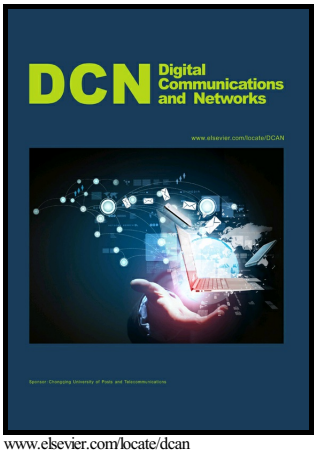

www.elsevier.com/locate/dcan

Using Discriminant Analysis to Detect Intrusions in External Communication of Self-Driving Vehicles

Khattab M Ali Alheeti, Anna Gruebler, Klaus McDonald-Maier

PII: S2352-8648(17)30091-3
DOI: http://dx.doi.org/10.1016/j.dcan.2017.03.001
Reference: DCAN77

To appear in: *Digital Communications and Networks*

Received date: 25 September 2016
Revised date: 26 February 2017
Accepted date: 7 March 2017

Cite this article as: Khattab M Ali Alheeti, Anna Gruebler and Klaus McDonald-Maier, Using Discriminant Analysis to Detect Intrusions in External Communication of Self-Driving Vehicles, *Digital Communications and Networks,* http://dx.doi.org/10.1016/j.dcan.2017.03.001

Digital Communications and Networks(DCN)

ACCEPTED MANUSCRIPT

Available online at www.sciencedirect.com

ScienceDirect

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

Using Discriminant Analysis to Detect Intrusions in External Communication of Self-Driving Vehicles

Khattab M Ali Alheeti*, Anna Gruebler, Klaus McDonald-Maier

Embedded and Intelligent Systems Research Laboratory, School of Computer Science and Electronic Engineering, University of Essex Wivenhoe Park, Colchester CO4 3SQ, UK;
kmali@essex.ac.uk, contact@annagruebler.com (A.G.); kdm@essex.ac.uk (K.M.-M.)

Abstract

Security systems are considered a necessity for the deployment of smart vehicles in our society. Security in vehicular ad hoc networks is crucial to the reliable exchange of information and control data. In this paper, an intelligent intrusion detection system (IDS) is proposed to protect the external communication of self-driving and semi self-driving vehicles. This technology has the ability to detect Denial of Service (DoS) and black hole attacks on VANETs. The advantage of the proposed IDS over incumbent security systems is that it detects the attack before it causes significant damage. The intrusion prediction technique is based on a Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA) to predict the attack based on an observed vehicle behaviour. Simulations utilised Network Simulator version 2 to demonstrate that the IDS exhibits a low rate of false alarms and high accuracy in detection.

KEYWORDS:
Security communication, vehicle ad hoc networks, IDS, self-driving vehicles, linear and quadratic discriminant analysis.

1. Introduction

Self-driving and semi self-driving vehicles are attracting increased attention from both industry and research community because of their potential positive and economic effects on society [1]. These vehicles depend heavily on internal and external communication systems to achieve their goals, such as traffic safety, ideal exploitation of resources, reducing human error and reducing the number of injuries and fatalities from traffic accidents [2]. In other words, autonomous and semi-autonomous vehicles operate without drivers and have the ability of improving traffic flow for vehicles on roads and reducing the number of human errors [3].

Vehicular Ad hoc Networks (VANETs) are external communication systems for these vehicles which support intelligent transportation systems [4]. VANETs an play important role in establish secure and safe environment for self-driving and semi self-driving vehicles [5]. VANETs applications can be classified into safety and non-safety applications [6]. Real-time safety applications, fleet management services, traffic management and monitoring are the most important features of these networks [7, 8]. Moreover, security systems are a very important factor for the safe application of these vehicles [7]. Strong and reliable security mechanisms are needed to protect information as well as the control data transferred between vehicles and their Road Side Units (RSUs) in radio coverage areas [8].

The IDS can be used as an effective tool to know whether unauthorized users are trying to gain access, already have access or have compromised the network. However, when IDS is compared with the wired network, there is an introduction of additional challenges in setting up an IDS by the dynamic topology of ad hoc

*Khattab M Ali Alheeti (Corresponding author) is with the School of Computer Science and Electronic Engineering, University of Essex, Colchester, CO4 3SQ, UK (e-mail: kmali@essex.ac.uk). Anna Gruebler is currently Head of Data Science at AltViz in London - Data Scientist, UK. (e-mail: contact@annagruebler.com). Klaus McDonald-Maier is with the School of Computer Science and Electronic Engineering, University of Essex, Colchester, CO4 3SQ, UK (e-mail: kdm@essex.ac.uk).