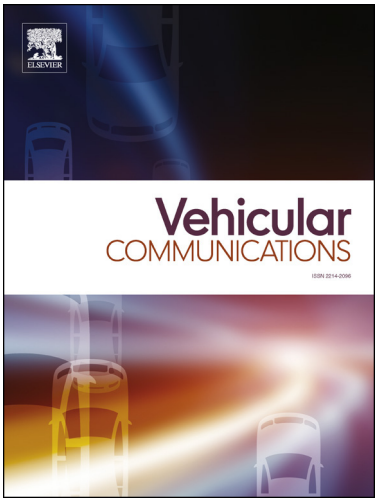
Accepted Manuscript



Predict and prevent from misbehaving intruders in heterogeneous vehicular networks

Hichem Sedjelmaci, Sidi Mohammed Senouci, Tarek Bouali

PII: S2214-2096(16)30062-6
DOI: http://dx.doi.org/10.1016/j.vehcom.2016.12.005
Reference: VEHCOM 72

To appear in: *Vehicular Communications*

Received date: 30 May 2016
Accepted date: 21 December 2016

Please cite this article in press as: H. Sedjelmaci et al., Predict and prevent from misbehaving intruders in heterogeneous vehicular networks, *Veh. Commun.* (2016), http://dx.doi.org/10.1016/j.vehcom.2016.12.005

Predict and Prevent From Misbehaving Intruders in Heterogeneous Vehicular Networks

Hichem Sedjelmaci, Sidi Mohammed Senouci
DRIVE EA1859, Univ. Bourgogne Franche Comté, F58000,
49 Rue Mademoiselle Bourgeois, 58000, Nevers, France
{Sid-Ahmed-Hichem.Sedjelmaci, Sidi-Mohammed.Senouci
}@u-bourgogne.fr

Tarek Bouali
AIT- Automotive, Infrastructure & Transport, Altran Technologies
2, rue Paul Dautier 78140 Vélizy-Villacoublay, France
tarek.bouali@altran.com

ABSTRACT
The great evolution of communication technologies and potential availability of network access mediums and service providers have led to the appearance of heterogeneous network concept. This paradigm refers to the seamless and ubiquitous interoperability between multi-coverage protocols with different access techniques. A heterogeneous vehicular network (HetVNet) is a heterogeneous network where a vehicle is a smart node equipped with various communication technologies such as Dedicated Short Range Communication (DSRC) and cellular network (3G/4G). The purpose of HetVNet is ensuring a wide area coverage to all vehicles in a large scale network, thus achieving the Always Best Connected (ABC) paradigm where the best continuous connectivity is offered to clients. In addition, HetVNet enables the acquisition and processing of a large amount of data from wide geographical areas via smart vehicles to offer various categories of services to drivers and passengers. There are many challenges in HetVNet and security is one of them since, in one hand, vehicles exchange vital data (about congestions, accidents, hazards, road-works, etc.) and in the other hand they form a specific network with particular characteristics (frequent fragmentation, dynamic topology, no centralized authority, etc.). Intrusion detection systems (IDS) act as a second wall of defense when cryptography is broken and already proved their effectiveness against both external and internal intruders. Therefore, in this research work we propose and implement an intrusion detection and prediction scheme able to detect and especially predict the future misbehavior of a malicious vehicle. The attack prediction technique proposed in this paper is based on a game theory to prevent the occurrence of malicious vehicles. Moreover, the proposed detection scheme detects the most dangerous attacks that target a HetVNet such as false alerts and Sybil attacks. This detection uses a rules-based technique to model a normal behavior of a vehicle. Simulations performed using NS-3 show that our scheme exhibits a high accuracy prediction, faster attack detection, and a low communication overhead compared to current detection frameworks.

Keywords: *HetVNet, Game model, Intrusion detection, Intrusion prediction, Accuracy prediction.*

I. INTRODUCTION

The unprecedented growth of sensing devices and communication technologies has led to the increase of the number of connected vehicles. According to recent statistics, in 2020, a significant number of smart vehicles will be deployed where a variety of Intelligent Transportation System (ITS) applications will be provided such as traffic efficiency and infotainment [1]. To benefit from these services and a continuous Internet connectivity, these smart vehicles are featured with a variety of heterogeneous communication technologies such as Dedicated Short Range Communication (DSRC) and cellular network (3G/4G) [2]. The vehicular network, composed of such smart vehicles and also known as Heterogeneous Vehicular Network (HetVNet), supports well the requirements of the different ITS applications since by combining these communication technologies, a wide area coverage and a good quality of service (QoS) is achieved and ensured, respectively [3]. Hence, in HetVNet, the vehicle is a smart node equipped with a computation unit, a set of sensors, and different communication mediums to exchange data with either other vehicles or the infrastructure [3].

The success of heterogeneous vehicular networks depends mainly on the underlying communications system, and particularly the information security since the vehicles exchange, in one hand, vital data (about congestion, accident, hazard, road-works, etc.) and