Securing Vehicular Networks

Maxim Raya, Panos Papadimitratos, Jean-Pierre Hubaux
Laboratory for computer Communications and Applications (LCA)
School of Computer and Communication Sciences
EPFL, Switzerland
Email: {maxim.raya, panos.papadimitratos, jean-pierre.hubaux}@epfl.ch

***Abstract*— This poster will describe the security problems of the emerging vehicular networks. It will also outline the solution architecture and several of its components.**

I. Introduction

Vehicular networks will enable a variety of applications for *safety*, *traffic efficiency and driver assistance*, and *infotainment*. For example, warnings for environmental hazards (e.g., ice on the pavement) or abrupt vehicle kinetic changes (e.g., emergency breaking), traffic and road conditions (e.g., congestion or construction sites), and tourist information downloads will be provided by these systems.

Vehicular networking protocols will allow nodes, that is, vehicles or road-side infrastructure units, to communicate with each other over single or multiple hops. In other words, nodes should act both as end points and routers, with vehicular networks emerging as the first commercial instantiation of the *mobile ad hoc networking* technology.

The self-organizing operation and the unique features of vehicular networks are a double-edged sword: a rich set of tools are offered to drivers and authorities, but a formidable set of exploits and attacks becomes possible. Hence, the security of vehicular networks is indispensable, because these systems can make anti-social and criminal behavior easier, in ways that will actually jeopardize the benefits from their deployment. Securing vehicular networking protocols is a hard problem, its solution involves both the industry, governments, and the academia, and can have a broad impact.

Our research focuses on the design and building of secure vehicular networking protocols and systems. We are closely collaborating with other academic and industrial partners within **SEVECOM** (SEcure VEhicular COMmunications), a new EU-funded project that focuses on providing a full definition and implementation of security requirements for vehicular communications.

In the rest of this proposal, we outline vulnerabilities and challenges, the security architecture we propose, and open research problems. More information on this topic can be found at http://ivc.epfl.ch and http://www.sevecom.org.

II. Vulnerabilities and Challenges

A. Vulnerabilities

Any wireless-enabled device that runs a rogue version of the vehicular communication protocol stack poses a threat. We denote such rogue devices deviating from the definition of protocols as *adversaries* or *attackers*. Next, we explore the most significant vulnerabilities of vehicular communications.

Jamming The jammer deliberately generates interfering transmissions that prevent communication. Since the network coverage area, e.g., along a highway, can be well-defined, at least locally, jamming is a low-effort exploit opportunity: an attacker can relatively easily, without compromising cryptographic mechanisms and with limited transmission power, partition the vehicular network.

Forgery Fig. 1 illustrates the fast '*contamination*' of large portions of the vehicular network coverage area with false information: a single attacker forges and transmits false hazard warnings (e.g., ice formation on the pavement), which are taken up by all vehicles in both traffic streams.

In-transit traffic tampering Any node acting as a relay can disrupt communications of other nodes: it can *drop* or *corrupt* messages, or, *meaningfully modify* messages. This way the reception of valuable or even critical traffic notifications or safety messages can be manipulated. Moreover, attackers can *replay* messages, e.g., to illegitimately obtain services.

Impersonation Message fabrication, alteration, and replay can also be used towards impersonation. Consider, for example, an attacker masquerading an emergency vehicle to mislead other vehicles to slow down and yield. Or, an adversary impersonating roadside units, spoofing service advertisements or safety messages.

Privacy With vehicular networks deployed, the collection of vehicle-specific information from overheard vehicular communications will become particularly easy. Then, inferences on the drivers' personal data could be made, and violate her or his *privacy*. Fig. 2 illustrates an eavesdropping attacker (which could even be a service provider), with 'strength' quantified by the number of network traffic sniffing points. The attacker extracts data such as time, location, vehicle identifier, technical descriptions, or trip details, and based on those derive private information.

On-board tampering Beyond exploits of communication protocols, the attacker may select to tinker with data (e.g., velocity, location, status of vehicle parts) at their source. Tampering with the on-board sensing and other hardware (e.g., real-time clocks), may, in fact, be relatively simple.

