https://ieeexplore.ieee.org/document/7429276

An Intrusion Detection System against Black Hole Attacks on the Communication Network of Self-Driving Cars

Publisher: IEEE

Anna Gruebler; Klaus D. McDonald-Maier; Khattab M. Ali Alheeti

Abstract:

The emergence of self-driving and semi self-driving vehicles which form vehicular ad hoc networks (VANETs) has attracted much interest in recent years. However, VANETs have some characteristics that make them more vulnerable to potential attacks when compared to other networks such as wired networks. The characteristics of VANETs are: an open medium, no traditional security infrastructure, high mobility and dynamic topology. In this paper, we build an intelligent intrusion detection system (IDS) for VANETs that uses a Proportional Overlapping Scores (POS) method to reduce the number of features that are extracted from the trace file of VANET behavior and used for classification. These are relevant features that describe the normal or abnormal behavior of vehicles. The IDS uses Artificial Neural Networks (ANNs) and fuzzified data to detect black hole attacks. The IDSs use the features extracted from the trace file as auditable data to detect the attack. In this paper, we propose hybrid detection (misuse and anomaly) to detect black holes.

Published in: 2015 Sixth International Conference on Emerging Security Technologies (EST)

Date of Conference: 3-5 Sept. 2015

Date Added to IEEE *Xplore*: 10 March 2016

Electronic ISBN:978-1-4673-9799-5

INSPEC Accession Number: 15838929

DOI: 10.1109/EST.2015.10

Publisher: IEEE

Conference Location: Braunschweig, Germany

Keywords

- Feature extraction,
- Vehicles,
- Intrusion detection,
- Vehicular ad hoc networks,
- Computational modeling,
- Cams