Available online at www.sciencedirect.com

ScienceDirect

Computer Standards & Interfaces 30 (2008) 390 – 397

COMPUTER STANDARDS & INTERFACES

www.elsevier.com/locate/csi

A privacy aware and efficient security infrastructure for vehicular ad hoc networks

Klaus Plößl [*], Hannes Federrath

University of Regensburg, Department of Information Security Management, 93040 Regensburg, Germany

Available online 8 March 2008

Abstract

VANETs have the potential to dramatically increase road safety by giving drivers more time to react adequately to dangerous situations. To prevent abuse of VANETs, a security infrastructure is needed that ensures security requirements like message integrity, confidentiality, and availability. After giving more details on the requirements we propose a security infrastructure that uses asymmetric as well as symmetric cryptography and tamper resistant hardware. While fulfilling the requirements, our proposal is especially designed to protect privacy of the VANET users and proves to be very efficient in terms of computational needs and bandwidth overhead.

Keywords: Vehicular ad hoc network (VANET); Security; Privacy; Cryptography; PKI

1. Introduction

The term vehicular ad hoc network (VANET) is used for a subgroup of mobile ad hoc networks (MANETs, defined in [15]). The distinguishing property of the VANET is that it is formed mainly by vehicles like cars, trucks, buses and motorcycles. This implies that node movement is restricted by factors like road course, encompassing traffic and traffic regulations. Because of the restricted node movement it is a feasible assumption that the VANET will be supported by some fixed infrastructure that assists with some services and can provide access to stationary networks [17]. The fixed infrastructure will be deployed at critical locations like slip roads, service stations, dangerous intersections or places well-known for hazardous weather conditions.

Nodes are expected to communicate by means of North American DSRC standard [12] that employs the IEEE 802.11p standard for wireless communication. To allow communication with participants out of radio range, messages have to be forwarded by other nodes (multi-hop communication). Vehicles are not subject to the strict energy, space and computing capabilities restrictions normally adopted for MANETs [20]. More challenging is the potentially very high speed of the nodes (up to 250 km/h) and the large dimensions of the VANET.

The primary VANET's goal is to increase road safety. To achieve this, the vehicles act as sensors and exchange warnings or – more generally – telematics information (like current speed, location or ESP activity) that enables the drivers to react early to abnormal and potentially dangerous situations like accidents, traffic jams or glaze. In addition, authorized entities like police or firefighters should be able to send alarm signals and instructions e.g. to clear their way or stop other road users. Besides that, the VANET should increase comfort by means of value-added services like location based services or Internet on the road [16].

These three application categories ("warnings and telematics information" (W), "alarm signals and instructions" (A), and "value-added services" (V)) imply different security and privacy requirements with respect to the protection goals integrity, confidentiality and availability. Nevertheless, there is a common need for a security infrastructure establishing mutual trust and enabling cryptography. The security infrastructure therefore includes all technical and organizational measures and facilities needed to provide for the protection goals. After defining the requirements for any such security infrastructure (Section 2) we present a new proposal (Section 3) that particularly aims to protect privacy of the participants and is designed to be very efficient in terms of computing capabilities and communication bandwidth. Our

[*] Corresponding author.
E-mail addresses: klaus.ploessl@wiwi.uni-regensburg.de (K. Plößl), hannes.federrath@wiwi.uni-regensburg.de (H. Federrath).

0920-5489/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2008.03.007

system is evaluated in Section 4. In Section 5 we review related work and Section 6 outlines our conclusion and future work.

2. Security requirements

In this section we explain the requirements for a VANET security infrastructure. If necessary, we distinguish between the three application categories W, A, and V as defined in Section 1. The requirements are summarized in Table 1.

2.1. Integrity

The security infrastructure has to provide mechanisms that prevent or at least detect message modification (I1). This hinders malicious nodes from modifying forwarded messages and protects message integrity for all application categories.

