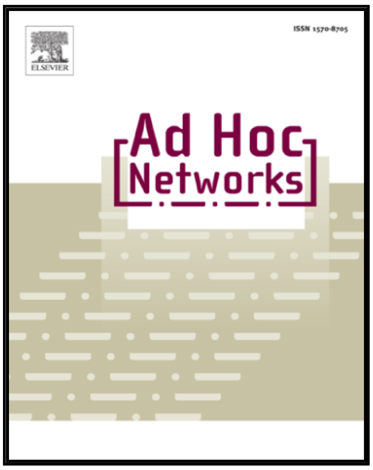

A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV

Fatih Sakiz , Sevil Sen

PII: S1570-8705(17)30056-2
DOI: 10.1016/j.adhoc.2017.03.006
Reference: ADHOC 1529

To appear in: *Ad Hoc Networks*

Received date: 8 September 2016
Revised date: 26 February 2017
Accepted date: 12 March 2017

Please cite this article as: Fatih Sakiz , Sevil Sen , A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV, *Ad Hoc Networks* (2017), doi: 10.1016/j.adhoc.2017.03.006

A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV

Fatih Sakiz* and Sevil Sen
Department of Computer Engineering, Hacettepe University, Turkey

Abstract—**Vehicular ad hoc networks (VANETs) have become one of the most promising and fastest growing subsets of mobile ad hoc networks (MANETs). They are comprised of smart vehicles and roadside units (RSU) which communicate through unreliable wireless media. By their very nature, they are very susceptible to attacks which may result in life-endangering situations. Due to the potential for serious consequences, it is vital to develop security mechanisms in order to detect such attacks against VANETs. This paper aims to survey such possible attacks and the corresponding detection mechanisms that are proposed in the literature. The attacks are classified and explained along with their effects, and the solutions are presented together with their advantages and disadvantages. An evaluation and summary table which provides a holistic view of the solutions surveyed is also presented.**

Keywords— **Attacks, intrusion detection, misbehavior detection, IoV, VANET, security**

1. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) are a special type of mobile ad hoc network used for communication among and between vehicles and roadside units. VANETs are an emerging technology for many applications, including congestion monitoring and traffic management. For example, vehicles on a road where an accident has occurred can alert each other to take an alternative route in order to avoid the traffic jam that has built up following the accident. Beside safety-related applications, there are also other applications such as infotainment, payment services, insurance calculations based on usage, and other similar means. These are applications which require vehicles to communicate with infrastructure, people and the Internet, resulting in VANETs having evolved into the universal paradigm known as the Internet of Vehicles (IoV) [1].

The special characteristics of VANETs, such as high mobility, dynamic network topology, and

* Corresponding author. Tel.: +90-312-297-7500
E-mail addresses: fatihsakiz@hacettepe.edu.tr, ssen@cs.hacettepe.edu.tr.