Chapter 30

IP-CHOCK Reference Detection and Prevention of Denial of Service (DoS) Attacks in Vehicular Ad-Hoc Network:

Detection and Prevention of Denial of Service (DoS) Attacks in Vehicular Ad-Hoc Network

Karan Verma

Central University of Rajasthan, India

ABSTRACT

Vehicular Ad-Hoc Network (VANET) is a subset of Mobile Ad-Hoc Network (MANET) and it is considered as a substantial component of Intelligent Transportation System (ITS). DoS attacks on VANET are varying and may be overwhelmed by VANET protocols, such as TCP or UDP flooding attacks. Different secure communications models can be used to detect and prevent IP spoofing DoS attacks, by which the attacks are committed by fraudulent and malicious nodes. In this chapter, an efficient detection method has been proposed to detect UDP flooding attacks, called Bloom-Filter-Based IP-CHOCK (BFICK). A prevention method using IP-CHOCK has also been proposed to prevent DoS, called Reference Broadcast Synchronization (RBS). In principle, the combined method is based on the IP-CHOCK filter concept of packets during an attack incident and with busy traffic condition. Fake identities from malicious vehicles can be analyzed with help of the existing reliable IP addresses. Beacon packets were exchanged periodically by all the vehicles to announce their presence and to forward it to the next node.

DOI: 10.4018/978-1-7998-5348-0.ch030

INTRODUCTION

Population growth has led to an increase in transportation needs, while advances in technology has motivated for the development of an Intelligent Transportation System (ITS). For ITS to work, each vehicle on road is equipped with communication devices, and they are communicating wirelessly with each other over a wireless network known as Vehicular Ad-hoc Network (VANET). In general, wireless network that supports user mobility is known as Mobile Ad-hoc Network (MANET). Hence, VANET is a sub-set of MANET, which today ITS is relying on VANET to powerfully implement it (Isaac, Zeadally, & Cámara, 2010; Wu, Chen, Wu, & Cardei, 2007). VANET can be expected to provide efficient transportation and management services.

In a VANET, vehicle nodes are mobile and interconnected through a wireless interface (Antolino Rivas, Barceló-Ordinas, Guerrero Zapata, & Morillo-Pozo, 2011; Sichitiu & Kihl, 2008). In the United States, the Federal Communication Commission (FCC) allocated a 75 MHz spectrum at 5.9 GHz for vehicular communications, which are of types of so-called Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I). Similar bands have been allocated in other countries (Aslam, Park, Zou, & Turgut, 2010; Lo & Tsai, 2007). As for protocols supporting VANET, Dedicated Short Range Communication (DRSC) is the underlying transport protocol, with its specification stated as IEEE 802.11p. It supports both public safety and licensed private operatives over V2V and V2I communications, in addition to upper-layer protocols for wireless access in a vehicular environment. Wireless Access for Vehicular Environment (WAVE)-IEEE 1609 protocols are also under development (Isaac et al., 2010; Raya & Hubaux, 2007) to support mobile communications.

As VANET is closely related to human daily life activities, it is expected that it shall provide reliable and secure communications, as nodes join or leave the network arbitrarily without human intervention. It is noted that data traffic in VANET will travel through multiple hops, and routed through vulnerable wireless media, thus exposing to security risks. Inter-vehicular communications (V2V) and Vehicle-to- Infrastructure communications (V2I) require applications that serve users and that secure their transportation goals (see: Figure 1). VANET has two main application categories: safety and non-safety (Wu et al., 2007). Safety applications are the focus of most research in the area of VANET systems. Although drivers have no ability to predict road conditions (Amadeo, Campolo, & Molinaro, 2013), with the aid of sensors, computer equipment, wireless communication devices and a combination of similar technologically equipped devices, it is possible to provide methods by which drivers can foresee the speed of other vehicles and assess possible risks. Through such systems, warnings are periodically sent to predict vehicular speeding to reduce the incidence of collisions (Zeadally, Hunt, Chen, Irwin, & Hassan, 2012). What is needed is to improve the application efficiency, which may effect in reducing number of fatalities and provide safer, cleaner and more comfortable road travel. Non-safety applications provide additional information for pleasant, convenient, and entertaining journey to users, while they are moving on roads. This class of application is categorized as infotainment.

Unfortunately, VANET comes with a set of challenges to both classes, especially safety. Due to its wireless communication capability in V2V and V2I modes, VANET is subjected to numerous threats that can lead to increase malicious attacks and service abuses (see: Figure 1) (Antolino Rivas et al., 2011; Y.-S. Chen, Hsu, & Yi, 2012; Y. Zhang & Cao, 2011).