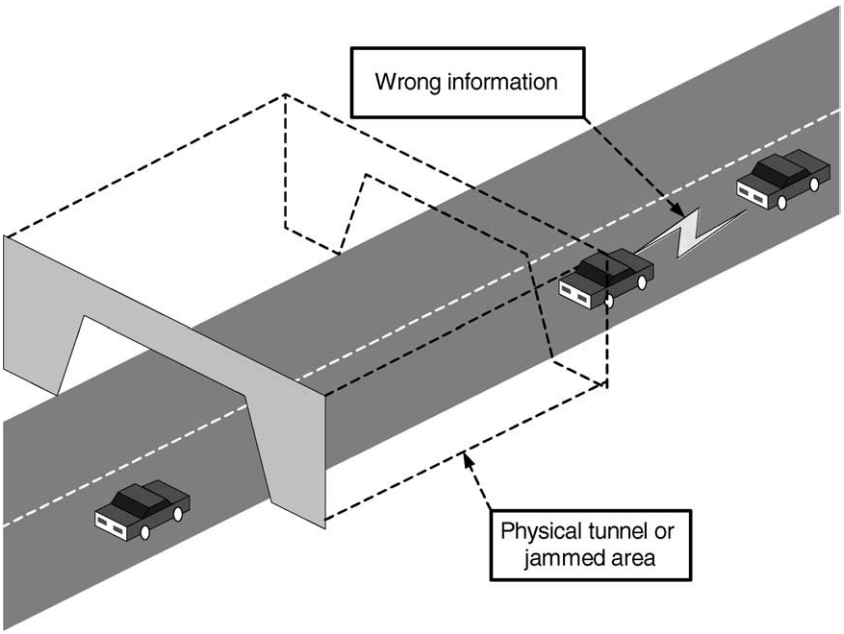

Fig. 4. Tunnel attack.

4. *Bush telegraph*[2]: This is a developed form of the bogus information attack. The difference is that in this case the attacker controls several entities spread over several wireless hops. Similarly to the social phenomenon of information spreading and its en-route modification, this attack consists in adding incremental errors to the information at each hop. While the errors are small enough to be considered within tolerance margins at each hop and hence accepted by the neighbors, the intentional accumulation of these errors may yield to a bogus information at the last hop.

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.

[2]Bush telegraph stands for the rapid spreading of information, rumors, etc., usually by word of mouth. As this information is propagated along a human chain, it is frequently modified by each person in the chain. The result may sometimes be completely different from the original.

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. This requirement is sometimes called "plausibility".
- *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.

As we will show in detail in Section 6, we have chosen digital signatures over other forms for message authentication. The simplest and the most efficient method is to assign to each vehicle a set of public/private key pairs that will allow the vehicle to digitally sign messages and thus authenticate itself to receivers. Because of the liability issues present in VANETs, a self-organized trust management approach such as the one in PGP (Pretty Good Privacy) is not satisfactory. Indeed, these public keys should be issued and signed by a trusted authority. The need for certificates issued by an authority implies the use of a PKI (Public Key Infrastructure).

Under the PKI solution, before a vehicle sends a safety message, it signs it[3] with its private key and includes the CA's (Certification Authority, discussed in Section 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 (TPD) 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. As its name implies, the TPD contains a set of sensors that can detect hardware tampering and erase all the stored keys to prevent them from being compromised. The availability of this feature makes the TPD on one hand too sensitive for VANET conditions (for example, the device can be subject to light shocks because of road imperfections; TPDs also cannot tolerate extreme temperatures that may not be unusual for vehicles) and on the other hand too expensive for non-business consumers. In fact, current commercial products such as the IBM 4758 card [4] contain cryptographic coprocessors, are oriented towards financial applications and cost several thousands of dollars.

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

An alternative option to a TPD would be to use a TPM (Trusted Platform Module [5]) that can resist to software attacks but not to sophisticated hardware tampering. Such units are gaining wide usage in notebooks and cost only a few tens of dollars.