B. Challenges

The operational conditions, the constraints, and the user requirements for vehicular networks make security a hard

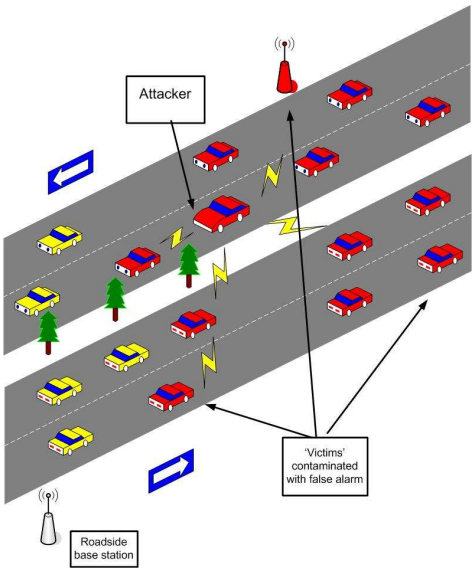

Fig. 1. Message Forgery

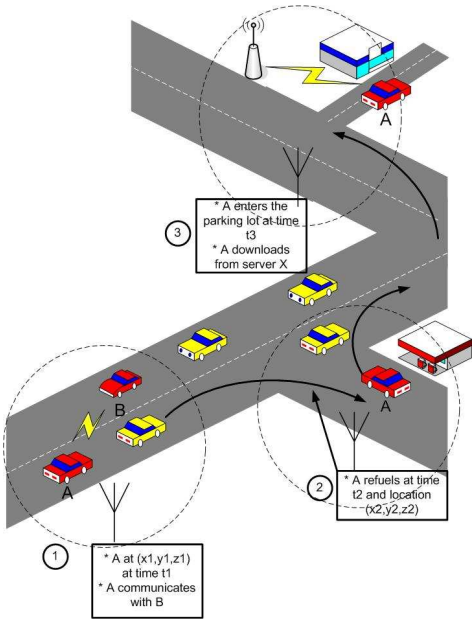

Fig. 2. Vehicle Tracking

problem, facing a number of challenges specific to vehicular networks; the most significant ones are discussed next.

Highly transient associations The associations among nodes can quite often be highly transient and almost *once-in-a-lifetime*. Two vehicles (nodes) traveling on a highway may remain within their transceiver range, or within a few wireless hops, only for few seconds. This means that techniques appropriate for other types of networks, which allow long-lived associations, or user contact, or need to communicate only with few end-points, can be impractical for securing vehicular networks.

Liability vs. Privacy To make the problem harder, accountability, and eventually liability, of the vehicles and their drivers is required. Vehicular communication is envisioned as an excellent opportunity to obtain data that can assist legal investigations (e.g., in the case of accidents). This implies that unambiguous identification of the vehicles should be possible, as sources of messages. Moreover, context-specific information, such as coordinates, time intervals, and associated vehicles, should be possible to extract or reconstruct. But such requirements raise even stronger privacy concerns.

Real-time communication Many of the envisioned safety and driver-assistance applications pose strict deadlines for message delivery or are time-sensitive. This means that security protocols should impose low processing and messaging overhead, and be robust to clogging denial of service attacks.

Vehicular Network Scale With roughly a billion vehicles around the globe, and a multitude of authorities governing transportation systems, the design of a facility that provides cryptographic keys is significant challenge. Especially because vehicles' communication essentially has no administrative boundaries.

III. Security Architecture

In this section, we present the components needed to protect vehicular networks against a wide range of threats. Fig. 3 depicts the general architecture, the components of which are described next.

A. Security hardware

Among the vehicle onboard equipment, two hardware modules, namely the *Event Data Recorder* (EDR) and the *Tamper-Proof Device* (TPD), will be dedicated to security.

The EDR will be responsible for recording the vehicle's critical data, such as position, speed, time, etc., during emergency events, similarly to a plane's black box. It will also record all the received safety messages during these events. This data will help in accident reconstruction and the attribution of liability. The EDR must be tamper-proof; EDRs are already installed nowadays in many road vehicles, especially trucks.

The car electronics can be easily tampered due to their easy accessibility (e.g., by the owner or a mechanic). This is why the cryptographic keys of a vehicle need proper hardware protection, namely a TPD. The TPD will take care of storing all the cryptographic material and performing cryptographic operations, especially signing and verifying safety messages. The TPD can also include its own clock and battery that is periodically recharged from the vehicle's electric circuits.

B. Vehicular Public Key Infrastructure

The huge number of vehicles (there are over 750 million vehicles worldwide today), registered in different countries and traveling long distances well beyond their initial registration region, requires a robust and scalable key management scheme. The involvement of authorities in vehicle registration implies a certain level of centralization. Hence the need for a

