Performance Evaluation 87 (2015) 47–59

Contents lists available at ScienceDirect

Performance Evaluation

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

DJAVAN: Detecting jamming attacks in Vehicle Ad hoc Networks

Lynda Mokdad [a], Jalel Ben-Othman [b,*], Anh Tuan Nguyen [a]

[a] LACL, University of Paris-Est, France
[b] L2TI, University of Paris 13, France

ARTICLE INFO

Article history:
Available online 18 February 2015

Keywords:
Vehicular Ad hoc Networks (VANET)
DOS attacks
Jamming
Greedy behavior
Packet delivery ratio (PDR)
Markov chains

ABSTRACT

With development of wireless communications in the two last decades, new infrastructures have been developed. One of them is the Vehicular Ad hoc Networks (VANETs). They are considered as ad hoc networks with the particularity that the topology is always changed, that make more complicated the resource management and open some beaches in security. Specifically on the Physical and MAC layers that are more vulnerable as they are built on distributed systems and a fluctuating radio channel. Thus, it is not easy to know when transmitted data are not delivered to the destination, if this is due to an attack or to a propagation problem. In this study, we propose a new algorithm DJAVAN (solution of Detecting Jamming Attacks in Vehicle Ad Hoc Networks) to detect a jamming attack in VANETs using the Packet Delivery Ratio (PDR) and with the performance analysis, we determine the threshold that can make the difference between an attack and a poor radio link.

1. Introduction

IEEE 802.11 has been developed to allow devices to communicate wirelessly. Physical layer of IEEE 802.11 is independent of MAC layer. Physical layer allows to communicate at different frequencies such as ISM bands (2.4 GHZ) and UNII band (5GHZ) and can operate in (Direct Sequence Spread Spectrum) DSSS or FFHSS (Fast Frequency Hopping Spread Spectrum) mode as well. On MAC layer, IEEE 802.11 includes DCF (Distributed Coordination Function) using CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) protocol. This protocol is based on the non-persistent CSMA and explicit acknowledge. Using the explicit acknowledge, the MAC and LLC layers are ensured during the transmission of data. Another specificity of IEEE 802.11, is that it is built as a distributed algorithm that is executed locally on each node to determine whether the access time periods to the channel. Since the development of IEEE 802.11, new configurations and modes have been developed as Ad hoc, Mesh modes, and recently Vehicular Ad hoc Networks. All these, use the basic concept of IEEE 802.11 with specific functions adapted to the configuration. In this paper, we have focused on VANET networks. Vehicular ad hoc network (VANET) is a specific case of mobile ad hoc network (MANET) in which the participants nodes are vehicles [1]. VANET networks are enable to communicate between vehicles (V2V) and/or between vehicle and infrastructure (V2I) in the high-speed environment on the frequency of approximately 5.9 GHz. It can be defined as an Ad Hoc network with a dynamic topology as the nodes are vehicles and a topology can be changed when a car get in or out the topology. Beside, using this mode, vehicles can directly communicate with each other without any infrastructure. Thus, VANET can be defined

* Corresponding author.
E-mail addresses: lynda.mokdad@univ-paris12.fr (L. Mokdad), tuan.ant117@gmail.com (A.T. Nguyen).

http://dx.doi.org/10.1016/j.peva.2015.01.003
0166-5316/

as a collection of vehicles hosts with wireless network interfaces. It forms a temporary topology network without any fixed infrastructure or centralized administration. In these networks, vehicles are equipped with wireless transmitters/receivers using antennas that can be omnidirectional that can broadcast on the vehicle coverage, and/or directional in the case or only point to point communication is tackled. Beside, the system can be viewed as a random graph at a specific time. This random graph is due to the vehicle movements, their transmitter/receiver coverage patterns, the power levels of transmission, and the co-channel interference levels. Doppler effects should be considered as well with the different speeds of vehicles. The topology can be changed at any time as the vehicles can be moved at different directions and at different speeds. They have to adjust their transmission and reception parameters. VANET network aims to improve transportation reliability, optimize driving, navigation and enhance the vehicle users safety. Vehicles can self-react in order to avoid accidents by preventing the proximity location.

The IEEE 802.11 protocol dedicated to VANET, has been normalized by the IEEE 802.11p [2]. It is an approved amendment to the IEEE 802.11 standard to add wireless access in vehicular environments. The IEEE 802.11p protocol was published on July 2010 [3,4] and contains the definition of the PHYsical layer (PHY) and the Medium Access Control layer (MAC) [5]. Those amendments will be described later.