The final definition of the security hardware will depend mainly on economic and technical factors. This hardware may still have to be designed as a compromise between TPD and TPM. Our goal in this work is to set the operational requirements that can guide later the choice or design of such a device.

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*) [21] 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 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 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 ith 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

The advantages of using a PKI for VANETs are accompanied by some challenging problems, notably certificate revocation. For example, the certificates of a detected attacker or malfunctioning device have to be revoked, i.e., it should not be able to use its keys or if it still does, vehicles verifying them should be made aware of their invalidity.

The most common way to revoke certificates is the distribution of CRLs (Certificate Revocation Lists) that contain the most recently revoked certificates; CRLs are provided when infrastructure is available. In addition, using short-lived certificates automatically revokes keys. These are the methods proposed in the IEEE P1609.2/D2

draft standard [6]. But there are several drawbacks in this approach. First, CRLs can be very long due to the huge number of vehicles and their high mobility (meaning that a vehicle can encounter a high number of vehicles when travelling, especially over long distances). Second, the short lifetime of certificates still creates a vulnerability window. Last but not least, the availability of an infrastructure will not be pervasive, especially in the first years of deployment.

To avoid the above shortcomings, we have designed a specific solution [23]. As this topic is arguably the most difficult aspect of VANET security, we provide here the operating principles of the solution we propose. It includes a set of efficient revocation protocols, namely RTPD (Revocation Protocol of the Tamper-Proof Device), RCCRL (Revocation protocol using Compressed Certificate Revocation Lists), and DRP (Distributed Revocation Protocol). In RTPD, once the CA has decided to revoke all the keys of a given vehicle M, it sends to it a revocation message encrypted with the vehicle's public key. After the message is received and decrypted by the TPD of the vehicle, the TPD erases all the keys and stops signing safety messages. Then it sends an ACK to the CA. All the communications between the CA and the vehicle take place in this case via base stations. In fact, the CA has to know the vehicle's location in order to select the base station through which it will send the revocation message. If it does not know the exact location, it retrieves the most recent location of the vehicle from a location database and defines a paging area with base stations covering these locations. Then it multicasts the revocation message to all these base stations. In the case when there are no recent location entries or the ACK is not received after a timeout, the CA broadcasts the revocation message, for example, via the low-speed FM radio on a nationwide scale or via satellite.

The RCCRL protocol is used when the CA wants to revoke only a subset of a vehicle's keys or when the TPD of the target vehicle is unreachable (e.g., because of jamming); RCCRL also relies on the availability of infrastructure. Compared to RTPD, RCCRL has the special feature of warning the neighbors of a revoked vehicle.

The DRP protocol is used in the pure ad hoc mode whereby vehicles accumulate accusations against misbehaving vehicles and report them to the CA once a connection is available. Unlike RTPD and RCCRL, the revocation in DRP is triggered by the neighbors of a vehicle upon the detection of misbehavior. Mechanisms for the detection of malicious data [16] can be leveraged to spot vehicles generating these data (since all messages are signed).

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

All vehicle identifiers, in particular MAC and IP addresses, must change over time. And 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 7.2 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 [36] 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 [22].

6. Alternative authentication mechanisms

Attaching a digital signature and a certificate to each safety message for the sake of security inevitably creates overhead that can be larger than the message itself [33]. Therefore we have considered several options to reduce this overhead, notably relying on the establishment of symmetric keys. Next we consider two different symmetric key types, pairwise and group keys. Our aim in presenting these mechanisms is to make a comprehensive investigation of possible authentication solutions and compare them in Section 8.3. Hence the following descriptions are not full-fledged solutions but rather simplified versions thereof. Section 8.3 shows that digital signatures are the best authentication option, even compared to these simplified, and hence less costly in terms of overhead, versions.

6.1. Pairwise keys

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 much more efficient (in terms of time and space overhead) than the asymmetric ones.