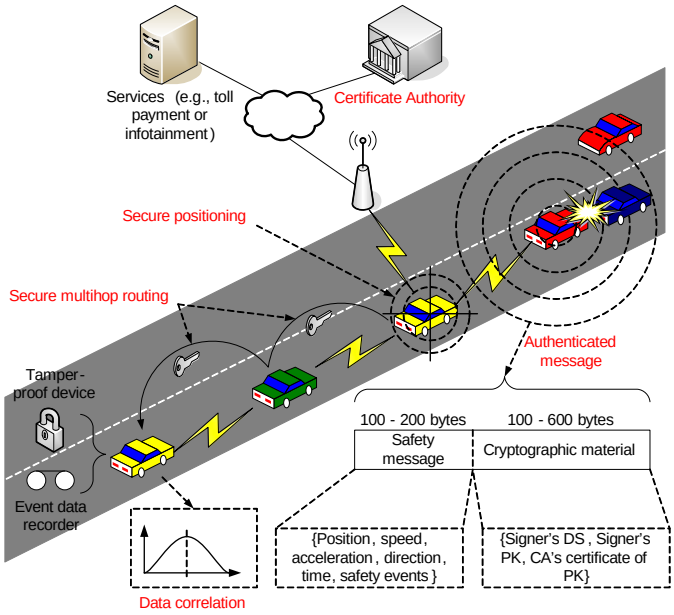

Fig. 3. Overview of the security architecture

Vehicular Public Key Infrastructure (VPKI), where Certificate Authorities (CAs) will issue certified public/private key pairs to vehicles (with many pairs per vehicle for privacy reasons as will be explained in Section III-D). Similarly to current vehicle registration authorities, there will be several CAs, each corresponding to a given region (e.g., country, state, metropolitan area, etc.). Other candidates for taking the role of CAs are car manufacturers. In either case, the different CAs will have to be cross-certified so that vehicles from different regions or different manufacturers can authenticate each other. This will require that each vehicle stores the public keys of all CAs whose certificates it may need to verify.

C. Authentication

The fundamental security functions in vehicular networks will include authentication of the origin of data packets, to solve the *in-transit traffic tampering* and *impersonation* attacks. To achieve this, vehicles will sign each message with their private key and attach the corresponding certificate. Thus, when another vehicle receives this message, it verifies the key used to sign the message and once this is done correctly, it verifies the message. The drawbacks of asymmetric cryptography show up in this basic authentication operation. In fact, using ECC (Elliptic Curve Cryptography), the most compact public key cryptosystem so far, the estimated security overhead of the signature and certificate is around 140 bytes. But it is possible to reduce this overhead by signing only critical messages. In addition, given the frequency of safety message broadcasts (typically, every 300 ms), a vehicle could ignore redundant messages.

D. Privacy

To conceal the vehicle's identity, we propose using a set of anonymous keys that change frequently according to the driving speed. These keys are preloaded in the vehicle's TPD for a long duration, for example, until the next yearly checkup. Each key is certified by the issuing CA and has a short lifetime (e.g., a specific week of the year). In addition, it can be tracked back to the real identity of the vehicle (the Electronic License Plate, ELP) in case law enforcement necessitates this and only after obtaining a permission from a judge. This conditional anonymity will help determine the liability of drivers in the case of accidents. The downside of this approach is the storage space needed for the set of anonymous keys to be used during a whole year; nevertheless, this is feasible with relatively small hard drives (a few Mbytes).

E. Secure positioning

In vehicular networks, position is one of the most important data for vehicular communication protocols and applications. Each vehicle needs to know not only its own position, but also those of other vehicles (e.g., those involved in accidents or traffic jams). Hence, the correctness of positioning information is crucial. GPS is well known to function poorly in microwave signal attenuating environments, such as high building areas, tunnels, valleys, and in some cases bad weather (e.g., when there is a thin film of water on the receiver's antenna). All these factors lead to the conclusion that GPS positioning information cannot be totally trusted. Moreover, vehicles can intentionally lie about their positions. Hence the need for a secure positioning system that will allow vehicles to correctly determine their own as well as other vehicles' positions.

IV. Open problems

There remains a set of unexplored problems directly related to vehicular network security:

Secure routing: the basic safety message dissemination model in vehicular networking consists in local broadcasting of regular or event warning messages. But there are scenarios when messages need to be delivered to specific areas, e.g., to the end of a traffic jam queue so that arriving vehicles have the option of taking another route before getting stuck. In vehicular networks, this can be supported by the geocast primitive that is a form of position-based routing protocols. Yet none of these solutions is secure. But there is rich literature on topology-based secure routing protocols whose applicability to vehicular networks still needs to be investigated.

Data verification helps to prevent the *forgery* attack. This can be achieved by a *data correlation* mechanism that compares all collected data regarding a given event. Such mechanisms still have to be designed.

DoS resilience: DoS attacks, and especially *jamming*, are relatively simple to mount yet their effects can be devastating, bringing down the whole network. Existing solutions like frequency hopping do not completely solve the problem. The use of multiple radio transceivers, operating disjoint frequency bands, can be a feasible approach.