https://ieeexplore.ieee.org/document/7604962/keywords#keywords

Hybrid intrusion detection in connected self-driving vehicles

Publisher: IEEE

Khattab M. Ali Alheeti; Klaus McDonald-Maier

Abstract:

Emerging self-driving vehicles are vulnerable to different attacks due to the principle and the type of communication systems that are used in these vehicles. These vehicles are increasingly relying on external communication via vehicular ad hoc networks (VANETs). VANETs add new threats to self-driving vehicles that contribute to substantial challenges in autonomous systems. These communication systems render self-driving vehicles vulnerable to many types of malicious attacks, such as Sybil attacks, Denial of Service (DoS), black hole, grey hole and wormhole attacks. In this paper, we propose an intelligent security system designed to secure external communications for self-driving and semi self-driving cars. The proposed scheme is based on Proportional Overlapping Score (POS) to decrease the number of features found in the Kyoto benchmark dataset. The hybrid detection system relies on the Back Propagation neural networks (BP), to detect a common type of attack in VANETs: Denial-of-Service (DoS). The experimental results show that the proposed BP-IDS is capable of identifying malicious vehicles in self-driving and semi self-driving vehicles.

Published in: 2016 22nd International Conference on Automation and Computing (ICAC)

Date of Conference: 7-8 Sept. 2016

Date Added to IEEE *Xplore*: 24 October 2016

ISBN Information:

INSPEC Accession Number: 16398195

DOI: 10.1109/IConAC.2016.7604962

Publisher: IEEE

Conference Location: Colchester, UK

Keywords

- Vehicles,
- Feature extraction,
- Benchmark testing,
- Training,
- IP networks,
- Intrusion detection