As before, we are mainly concerned with inter-vehicle authentication since it will constitute the bulk of VANET security operations. We have considered the typical scenario of two vehicles A and B happening to remain in power range of each other for a while and that decide to establish a session key. Obviously, the huge scale of VANETs prohibits from preloading pairwise shared keys into vehicles. Hence, key establishment should be dynamic. Once the initial public key and certificate exchange is complete, the most efficient way for key establishment is using ISO/IEC 11770-3 Key Transport Mechanism 3 [8] whereby one of the vehicles A sends the session key K to B encrypted with B's public key:

$$A \rightarrow B : \{B|K|T\}_{PuK_B}, Sig_{PrK_A}[B|K|T]$$

Subsequent message exchanges can use Hashed Message Authentication Codes (HMAC) with the key K:

$$A \rightarrow B : m, HMAC_K(m)$$

There are several problems with this approach, which prevents the use of dynamically established symmetric session keys in VANETs as a viable solution. In fact, as expected and will be shown in Section 8.3, session key establishment does not scale well with the number of vehicles (even with a few vehicles) and soon exceeds digital signatures in terms of overhead. For scenarios with only few vehicles, the establishment of session keys for efficiency purposes is not justified because of the lack of congestion on the wireless channel. In addition, non-repudiation is an important VANET property for liability attribution and cannot be achieved with symmetric keys. Hence critical safety applications cannot rely on symmetric session keys.

6.2. Secure group communication

When considering the group nature of VANET applications such as platooning[4], it is tempting from the security standpoint to think of establishing secure groups with secret group keys. The use of symmetric keys for authentication would reduce the security overhead. In terms of security, group keys are meant, similarly to digital signatures, to cope with outsider adversaries. An attacker can still be a group member, given that it had certified public keys when joining the group. We have considered several options for this approach in VANETs, inspired from the existing rich literature on the subject [31]. In the VANET context, we can distinguish several problems:

[4] *Platooning* consists in grouping vehicles in a way that allows them to accelerate or brake simultaneously, thus increasing road capacity without building additional traffic lanes.

- **Key agreement vs. key transport**: On one hand, given the distributed nature of VANET groups (because of the equality of their members), key agreement is the normal approach for key establishment. There are several methods to achieve this, but all of them involve several rounds of broadcasts by all participants. On the other hand, key transport consists in allowing a group leader, either chosen by the specific application or randomly, to create a group key and broadcast it to all members; this method can terminate in one round but focuses most of the computational burden on the group leader that is also a single point of failure.
- **Join/Leave operations**: In VANETs, group memberships are likely to change very fast. Hence another challenge in secure group management is the efficient handling of join and especially leave operations of new members. Simple approaches like key transport can transfer the existing key to a new member but have to recompute and redistribute a new key in the case of a leaving member. Protocols based on key trees [31] may require the recomputation of only a subset of keys for both operations; the management of such trees requires higher level of complexity but distributes the computation load compared to simple key transport.
  It is important to note here that most vehicles in VANETs will have similar security levels, hence the creation of secure groups will only contribute to reducing the security overhead and not defining different security levels among VANET members. Similarly to digital signatures, the use of secure groups protects the network from outsiders and not insiders as defined in Section 4. Hence, while renewing or transferring existing keys during member joins is still necessary, member leaves should not necessarily entail an update of the group key.
- **Definition of group memberships**: As stated several times before, the mobility model of VANETs is highly dynamic. While some vehicles may drive close to each other for several kilometers, other vehicles may bypass them quickly or alternately join the self-formed groups. In these scenarios it is extremely hard to define group boundaries. For example, a platoon may be stretched over several wireless hops and hence not all group members, especially the leading vehicle, may be aware of a new vehicle joining from behind. Any group rekeying based on tree recomputation and rebalancing or key agreement will be costly in terms of delay and message overhead. A simple solution in this case could be a key transfer from the closest neighbor of the new member.
  Yet, vehicles bypassing a group or belonging to another group may become unnecessarily involved in a key establishment attempt because of a lack of a clear definition of group boundaries. In addition, these vehicles must still receive safety messages without possessing the group key, which means the recurring necessity of periodic broadcasts with digital signatures.
  To alleviate the problem of dynamic group boundaries, the latter can be fixed and preloaded into vehicles. For example, roads can be divided into geographic cells and thus groups can be formed based on cell membership. Such a mechanism is described in detail in [32].

