Chapter 3.8
Efficient and Reliable Pseudonymous Authentication

Giorgio Calandriello
Politecnico di Torino, Italy

Antonio Lioy
Politecnico di Torino, Italy

ABSTRACT

Privacy, security, and reliability are key requirements in deploying vehicular ad-hoc networks (VANET). Without those the VANET technology won't be suitable for market diffusion. In this chapter, the authors are concerned with how to fulfill these requirements by using pseudonym-based authentication, designing security schemes that don't endanger transport safety while maintaining low overhead. At the same time our design improves the system usability by allowing nodes to self-generate their own pseudonyms.

INTRODUCTION

Vehicular ad-hoc networks (VANET) are composed by mobile nodes, that is, vehicles, and road-side units (RSU) equipped with sensing, processing and communication capabilities, and are deployed to increase road safety and the efficiency of transportation systems through a number of applications, most of which will be based on *beacons,* that is, vehicles disseminating frequently their position, state and eventual situation-dependent warnings (for example, ice on the road).

Such applications are sensible to attacks, for example by injecting false beacons into the network, and can disclose users' personal information or track vehicles, as an attacker collecting VANET data could do. Thus there's the need of security mechanisms and privacy-enabling technologies, which actually are a prerequisite for deployment. Three recent research efforts, the IEEE 1609.2 working group (IEEE1609.2, 2006), the NoW

DOI: 10.4018/978-1-61350-323-2.ch3.8

project (Gerlach *et al*., 2007), and the SeVeCom project (Papadimitratos, Buttyan, Hubaux, Kargl, Kung & Raya, 2007), are currently working on VANET security architectures, whose common mechanism is the use of public key cryptography to protect V2V and V2I messages.

Message authentication, integrity, and non-repudiation, as well as protection of private user information are identified as primary requirements. On one hand, traditional public key cryptography in combination with periodic key changing is known as *pseudonymous authentication,* in which nodes are equipped with multiple credentials, termed *pseudonyms* that do not reveal the node real identity, e.g., as those proposed by Chaum (1985). This prevents messages signed under different pseudonyms to be linked (Armknecht *et al.*, 2007; Raya & Hubaux, 2005; Gerlach, 2005; Raya & Papadimitratos, 2006). On the other hand, g*roup signatures*, that is, cryptographic primitives for *anonymous authentication,* are also applicable to VANET (Ateniese & Tsudik, 1999; Brickell *et al.*, 2004; Chaum & van Heyst, 1991; Syverson & Stubblebine, 1999). This guarantees a stronger level of anonymity as an eavesdropper cannot link *any* two signatures from any node. This property comes at a higher security overhead as it will be explained in the rest of the chapter, while pseudonym-based authentication gathered a warmer and wider acceptance by the research community (Gerlach *et al.*, 2007; IEEE1609.2, 2006; Papadimitratos, Buttyan, Hubaux, Kargl, Kung & Raya, 2007), reason for which our focus in this chapter is on pseudonym-based systems.

In this chapter we investigate technical issues related to the use of pseudonyms in vehicular communications.

First, we ask ourselves how the security overhead can be reduced while maintaining acceptable levels of security and application robustness. Second, do safety applications remain reliable in presence of security mechanisms? Finally, can self-generation of pseudonyms still meet the security and privacy mechanisms? In this chapter, we provide answers to these questions. First we define more precisely the problem at hand and we outline our approach to solve it. Then we analyze the costs of the proposed solutions and their impact on transportation safety.

BACKGROUND

We present the idea of self-generation of pseudonyms in our previous work (Calandriello *et al.*, 2007). Zeng (2006) presents the same approach independent of our work, and Armknecht *et al.* (2007) apply it to VANET. Calandriello *et al*. (2007) show that the proposed optimizations can also be applied to the cryptosystem presented by Zeng (2006).

The work of Raya & Hubaux (2005) presents the main problems and challenges of VANET security, and outlines in detail the Baseline scheme which we summarize in the following. Papadimitratos, Gligor & Hubaux (2006) survey the security requirements of VANET and provide models for the system and the adversaries. We invite the non-specialized reader to refer to the above works for an in-depth introduction to VANET security.

Chaum (1985) presents the original idea of using pseudonyms, while their applicability to VANET has been explored by other studies in the context of the SeVeCom and NoW projects: (Gerlach, 2005; Gerlach *et al.*, 2007; Papadimitratos, Buttyan, Hubaux, Kargl, Kung & Raya, 2007; Raya & Hubaux, 2005). Papadimitratos, Kung, Hubaux & Kargl (2006) discuss in general the issue of privacy in vehicular communications.

A number of works are concerned with different aspects of security and privacy of vehicular networks, either outlining challenges (El Zarki *et al.*, 2002; Parno & Perrig, 2005), describing particular attacks (Blum & Eskandarian, 2004; Jakobsson *et al.*, 2004) or more general attack overviews (Aijaz *et al.*, 2005), offering general suggestions towards solutions (Gerlach, 2005; Raya, Papadimitratos &