Chapter 10
Intrusion Detection in Vehicular Ad-Hoc Networks on Lower Layers

Chong Han
University of Surrey, UK

Ibrahim Abualhaol
Khalifa University, UAE

Sami Muhaidat
Khalifa University, UAE

Mehrdad Dianati
University of Surrey, UK

Rahim Tafazolli
University of Surrey, UK

ABSTRACT

Vehicular Ad-Hoc Networks (VANETs) are a critical component of the Intelligent Transportation Systems (ITS), which involve the applications of advanced information processing, communications, sensing, and controlling technologies in an integrated manner to improve the functionality and the safety of transportation systems, providing drivers with timely information on road and traffic conditions, and achieving smooth traffic flow on the roads. Recently, the security of VANETs has attracted major attention for the possible presence of malicious elements, and the presence of altered messages due to channel errors in transmissions. In order to provide reliable and secure communications, Intrusion Detection Systems (IDSs) can serve as a second defense wall after prevention-based approaches, such as encryption. This chapter first presents the state-of-the-art literature on intrusion detection in VANETs. Next, the detection of illicit wireless transmissions from the physical layer perspective is investigated, assuming the presence of regular ongoing legitimate transmissions. Finally, a novel cooperative intrusion detection scheme from the MAC sub-layer perspective is discussed.

INTRODUCTION

Intelligent Transportation Systems (ITS) and related applications have been designed and deployed in recent years. ITS applications, which consist of safety-related and non-safety-related applications, provide timely life-critical information, help drivers and traffic controlling centre with efficient decision making, and provide commercial, leisure, and convenience services. As the key component

DOI: 10.4018/978-1-4666-8473-7.ch010

of ITS, Vehicular Ad-Hoc Networks (VANETs) have attracted the attention in both industrial and academic communities because of the commercial potentials and the required research for their realization. The cooperative, self-organizing communication terminals in VANETs relay information with each other and also exchange data with fixed network infrastructure (Seyfi, Muhaidat, Jie, & Uysal, 2011). Communications are enabled among vehicles and infrastructure to enhance transportation safety, efficiency, and entertainment via Vehicle-to-Vehicle (V2V) communications and Vehicle-to-Infrastructure (V2I) communications. New research is required for developing many of the components and the architecture of such communications systems. Potential applications are diverse and pervasive. Safe and efficient transportation systems can be realized through fast dissemination of road and traffic information (i.e., updates regarding collisions, incidents, congestion, surface, and weather conditions) and coordination of vehicles at critical points such as highway entries and other intersections. In addition, many new applications will be facilitated, e.g., cooperative high-speed internet access from within the vehicular network, cooperative downloading, network gaming among passengers of adjacent vehicles, and virtual, video-enabled meetings among co-workers travelling in different vehicles, and previously unimagined products which tend to be spawned by new communications services. Currently, it is easy to imagine realistic-experience multimedia meetings for personal or business purposes, as well as for emergency services. In medical services, paramedics and other first responders could link with hospitals and other expert bases from incident sites and from ambulances and other emergency vehicles. For public transport, streaming multimedia offers new possibilities for security, fleet management, and advertising, in particular for buses and trains. New data services also enable new user-charging strategies for new or improved efficiency public services. Such services are only possible with enabling communication and networking technologies. Different service requirements must be addressed piecemeal-wise with different mobile technologies and different standards. The goal of VANETs is to offer economical, common, reliable, high rate, low latency systems for terrestrial communications-based services. They will use many industry standard components and cooperatively share the radio spectrum, a finite and shared resource.

Designs of protocols for different layers take into account the special characteristics of VANETs, such as the real-time constrains, high node mobility, frequent changing topology, large network scale, and the ad hoc communication structure. However, the vehicular networks turn to be vulnerable to various attacks naturally. Security in VANETs has attracted more attentions recently, since any malicious intruder with access to the open medium of VANET can threaten the information security and as a consequence affects the passengers' safety. Safety related applications have to be protected from malicious manipulation, such as altered messages, false alarm, and repudiation, in order to avoid potential harm to vehicle drivers due to failure to make correct decisions. Non-safety applications needs to avoid attacks from illicit users in terms of traffic jamming, overloading, and/or having a non-cooperative behavior (e.g., dropping packets). Moreover, manufactures and service providers need protection of their commercial profit. Hence, there is a need for a secure and reliable system to ensure that messages with life-critical information will not be modified, discarded or forged by any attacker. Since existing prevention based techniques are limited in their effectiveness and emerging intrusions, intrusion detection becomes an indispensable part to maintain the security in VANETs.

This chapter focuses on the problems of intrusions in vehicular networks. The chapter starts by presenting the security requirements of vehicular networks and their impacts on the security of these networks. A literature review is given on the existing efforts on the security for vehicular