Based on the above discussion, we designed a simple secure group protocol for VANETs inspired notably from the Group Key Management Protocol (GKMP) [17] with geographically defined groups. As explained above, roads are divided into cells that define groups, with the group leader being the vehicle closest to the cell center. Leveraging on periodic broadcasts of certified public keys, the group leader (L in this example) distributes the group key K to members A, B, and C as follows:

$$L \rightarrow * : H_A, \{K\}_{PuK_A}, H_B, \{K\}_{PuK_B}, H_C, \{K\}_{PuK_C}, Sig_{PrK_L}$$

[*the whole message*]

In addition to the encrypted keys, the group leader includes hashes (e.g., H_A) of the receivers' public keys to help the receivers identify which encrypted group key to decrypt. A simple hash comparison suffices to achieve this.

Subsequent message broadcasts will include only a HMAC in addition to the message itself:

$$L \rightarrow * : m, HMAC_K(m)$$

When a new vehicle D enters the cell, it receives the group key from the current group leader:

$$L \rightarrow D : \{K\}_{PuK_D}, Sig_{PrK_L}[\{K\}_{PuK_D}]$$

When a vehicle leaves the cell, nothing needs to be done. Special attention needs to be paid to exchanges on cell boundaries when a vehicle switches from one group to another. In order to make this operation smooth, cell dimensions should be smaller than the diameter of the transmission range disk. For example, if the transmission range is 300 m, the disk diameter is 600 m, we can choose a cell size of 400 m. Hence, at the cell boundaries, a vehicle will receive messages from the leaders of both its previous and new groups.

Given the relative sophistication of this protocol compared to the basic digital signature broadcast, it is possible that it does not function properly at all times. For example, if there are few vehicles in an area, a group may not be able to form, due to the lack of a leader. But these shortcomings do not hinder the functionality of the VANET since a vehicle falls back automatically into the digital signature mode when it cannot join a group. It is also important to note here that all these security functions should be implemented in the TPD; hence, an attacker cannot alter the protocol function by changing the protocol itself.

There are several other functional details of this protocol that need to be worked out. But our purpose is to make it as simple as possible and compare its performance to the de facto broadcasts of digital signatures in Section 8.3.

As with symmetric session keys, non-tree based group keys lack the non-repudiation property and hence cannot be used for critical safety applications.

6.3. Efficient broadcast authentication

The TESLA protocol [30] enables broadcast authentication without using digital signatures all the time. The basic idea is to establish one-way hash chains where the key needed to verify a message is carried by the next message, thus allowing a receiver to authenticate messages. There are several drawbacks to applying this method in VANETs:

- There is an initialization phase where the first element in the hash chain has to be distributed to all receivers. Authentication in this phase is done using traditional asymmetric cryptography. And once the hash chain is consumed, a new chain needs to be established. This also means that the set of receivers should not change during the usage of one hash chain, an unrealistic requirement in VANETs.
- The verification of a message is only possible once the next message is received, which is not acceptable in delay-intolerant VANETs.

For these reasons, TESLA-like protocols are not suitable for VANETs.

7. Security analysis

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

7.1. Compliance with the security requirements

Authentication of messages 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.

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 9.2) can reduce the impact of such attacks.

Non-repudiation is achieved as follows:

- Vehicles cannot claim to be other vehicles (*masquerade* attack) since all the messages they transmit are signed by their (anonymous) public keys. ELPs cannot be forged because they are unique and verifiable.
- 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.

- Vehicles cannot cheat about their position and related parameters if a secure positioning solution is used (Section 9.4).

