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/

Another challenge concerns users' privacy: drivers will not accept to be tracked by a central system such as a big brother program, yet some security solutions may threaten users' privacy.

In this paper, we shall classify the attacks according to their characteristics, the requirements involved, and the defences that could be used. A description of the type of attackers will also be introduced. Presenting security threats while keeping in mind all of the other aspects involved in such attacks consists of a new approach. A global security architecture in VANETs will also be proposed. Moreover, we plan to classify VANETs' threats while considering the security layer level in the system.

This paper is structured as follows: Section 2 presents VANET's architectures and their characteristics, Section 3 inventories the relevant challenges and Section 4 discusses VANETs' applications. In Section 5, security requirements are examined, while security threats are presented in Section 6. Section 7 paints a portrait of the attackers' profiles. Section 8 lists the attack characteristics while Section 9 presents users' privacy issues and Section 10 offers some security solutions. Finally, Section 11 proposes a global security architecture.

2. VANET architecture and characteristics

VANET architecture can be divided into three categories: the cellular/WLAN, ad hoc and hybrid architectures [2].

If the infrastructure consists of a cellular gateway or a WLAN or a WIMAX access point, the network will be considered a pure cellular/WLAN.

When no infrastructure is available, the nodes must communicate with one another without relying on an infrastructure. This denotes a pure ad hoc architecture.

Sometimes, various access points, such as cellular gateways, will be available for communication. In this case, nodes can communicate with these infrastructures or they may also communicate directly with one another. This is called a hybrid architecture.

VANETs have many unique characteristics and some of them are presented in this section. First of all, the channel characteristics will be introduced. Secondly, we will present some equipments that helps vehicles to be smart and that enable them to communicate. Finally, the relationship between the vehicles and their infrastructures will be addressed.

2.1. Channel characteristics

In 1999, the United States Federal Communications Commission (FCC) allocated a block of spectrum in the 5.850–5.925 GHz for Vehicular Communications (VC). In Japan, the 700 MHz band is used and similar bands have been attributed in Europe. For the same purpose, a bandwidth of 75 MHz has also been allocated by the FCC for this kind of communication which is referred to as DSRC (Dedicated Short Range Communication) [4]. DSRC is based on IEEE 802.11 technology which is about to become the standard under the name 802.11p [6]. This standard, which is specified for VANETs, uses a 10 MHz channel. The data rate ranges between 3 and 27 Mbps for each channel [10].

Vehicles send periodic information to their neighbors by beacon packets with a required frequency of 10 messages per second and within a maximum range of 150 m.

2.2. On-board equipment

On-board equipment installed in vehicles makes them smart and provides them with the means to communicate [11,12]. They consist of different equipments in vehicle.

An Event Data Recorder (EDR) records transmissions and receives messages and all of the events that occurred in the vehicle environment during the trip. A Global Positioning System (GPS) receiver communicates the geographic location, the speed, the direction of the movement and the node acceleration at specified time intervals. A computing device is used to take appropriate actions in response to messages received from other nodes. Radars and sensors are used to detect obstacles in the vehicle environment. An omnidirectional antenna is used to access wireless channels. An Electronic License Plate (ELP) is installed on every new vehicle in the factory. It provides an ID number used by the police or any official order [3].

2.3. Relationship between Vehicles and their Infrastructures

In a VANET system, some entities such as Regional Transportation Authorities (RTAs), Network Authorities (NAs), Law Enforcement Authorities (LEAs) and roadside infrastructure consist of border RSUs for pseudonym management, simple and regular RSUs for Internet access and users' vehicles [4,13]. In this system, the RSUs provide infrastructure access and network services. They are operated by third-party service providers. Service providers have business contracts with the RTA to build access infrastructure in the RTA's region. Therefore, RSUs are not owned by the RTA although border RSUs are owned and operated by the RTA and they act as the agents delegated with the RTA's authority.

There are three types of communication to consider in VANETs (see Fig. 1): Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) and Infrastructure-to-Vehicle (I2V).

In V2V communication, vehicles can communicate with each other directly in wireless range or indirectly in a multi-hop mode. For example, when a car using V2V communication encounters a dangerous situation, it communicates with other cars and provides useful information, by suggesting that they avoid the area. Furthermore, V2V communication can be classified into two distinct categories depending on the positions of the sender and the receiver: single-hop and multi-hop. The vehicle's local broadcasts send

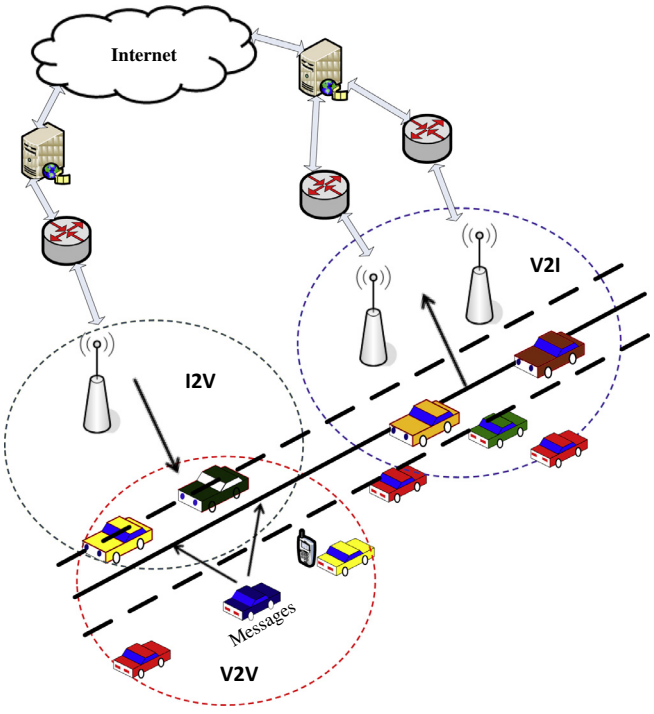

Fig. 1. System architecture in VANETs.