IGI PUBLISHING **ITJ 4692**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, International Journal of Ambient Computing and Intelligence, Volume 1, Issue 1
edited by **Kevin Curran © 2009, IGI Global**

Vehicular Networks Security: Attacks, Requirements, Challenges and Current Contributions

Christian Tchepnda, Orange Labs-France Telecom Group, France

Hassnaa Moustafa, Orange Labs-France Telecom Group, France

Houda Labiod, Institut Telecom–Telecom ParisTech, France

Gilles Bourdon,Orange Labs-France Telecom Group, France

ABSTRACT

This article provides a panorama on the security in vehicular networks' environments. The special characteristics of these environments are presented and a general classification for the different types of attacks illustrated by some relevant attacks examples is introduced. Consequently, some key security requirements and security challenges are derived, considering Intelligent Transportation System (ITS) or Safety services as well as non-ITS or non-Safety services. Finally, some existing contributions in this subject are presented, and their deployment feasibility is discussed.

Keywords: *attacks; related works; security challenges; security requirements; vehicular communications security; vehicular networks security*

INTRODUCTION

Vehicular communication is an emerging class of mobile communication enabling mobile users in their vehicles to communicate to the road and to each other. Currently, Inter-Vehicle Communication Systems (IVCS) are widely discussed, attracting considerable attention from the research community as well as the automotive industry. In fact, vehicular networks are expected to be massively deployed in the near future, driven by navigation safety requirements and by the investments of car manufacturers and Public Transportation Authorities. New standards are emerging for vehicular communications. Dedicated Short Range Communications (DSRC) is a block of spectrum in the 5.850 to 5.925 GHz band allocated by the US Federal Communications Commission (FCC) to vehicular communications (5.9 GHz DSRC). Consensus around the world is emerging around a customized version of IEEE 802.11 in the 5GHz band also known as 802.11p or WAVE (Wireless Access for the Vehicular Environment). Vehicular networks have special behavior and characteristics, distinguishing them from

other types of ad-hoc networks. The nodes' (vehicles') mobility in these networks is high and may reach up to 200Km/h, these networks may experience frequent disconnections and impaired propagation channel resulting in a highly bandwidth constrained environment, these networks performance and motion patterns are closely interdependent, these networks topologies are dynamic but constrained by roads' topologies, these networks may scale to a very large number of nodes (vehicles) according to the traffic condition and finally these networks probably have a potentially heterogeneous administration. We can assume that vehicular communications, opposing the wireless mobile communications, are not resource constrained (energy, CPU, memory, etc.) as vehicles are not tiny nodes and are capable of providing large resources.

Although, vehicular networks are considered as one of the promising concrete applications of ad hoc networks, their special behavior and characteristics create some communication challenges (for network operators and service providers), which can greatly impact the future deployment of these networks. An important research and development aspect in vehicular communication concerns the development of security mechanisms that allow trust among the communicating parties (whether vehicles or infrastructure elements) and guarantee only authorized users' access to network resources and services offered by the provider as well as secure data transfer. In fact, security requirements differ according to the type of applications/services, where different security levels are needed. We notice that vehicular communication security is a young research domain, showing few contributions and lacking concrete security solutions.

This article gives a panorama on vehicular communication security. We discuss the different types of attacks in this environment and present from a deployment perspective the security requirements that should be satisfied, taking into consideration safety applications and commercial applications expected in the future. The remainder of this article is organized as follows: Section 2 figures out services and potential architectures in vehicular networks. Section 3 presents a classification for potential attacks giving some attacks examples. Section 4 introduces our view of the main security requirements and security challenges for vehicular communications deployment. In Section 5, we give an overview on the related work discussing the main contributions and mentioning their limitations as well as some open issues. Finally, the article is concluded in Section 6.

SERVICES AND ARCHITECTURES

Services

Vehicular communications are expected to provide a wide set of useful services to drivers and passengers. We classify these services into two main classes: i) Intelligent Transportation System (ITS) or Safety services, ii) non-ITS or non-Safety services. ITS was the main objective in the emergence of vehicular communications, where the primary works aimed at providing ITS solutions. ITS target is to minimize accidents and improve traffic conditions through providing drivers and passengers with useful information, e.g. road conditions alarms, congestions alarms, fire alarms, accident-ahead warnings, speed limit reminder, and traffic messages' exchange that is useful in avoiding collision at intersection, optimizing traffic flows, and avoiding crash situations.

On the other hand, non-ITS services aim at providing commercial, leisure and convenience services. Non-ITS services have taken recent attention in vehicular communications, being a target of some recent research contributions in this domain. Such services should guarantee data transfer between vehicles and are expected to provide passengers and drivers with Internet connections facility exploiting an available infrastructure in an "on-demand" fashion. Examples of useful non-ITS services are: electronic tolling system, multimedia services (*e.g.*