The satisfaction of the privacy requirement is addressed in the next section and the real-time constraints are addressed in Section 8.

7.2. 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 a 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 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); this is typical of a highway scenario. 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. 5 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}:

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

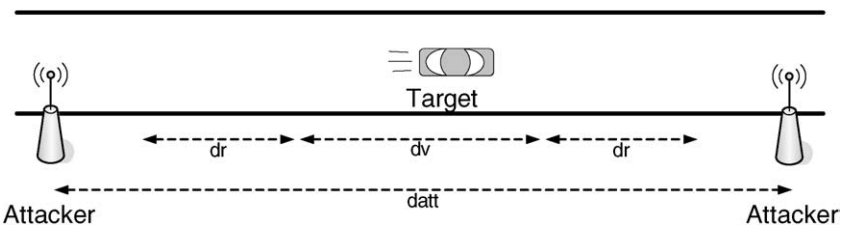

Fig. 5. To uncover the identity of its targets, the attacker leverages on key correlation and the target's transmission range.

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:

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

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:

$$N_{msg} = \lceil r_m \times T_{key} \rceil \text{ messages}$$

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

8. Implementation issues

8.1. Certificate lifetime and key set size

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

8.1.1. Certificate lifetime

Each anonymous key should be used only with a sequence of consecutive messages as described in Section 7.2, 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).

8.1.2. Anonymous key set size

Leveraging on the analysis in Section 7.2, a vehicle should change its anonymous key only after having used it for a certain number of messages. Reusing the example in 7.2, 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 43 800, which amounts to around 4.2 Mbytes (assuming a storage space of 100 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.

8.2. Choice of the cryptosystem

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 vehicles 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.

Each message will contain a digital signature and a corresponding certificate. Hence the need for a Public Key Cryptosystem (PKCS) with a compact signature size and efficient execution time. A prominent candidate for playing this role is Elliptic Curve Cryptography (ECC) with keys of 224 bits (28 bytes) and signature sizes of 56 bytes, resulting in a security level roughly equivalent to RSA 2048 according to [25]. The cryptographic overhead is hence around 140 bytes (1 digital signature, 1 key, and 1 certificate that is actually a signature). 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. We have shown in [33] that this is a feasible solution even on low-end processors (Pentium II 400 MHz in this case). As mentioned in Section 5.3, the actual nature and capacity of the security hardware has still to be defined but it will certainly be enough to perform ECC crypto operations.

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.

8.3. Comparison of authentication mechanisms

In this section we roughly compare the performance of the different authentication mechanisms discussed in this paper, namely digital signatures, symmetric pairwise

keys, and symmetric group keys. Our evaluations are analytical and indicative since there are many factors that affect performance and that remain undecided so far, such as the size of the digital signatures or the computational capacities of on-board processors.

In the following we will focus on the message size and message number overhead corresponding to each mechanism while leaving the local execution times of each mechanism out of scope since the computational power of in-vehicle processors will soon inevitably increase while the available bandwidth may remain constant for a longer while.

As discussed in Section 8.2, we assume that the public key cryptosystem is ECC with a key size of 28 bytes; the signature and ciphertext sizes are roughly double the key size (i.e., 56 bytes each) and the certificate consists mainly of the public key and the CA's signature over it (i.e., 84 bytes in total). For symmetric cryptography, we assume a HMAC using the hash function SHA-224 (i.e., 28 bytes). Let us also assume a group of N vehicles (all in power range of each other) that want to locally broadcast M safety messages each. The computation of the overheads follows.

8.3.1. Digital signatures

Using the message format in Section 5.2, the size of the overhead is the same for each message and is equal to $56 + 84 = 140$ bytes/vehicle$*$message.

