Chapter 8.4
Emerging Security Issues in VANETs for E-Business

S. S. Manvi
REVA Institute of Technology and Management, India

M. S. Kakkasageri
Basaveshwar Engineering College, India

ABSTRACT

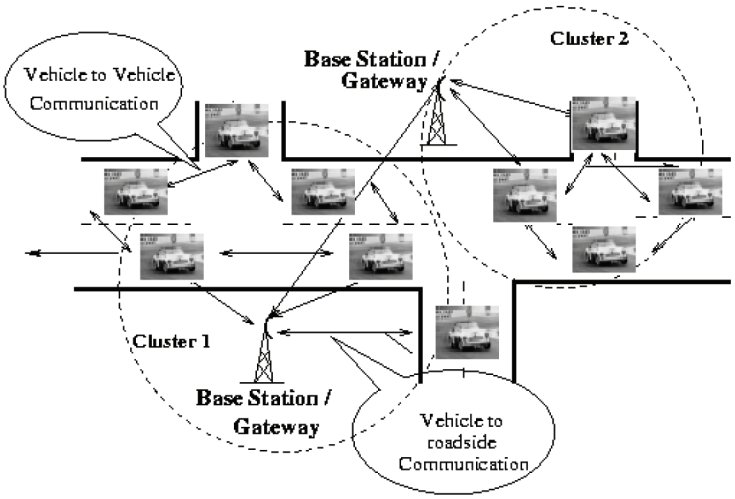
This chapter presents the emerging security issues in Vehicular Ad hoc Networks (VANETs) for e-business along with some of the solutions provided by the research community. The VANET will facilitate new applications for e-business that will revolutionize the driving experience, providing everything from instant, localized traffic updates to warning signals when the vehicle ahead abruptly brakes. In the emerging global economy, e-business has increasingly become a necessary component of business strategy and a strong catalyst for economic development. In near future, vehicles may be equipped with short-range radios capable of communicating with other vehicles and highway infrastructure using a VANET. However, providing security in VANETs for e-business raises privacy concerns that must be considered. The deployment of VANETs for e-business is rapidly approaching, and their success and safety will depend on viable security solutions acceptable to consumers, manufacturers and governments.

INTRODUCTION

VANET is a form of Mobile Ad-hoc NETwork (MANET) that provides communications between vehicles and external network infrastructure. VANETs are expected to have great potential to improve both traffic safety and comfort in the future (Murat, 2005; Holgar, 2005; Sascha, 2006). E-business can be conducted over VANET to facilitate business activities among users traveling in the vehicles. It is a process that relies on an automated information system. E-business methods enable companies to link their internal and external data processing systems more efficiently and flexibly, to work more closely with suppliers

DOI: 10.4018/978-1-61350-323-2.ch8.4

Figure 1. A typical VANET scenario



and partners, and to better satisfy the needs and expectations of their customers.

VANET has become a promising field of research since the world is advancing towards the vision of Intelligent Transportation Systems (Sascha, 2004; Manvi, 2006; Manvi 2007).

Vehicles (or nodes) in VANET are assumed to be equipped with the following.

- GPS (Global Positioning System) receiver enabling the vehicle to track its own location.
- Onboard computing devices allowing the vehicle to perform simple calculations including encryption and other vehicle's positions.
- Communication devices (Direct Short Range Communication compliant) to propagate/receive information.
- Equipment enabling to verify neighbor's position and identify obstacles.
- A set of sensors reporting crashes, engine statistics, weather conditions, etc.
- Pre-stored digital maps.
- Dedicated and secured memory.
- Its own clock to obtain an accurate timestamp.

VANET enables communications between nearby vehicles (V2V communications) and the roadside infrastructure (V2I communications). While using mostly V2V communications, VANET does not entirely rely on a fixed infrastructure, but can harness it for improved performance and functionality when it is available. A typical VANET scenario is as shown in Figure 1. Vehicle to vehicle and vehicle to roadside base station/gateway communication is required for providing safety and other information services to vehicle users. Group of vehicles together may form a cluster to disseminate information among themselves as well as to other clusters and base stations.

Safety applications require reliable delivery of emergency warning messages with high reliability and low latency constraints to nearby and approaching vehicles. However, existing IEEE 802.11x standards fall short of what is required for high-speed VANET applications. In order to provide latency minimization, message prioritization, and elements of security (authorization and anonymity), in 1999, the Federal Communication Commission has allocated 75 MHz of spectrum in the 5.9 GHz band for Dedicated Short Range Communications (DSRC or 802.11p) for VANET