Computer Communications 44 (2014) 1–13

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

VANET security surveys

Richard Gilles Engoulou, Martine Bellaïche *, Samuel Pierre, Alejandro Quintero

Département de Génie Informatique et Logiciel, École Polytechnique de Montréal 2900, Boulevard Edouard-Montpetit, Montréal QC H3T 1J4, Canada

ARTICLE INFO

Article history:
Received 11 July 2013
Received in revised form 23 February 2014
Accepted 27 February 2014
Available online 11 March 2014

Keywords:
Security
Vehicular ad hoc networks
Malicious nodes
VANETs

ABSTRACT

Vehicular ad hoc networks (VANETs), a subset of Mobile Ad hoc NETworks (MANETs), refer to a set of smart vehicles used on the road. These vehicles provide communication services among one another or with Road Side Infrastructure (RSU) based on wireless Local Area Network (LAN) technologies.

The main benefits of VANETs are that they enhance road safety and vehicle security while protecting drivers' privacy from attacks perpetrated by adversaries. Security is one of the most critical issues related to VANETs since the information transmitted is distributed in an open access environment.

VANETs face many challenges. This paper presents a survey of the security issues and the challenges they generate. The various categories of applications in VANETs are introduced, as well as some security requirements, threats and certain architectures are proposed to solve the security problem. Finally, global security architecture for VANETs is proposed.

1. Introduction

A vehicular ad hoc network is a specific type of Mobile Ad hoc NETwork (MANET) that provides communication between nearby vehicles and roadside equipment [1–3]. In this type of network, vehicles are considered communication nodes that are able to belong to a self-organizing network without prior screening or knowledge of each other's presence [4]. There are two categories of nodes: On-Board Units (OBUs) and Road Side Units (RSUs). OBUs are radio devices installed in vehicles that move, while RSUs are placed along the road and constitute the network infrastructure. RSUs work as a router between the vehicles. Using Dedicated Short Range Communication (DSRC) radios, OBUs can link the vehicle to RSUs [5].

VANETs are becoming the most relevant wireless mobile technology. It is one of the promising approaches to implement Intelligent Transportation Systems (ITS). VANETs differ from MANETs in many ways: high node mobility, large scale of networks, a geographically constrained topology that is highly dynamic, strict real time deadline, unreliable channel conditions, unavoidably slow deployment, sporadic connectivity between nodes, driver behavior and frequent network fragmentation [1,2,6]. The goal of VANETs is to allow communication between vehicles. Thus, these nodes need to incorporate radio interfaces for communication and a specific range spectrum must be dedicated for VANET data exchange.

In order to be an integral component of a VANET and to communicate efficiently, nodes need certain features that will help them to gather information, to inform their neighbors and to make decisions by considering all of the collected information. Such features are sensors, cameras, on-board computers, Global Positioning System (GPS) receivers, Event Data Recorders (EDR) and omnidirectional antennas [7].

VANET technology presents certain advantages, such as a reduction in the number of road accidents, a more enjoyable driving and traveling experience with the simplification of certain payment processes for tolls, parking, fuel, etc. Road users employ various applications for safety and efficiency, traffic management, infotainment, warning, comfort, maintenance, music sharing and network gaming [8]. These applications involve the exchange of messages such as emergency message distribution, traffic incidents and road condition warnings that enhance traffic safety and driving efficiency. These applications require data communication between nodes. The content of the message can have an impact on drivers' behavior. This may change the network topology and security may be threatened if a malicious user alters the message [9]. Some possible attacks could cause traffic jams, spread bogus information, cheat the positioning information, disclose IDs, replay, masquerade or forge data, violate privacy or cause wormholes, Denial-of-Service (DoS) attacks, in-transit traffic tampering, impersonation as well as hardware tampering [2].

* Corresponding author.
E-mail addresses: richard.engoulou@polymtl.ca (R.G. Engoulou), martine.bellaiche@polymtl.ca (M. Bellaïche), samuel.pierre@polymtl.ca (S. Pierre), Alejandro.quintero@polymtl.ca (A. Quintero).

http://dx.doi.org/10.1016/j.comcom.2014.02.020
0140-3664/