8.3.2. Pairwise keys

Using the message formats in Section 6.1, the cost of key establishment for N vehicles is $(56 + 56)N(N - 1)/2$ hence $56(N - 1)$ bytes/vehicle. Once the keys are established, the cost for one vehicle to send messages to the remaining $(N - 1)$ vehicles is $28(N - 1)$ bytes/vehicle$*$message (one HMAC per vehicle). The total overhead to send one message is hence $(56/M + 28)(N - 1)$ bytes/vehicle$*$message. The total number of messages is $M * (N - 1)$/vehicle, i.e., $N - 1$ times the number of digitally signed messages.

8.3.3. Group key

Using the message formats in Section 6.2, key establishment for N vehicles requires the leader to send $(N - 1)$ ciphertexts in addition to one signature, which costs $(56(N - 1) + 56)/N = 56$ bytes/vehicle. After key establishment, a vehicle sends one message to all the other vehicles using the shared group key at a cost of 28 bytes/vehicle$*$message (one HMAC). In addition, let us assume that the leader broadcasts a digitally signed message (140 bytes) every 10 group messages (i.e., every 3 s if the messages are sent every 300 ms) to announce itself to newcomers. Assuming cells overlap over 100 m (for reliable handover), 3 s is the time a vehicle needs to switch between two cells while driving at a speed of 120 km/h. Moreover, let us assume the leader adds 3 new members every 3 s (assuming a highway with 3 lanes per direction), which costs one encryption and one signature, i.e., $(56 + 56) * 3 = 336$ bytes. Hence the total overhead is $56/M + 28 + 140/10 + 336/10 = 56/M + 75.6$ bytes/vehicle$*$message. The total number of messages is $M + (M * 1/10 + M * 3/10)/N = M(1 + 0.4/N)$/vehicle.

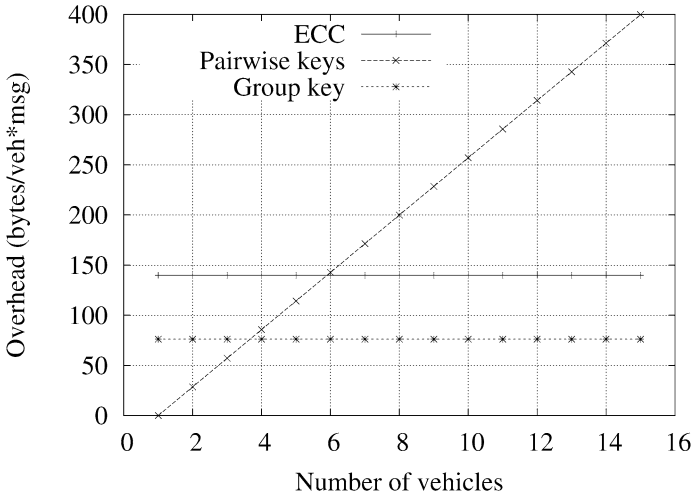

Fig. 6. Comparison of authentication mechanisms.

Figure 6 compares the overhead of the three approaches in bytes. We can notice that pairwise keys result in bigger overhead than ECC even when there are only a few vehicles; group keys result in this example in saving around 54% of the message overhead. But group key establishment and membership update require more messages than the digital signature approach; the actual overhead depends on the number of vehicles as well as the dynamics of the network. To conclude this comparison, symmetric group key establishment may lead to significant savings in bandwidth consumption but at the expense of more transmissions and the complexity needed to implement group protocols. Hence, digital signatures seems to be the most convenient and reliable solution for authentication, even though its efficiency leaves place for improvement.

As mentioned at the beginning of this section, this comparison is only analytical because an empirical evaluation is not possible without defining several performance related aspects, such as the power of on-board processors. But even analytically, we can see the major performance characteristics of each technique and make a conclusion that favors digital signatures.

9. Open problems

9.1. Secure geocast

The basic safety message dissemination model in VANETs consists in local broadcasting of regular or event warning messages. The propagation of warnings is assured by vehicles receiving and then rebroadcasting them over multiple hops, one hop at

a time. But there are scenarios where messages need to be delivered to specific areas. In vehicular networks, this can be supported by the *geocast* primitive [28] that is a form of position-based routing protocols. Yet none of these solutions is secure. But there is rich literature on secure routing protocols [18]. Their applicability to VANETs still needs to be investigated.