As those networks are built on distributed systems, a or several vehicle(s) could not respect the protocol and then with their misbehavior, they can attempt or degrade the functioning of all the VANET. Consequences may be light as a simple disconnection but can be dangerous such as an undetected accident occurs and as the vehicle trusts on the system that makes the vehicle not reacting. One main challenge in designing those networks, is their vulnerability to Denial-of-Service (DoS) attacks [6,7]. While DoS has been studied extensively for the wire-line networks, there is lack of research for preventing such attacks in VANET networks. Due to deployment in different environments such as city, highway, roads, they are exposed to be attacked by malicious intruders. The major difference between wire and wireless transmissions is that in wireline, we can distinguish an attack to a transmission error, which is very complicated in wireless networks due to the fluctuation of radio link, the vehicle mobility and the interferences with other vehicles and other systems as well.

Several DoS attacks have been detected and defined in the literature, specifically in MAC layer. The two major DoS Attacks are the greedy behavior, and jamming attacks. A greedy node is only concerned about improving its performance even at the expense of other vehicles by not respecting the protocol features (such as differing a transmission after a Backoff time). The second one is the jamming. Actually, the Vehicles in VANET share the wireless medium. Thus, a radio signal can be early jammed or interfered only by transmitting a radio signal when another vehicle is communicating. The effect of jamming causes the message to be corrupted or lost. If the attacker has a powerful transmitter, it can generate a signal too strong to overwhelm the targeted signals and disrupt communications. There are many different attack strategies that a jammer can perform in order to interfere with other wireless communications. Some of them are detailed in [8]. We tackle this last DoS attacks in this paper by developing a new method that can detect that a vehicle is under an attack. Different strategies can be adopted by the attacker that we have to identify as well. Moreover, since VANET is a dynamic network, and vehicles move quickly and can join or leave the network at any time, traffic jam can be occurred. Consequently, we need to differentiate between jammed scenarios and others conditions such as traffic congestion during the jam, interruption of communication due to failures of the transmitter when it is opposite the natural barrier. Jamming attack is like a more serious threat to the security in the domain of wireless networks. It continuously sends repeated signals to interfere with the communication between the vehicles. The victims of an attack can feel that the state of the channel is always busy. Therefore, it cannot send or receive the legal signal in the jammed area.

When jamming is effective, it will interfere with the legitimate communication. The sender does not detect an idle channel for sending packets. Even it successfully sends packets; the receiver cannot receive all the packets sent, this is due to the attacker that does not respect the communication protocol. Hence, its packet delivery ratio (PDR) is low. On the receiver MAC layer, all the received packets cannot be decoded correctly. Only packets sent by the sender can pass the Cyclic Redundancy Check (CRC). CRC is an error-detecting code. PDR is measured by using the ratio of the number of packets passing the CRC check with respect to the number of received packets (or preambles). The received packets should be sent either by the sender or by the compromised vehicle. Using the PDR criteria and by defining a threshold we can thus differentiate a corrupted packed due to a jamming attack with a transmission error, which is the aim of this study.

The remaining parts of this paper are structured as follows: after a brief description of the IEEE 802.11p amendments in Section 2, we give an overview of the related work in the domain of Jamming in Section 3. As this attack is not well known, we proposed a new analytical model based on Markov Chain to model the jamming attack in VANET. The model description and rewards are exposed in Section 4. In Section 5, we describe DJAVNET (Detecting Jamming Attacks in Vehicle Ad Hoc Networks) the proposed solution for detecting a jamming attack in VANET. To determine the threshold of the PDR that implies that vehicles are under attack area, we have conducted several simulations. Model, parameters and simulation results are given in Section 6. Finally, we summarize the main contribution of this study and we give the perspectives of this work in Section 7.

2. IEEE 802.11p: amendment OF IEEE 802.11 for VANET

IEEE 802.11p is the approved amendment to the IEEE 802.11 protocol for VANETs. This protocol extends the IEEE 802.11 protocol to have Wireless Access in Vehicular Environment (WAVE). It is builded on IEEE 802.11 protocol that support Intelligent Transportation Systems (ITS) applications. Two modes of communications are defined in the protocol: