Chapter 11
Analyzing the Trade-Offs Between Security and Performance in VANETs

Jetzabel Serna
Universitat Politècnica de Catalunya (UPC), Spain

Jesus Luna
Technische Universitaet Darmstadt, Germany

Roberto Morales
Universitat Politècnica de Catalunya (UPC), Spain

Manel Medina
Universitat Politècnica de Catalunya (UPC), Spain

ABSTRACT
Vehicular Ad-hoc NETworks (VANETs) currently provide a prominent field of research, which aims at improving everyday road safety and comfort. To achieve this, the deployment of several potential applications is envisioned, promising to provide extraordinary benefits, but will also represent important security challenges due to the unique characteristics of VANETs. In this chapter, VANET’s security issues are addressed, and the most outstanding security approaches are discussed. As a proof of concept, a PKI-based protocol, able to cope with the interoperability issues among untrusted CA domains is presented, and the trade-offs between security and performance are empirically analyzed and stressed.

INTRODUCTION
Vehicular Ad Hoc Networks (VANETs) are a subgroup of Mobile Ad hoc Networks (MANETs) and the technical basis of Intelligent Transportation Systems (ITS). The basic architecture of a VANET consists of vehicles and Road Side Units (RSUs), and the communications among them are classified as vehicle-to-vehicle (v2v) and vehicle-to-infrastructure (v2i). In VANET communication, the information exchanged among vehicles plays a fundamental role; the timely and accurate exchange of safety-related information could prevent a great number of fatal road acci-
Analyzing the Trade-Offs Between Security and Performance in VANETs

In any safety-related vehicular application, the information transmitted among vehicles is considered critical; thus, without security, an attacker could manipulate the information and potentially cause harm. Therefore, security is of utmost importance in order to prevent potential security attacks. Moreover, since vehicles in a VANET also benefit from accessing a wide number of infotainment applications offered by different Service Providers (SPs), confidentiality and privacy should also be provided by the infrastructure, which also plays an important role in any VANETs’ architectural solution.

The adoption of Public Key Infrastructure (PKI) technology, which has been proven to be a suitable solution in other distributed environments, will enable the establishment of secure communication channels, by providing services needed to prevent a wide range of security attacks. Current PKI systems consist of a Central Authority (CA) responsible for registering users and issuing credentials (containing the corresponding private and public key-pair). In VANETs, it is envisioned that vehicles will be registered with their own regional CA, and therefore a common architecture will require a wide range of CAs within regional scopes. Thus, when a vehicle travels to a different geographical region or domain, it is assumed that mutual authentication and trusted communication will be achieved thanks to previous cross-certification agreements (mostly manual). However, since certificate revocation is also the responsibility of the issuing CA, a disadvantage of cross-certification is that it is not possible to obtain up-to-date revocation information, which opens a vulnerability window for the relying party that must be considered.

Apart from the revocation issues just mentioned, and despite the benefits of enabling the use of PKI technologies in VANETs, due to the high mobility of vehicles, the system introduces different network constraints that should be taken into account for the overall security design. A successful deployment must process and transmit the information within the timing and communications parameters limited by the network, thus, the need of carefully designing a suitable security solution, able to meet the VANET’s performance requirements, especially those related to the bandwidth usage and the processing overhead.

The aim of this chapter is to provide an overview of VANETs’ authentication and interoperability challenges related with the use of several and possibly untrusted Certification Authorities. Via a set of empirical results, this chapter further analyzes the trade-offs between security and performance on the use of a PKI-based protocol, proposed by our research in order to cope with these security problems.

BACKGROUND

VANETs represent the most relevant form of MANETs and their successful deployment will allow the implementation of several interesting applications, primarily aimed at improving road’s overall safety and also capable of enhancing driver comfort. In this section we will first briefly introduce VANETs’ basic components and applications, and discuss the reasons why despite their potential benefits, VANETs also raise important security implications that must be solved. An extensive review of the literature focusing on VANETs’ authentication is then presented in the second part of this section.

VANET’s Components and Applications

In the VANET’s basic architecture, mobile nodes are represented by vehicles and fixed nodes by the infrastructure’s RSUs. Vehicles in a VANET are assumed to be equipped with processing, recording and communication features, capable of processing and storing a great amount of information. According to the Dedicated Short Range Communications - DSRC standard (Lee Armstrong),
17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:

www.igi-global.com/chapter/analyzing-trade-offs-between-security/62815?camid=4v1

This title is available in InfoSci-Books, InfoSci-Multimedia Technologies, Communications, Social Science, and Healthcare, InfoSci-Select, InfoSci-Media and Communication Science and Technology. Recommend this product to your librarian:

www.igi-global.com/e-resources/library-recommendation/?id=1

Related Content

Management of Distributed Project Teams in Networks

www.igi-global.com/chapter/management-distributed-project-teams-networks/49811?camid=4v1a

The Network-Extended Mind

www.igi-global.com/chapter/network-extended-mind/42525?camid=4v1a

Throughput Modeling, Analysis, and Optimization in Cognitive Wireless Networks

www.igi-global.com/chapter/throughput-modeling-analysis-optimization-cognitive/69221?camid=4v1a

Cross Layer Design for Multimedia Transmission over Wireless Networks

www.igi-global.com/chapter/cross-layer-design-multimedia-transmission/45257?camid=4v1a