9.2. 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, cellular, 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 (and inform the driver) 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.

9.3. Data verification

In the bogus information attack (Section 4.2) and its derivatives, 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 can be 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].

9.4. Secure positioning

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 a few centimeters [11]. GPS can also be subject to a series of attacks such as signal jamming and spoofing [38]. Some attempts have been made to correct this problem [24], although no definitive solution is available yet.

Thus far, there is little work done on secure positioning without GPS. Existing schemes, e.g., those for sensor networks, allow nodes to locate only themselves and

hence solve only part of the VANET positioning problem. The authors of [21] propose the use of *verifiable multilateration* whereby three or more base stations perform distance bounding on a vehicle before computing its location. The obvious drawback of this approach is the need for infrastructure coverage. In a different approach called *entanglement* [29], vehicles rebroadcast the public keys of other vehicles after signing them. This helps to perform relative localization. But this approach incurs overhead and does not provide absolute positions.

The final solution will probably be a hybrid system that will use a combination of GPS, radars, wheel rotation sensors, digital maps, and roadside beacons, depending on the availability and reliability of each of these techniques.

10. 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.

Using the analysis and results obtained in this work, we have come to the certainty that existing network security solutions cannot be readily applied to VANETs, given the radically different nature of this new type of networks. A good example is that of authentication mechanisms, where digital signatures showed to be the most suitable approach despite their seemingly high overhead.

Acknowledgements

We would like to thank Imad Aad, Levente Buttyan, Mario Cagalj, Virgil Gligor, Markus Jakobsson, Daniel Jungels, Tim Leinmüller, Christof Paar, Panos Papadimitratos, and Hans-Jörg Vögel for their helpful feedback on earlier versions of this work.

We thank also the students Julien Freudiger and Florent Garcin for contributing to the work on sophisticated attacks and authentication mechanisms, respectively.

References

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

[2] http://www.sevecom.org/.

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

[4] IBM 4758 PCI Cryptographic Coprocessor, http://www-03.ibm.com/security/cryptocards/pcicc/overview.shtml.

[5] Trusted Platform Module (TPM), https://www.trustedcomputinggroup.org/groups/tpm/.

[6] IEEE P1609.2/D2 – Draft Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages, November 2005.

[7] J. Blum and A. Eskandarian, The threat of intelligent collisions, *IT Professional* **6**(1) (2004), 24–29.

[8] C. Boyd and A. Mathuria, *Protocols for Authentication and Key Establishment*, Springer, 2003.

[9] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh and J.-M. Tang, Framework for security and privacy in automotive telematics, in: *Proceedings of the 2nd International Workshop on Mobile Commerce*, 2002, pp. 25–32.

[10] S. Eichler, J. Billion, R. Maier, H.-J. Voegel and R. Kroh, On providing security for an open telematics platform, in: *Proceedings of the 5th International Conference on ITS Telecommunications*, 2005.

[11] P. Enge, Retooling the Global Positioning System, *Scientific American* (May) (2004).

[12] W. Enkelmann, FleetNet – applications for inter-vehicle communication, in: *Proceedings of the IEEE Intelligent Vehicles Symposium'03*, 2003, pp. 162–167.

[13] I. Furgel and K. Lemke, A review of the digital tachograph system, in: *Proceedings of the Workshop on Embedded Security in Cars (escar)'04*, 2004.

[14] M. Gerlach, VaneSe – An approach to VANET security, in: *Proceedings of V2VCOM'05*, 2005.

[15] L. Gollan and C. Meinel, Digital signatures for automobiles, in: *Proceedings of Systemics, Cybernetics and Informatics (SCI)'02*, 2002.

[16] P. Golle, D. Greene and J. Staddon, Detecting and correcting malicious data in VANETs, in: *Proceedings of VANET'04*, 2004, pp. 29–37.

[17] H. Harney and C. Muckenhirn, Group Key Management Protocol (GKMP) architecture, RFC 2094, 1997.

[18] Y.-C. Hu and A. Perrig, A survey of secure wireless ad hoc routing, *IEEE Security & Privacy* **2**(3) (2004), 28–39.

[19] Y.-C. Hu, A. Perrig and D. Johnson, Ariadne: a secure on-demand routing protocol for ad hoc networks, in: *Proceedings of Mobicom'02*, 2002, pp. 12–23.

[20] Y.-C. Hu, A. Perrig and D.B. Johnson, Packet leashes: A defense against wormhole attacks in wireless networks, in: *Proceedings of IEEE Infocom'03*, 2003.

[21] J.-P. Hubaux, S. Capkun and J. Luo, The security and privacy of smart vehicles, *IEEE Security and Privacy Magazine* **2**(3) (2004), 49–55.

[22] M. Jakobsson, Privacy vs. Authenticity, PhD thesis, University of California at San Diego, 1997.

[23] D. Jungels, M. Raya, I. Aad and J.-P. Hubaux, Certificate revocation in vehicular ad hoc networks, Technical Report LCA-REPORT-2006-006, EPFL, 2006.

[24] M. Kuhn, An asymmetric security mechanism for navigation signals, in: *Proceedings of the 6th Information Hiding Workshop*, 2004.

[25] A.K. Lenstra and E.R. Verheul, Selecting cryptographic key sizes, *Journal of Cryptology* **14**(4) (2001), 255–293.

[26] M. Lott, R. Halfmann, E. Schultz and M. Radimirsch, Medium access and radio resource management for ad hoc networks based on UTRA TDD, in: *Proceedings of Mobihoc'01*, 2001, pp. 76–86.

[27] K. Matheus, R. Morich, I. Paulus, C. Menig, A. Lübke, B. Rech and W. Specks, Car-to-Car Communication – Market introduction and success factors, in: *Proceedings of ITS'05: 5th European Congress and Exhibition on Intelligent Transport Systems and Services*, 2005.

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

[29] B. Parno and A. Perrig, Challenges in securing vehicular networks, in: *Proceedings of the Workshop on Hot Topics in Networks (HotNets-IV)*, 2005.

[30] A. Perrig, R. Canetti, J.D. Tygar and D. Song, The TESLA broadcast authentication protocol, in: *Proceedings of RSA CryptoBytes'02*, 2002.

[31] S. Rafaeli and D. Hutchison, A survey of key management for secure group communication, *ACM Computing Surveys* **35**(3) (2003), 309–329.

[32] M. Raya, A. Aziz and J.-P. Hubaux, Efficient secure aggregation in VANETs, in: *Proceedings of VANET'06*, 2006.

[33] M. Raya and J.-P. Hubaux, The security of vehicular ad hoc networks, in: *Proceedings of SASN'05*, 2005, pp. 11–21.

[34] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura and K. Sezaki, CARAVAN: providing location privacy for VANET, in: *Proceedings of the Workshop on Embedded Security in Cars (escar)'05*, 2005.

[35] P. Samuel, Of sticker tags and 5.9 GHz, in: *ITS International*, 2004.

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

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

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

[39] M. Wolf, A. Weimerskirch and C. Paar, Security in automotive bus systems, in: *Proceedings of the Workshop on Embedded Security in Cars (escar)'04*, 2004.

[40] Q. Xu, T. Mak, J. Ko and R. Sengupta, Vehicle-to-vehicle safety messaging in DSRC, in: *Proceedings of VANET'04*, 2004, pp. 19–28.

[41] X. Yang, J. Liu, F. Zhao and N. Vaidya, A vehicle-to-vehicle communication protocol for cooperative collision warning, in: *Proceedings of MobiQuitous'04*, 2004.

[42] M. El Zarki, S. Mehrotra, G. Tsudik and N. Venkatasubramanianm, Security issues in a future vehicular network, in: *Proceedings of European Wireless'02*, 2002.