Chapter 56
Overview of Security Issues in Vehicular Ad-Hoc Networks

José María De Fuentes
Carlos III University of Madrid, Spain

Ana Isabel González-Tablas
Carlos III University of Madrid, Spain

Arturo Ribagorda
Carlos III University of Madrid, Spain

ABSTRACT

Vehicular ad-hoc networks (VANETs) are a promising communication scenario. Several new applications are envisioned, which will improve traffic management and safety. Nevertheless, those applications have stringent security requirements, as they affect road traffic safety. Moreover, VANETs face several security threats. As VANETs present some unique features (e.g. high mobility of nodes, geographic extension, etc.) traditional security mechanisms are not always suitable. Because of that, a plethora of research contributions have been presented so far. This chapter aims to describe and analyze the most representative VANET security developments.

INTRODUCTION

Nowadays, road traffic activities are one of the most important daily routines worldwide. Passenger and freight transport are essential for human development. Thus, new improvements on this area are achieved every day - better safety mechanisms, greener fuels, etc.

Driving is one of the most incident factors of traffic safety, so there is a clear need to make it safer. Apart from partially automating this task, reliable driver data provisioning is critical to achieve this goal. An accurate weather description or early warnings of upcoming dangers (e.g.

DOI: 10.4018/978-1-60960-042-6.ch056

bottlenecks, accidents) would be highly useful for drivers. For this purpose, a new kind of information technology called **VANET** (**V**ehicular **A**d-hoc **NET**work) is being developed.

VANETs are a subset of MANETs (Mobile Ad-hoc NETworks) in which communication nodes are mainly vehicles. As such, this kind of network should deal with a great number of highly mobile nodes, eventually dispersed in different roads. In VANETs, vehicles can communicate each other (V2V, Vehicle-to-Vehicle communications). Moreover, they can connect to an infrastructure (V2I, Vehicle-to-Infrastructure) to get some service. This infrastructure is assumed to be located along the roads.

Data interchanged over VANETs often play a vital role in traffic safety. For example, in the eCall project, an emergency call is made once in-vehicle sensors detect that an accident has occurred (eSafetySupport, 2007). Such information must be accurate and truthful, as lives could depend on this application. In this way, very stringent security requirements are to be achieved. Moreover, privacy of drivers should be protected – a vehicle should not be easily tracked by unauthorized entities. Satisfying all these security requirements have lead to a great amount of research contributions, each one covering different aspects of data security and privacy.

This chapter offers an overview of the current status of security issues over VANETs. For this purpose, different communication models have been identified and analyzed from the security point of view. Moreover, security requirements and potential attacks will be studied. Finally, the security developments to achieve such requirements will be analyzed. In this way, the reader will identify the current trends in data security proposed to solve not only traditional problems (e.g. data confidentiality) but also some context-specific ones (e.g. eviction of misbehaving vehicles from the VANET).

Chapter organization. On Section II, a typical VANET model is explained, covering the existing entities and their relationships. Different communication models will be identified as well. Section III presents the security requirements that must be achieved in VANETs and particularly in each communication model. Section IV shows a classification of attacks identified on VANETs. Section V analyzes the main security mechanisms proposed to achieve the security requirements previously introduced. Finally, Section VI sums up the main conclusions and lessons learned from this work, and points out future research directions on VANET security.

VANET MODEL OVERVIEW

There are many entities involved in a VANET settlement and deployment. Although the vast majority of VANET nodes are vehicles, there are other entities that perform basic operations in these networks. Moreover, they can communicate with each other in many different ways. In this Section we will firstly describe the most common entities that appear in VANETs. In the second part, we will analyze the different VANET settings that can be found among vehicles, and among vehicles and the remaining entities.

Common VANET Entities

Several different entities are usually assumed to exist in VANETs. To understand the internals and related security issues of these networks, it is necessary to analyze such entities and their relationships. Figure 1 shows the typical VANET scheme.

As seen on Figure 1, two different environments are generally considered in VANETs:

- **Infrastructure environment**. In this part of the network, entities can be permanently interconnected. It is mainly composed by those entities that manage the traffic or offer an external service. On one hand,