Alarm signals and instructions sent from authorized nodes like police cars, fire engines or ambulances have to be obeyed by the addressees. Therefore, the authenticity and integrity of the message as well as the authorization of the sender must be provable instantly without further information (I2a). In contrast, for warnings and telematics messages plausibility checks can be conducted by means of in car sensors or messages received from other VANET nodes. Hence no unchangeable and unique identity would be necessary in this case. Moreover, to hamper movement profile creation it would be preferable to cloak sender identity especially in periodically sent messages (P1). Nevertheless, ex post accountability and non-repudiation is necessary to be able to prosecute misuse of the VANET like injection of bogus information (I2b). Therefore anonymous participation should not be allowed, pseudonymous participation is desirable.

This ex post identification must only be allowed in severe cases like accidents with death results or sending bogus warnings. Automated traffic surveillance or automated prosecution – e.g. based on the sent telematics data – must not be allowed with regard to multilateral security (P2). Multilateral security means taking the interests of all parties involved into account. In this case, interests of law enforcement (to prosecute each violation of law with as few effort as possible) have to be balanced with interests of citizens (not to be monitored regardless of whether a suspicion exists). It is an interesting question how to define what such severe cases of VANET abuse are. Nevertheless, it will not be answered here because we focus on the technical details of the security infrastructure. We assume that in-car sensor data is correct. Additionally, we expect integration of correct time and position information in all messages to protect against replay and position spoofing attacks. This information is available from an infrastructure like Galileo [10].

Table 1
Requirements

Abbr.	Security Requirement	W	A	V
I1	Data integrity	x	x	x
I2a	Immediate sender authentication		x	
I2b	Ex post accountability	x		x
C1	Different levels of confidentiality	x	x	x
C2	Protection of the security infrastructure	x	x	x
P1	Protection against profile generation	x	x	x
P2	Protection against surveillance	x	x	x
A1	Computational and bandwidth efficiency	x	(x)	x

2.2. Confidentiality

Confidentiality requirements vary heavily between the three application categories. While confidentiality of alarm signals is negligible in most cases, it can e.g. be crucial for services subject to costs. The security infrastructure therefore has to provide mechanisms that support different levels of confidentiality (C1). For example these levels could be no confidentiality, confidentiality against outsiders and confidentiality against all except direct communication partners.

Besides application data administrative messages like routing protocol information or messages containing cryptographic material have to be protected against eavesdropping. Also, the cryptographic information held by participants or centralized instances has to be protected against unauthorized access. More generally, the security infrastructure has to be protected against attacks (C2).

2.3. Availability

Because most VANET messages are related to driving conditions and road safety, real-time processing of these messages is crucial. To be able to fulfill the above integrity and confidentiality requirements VANET nodes have to carry out additional cryptographic operations that extend message processing. Mechanisms to protect message integrity increase the message length. To satisfy the given real-time constraints the mechanisms of the security infrastructure must be as efficient as possible in terms of computational and bandwidth needs (A1). Despite the fact that there is no feasible protection against jamming attacks [24] actions must be taken that complicate denial-of-service attacks and therefore increase availability.

3. Proposal

In this section we present our proposal for a VANET security infrastructure that is designed to be very efficient in terms of computing capabilities and communication band-width while fulfilling all security and privacy requirements. After a once-only initialization it employs asymmetric cryptography within a public key infrastructure (PKI) for messages influencing road safety. All other messages (especially the periodically sent telematics messages) are protected by a system employing symmetric cryptography that is much faster and protects privacy of the participants better than the asymmetric part. After outlining our proposal in Section 3.1 we give some more details on the once-only initialization (Section 3.2) and the symmetric system part (Section 3.3).

Before explaining our proposal in more detail Fig. 1 gives an overview of a VANET with the different message types:

– In the upper right of the picture an accident happened. The involved vehicles start to send accident warnings (AW) protected by asymmetric cryptography. Supporting