https://ieeexplore.ieee.org/abstract/document/7158098

An intrusion detection system against malicious attacks on the communication network of driverless cars

Publisher: IEEE

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

Abstract:

Vehicular ad hoc networking (VANET) have become a significant technology in the current years because of the emerging generation of self-driving cars such as Google driverless cars. VANET have more vulnerabilities compared to other networks such as wired networks, because these networks are an autonomous collection of mobile vehicles and there is no fixed security infrastructure, no high dynamic topology and the open wireless medium makes them more vulnerable to attacks. It is important to design new approaches and mechanisms to rise the security these networks and protect them from attacks. In this paper, we design an intrusion detection mechanism for the VANETs using Artificial Neural Networks (ANNs) to detect Denial of Service (DoS) attacks. The main role of IDS is to detect the attack using a data generated from the network behavior such as a trace file. The IDSs use the features extracted from the trace file as auditable data. In this paper, we propose anomaly and misuse detection to detect the malicious attack.

Published in: 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)

Date of Conference: 9-12 Jan. 2015

Date Added to IEEE *Xplore*: 16 July 2015

ISBN Information:

ISSN Information:

INSPEC Accession Number: 15304778

DOI: 10.1109/CCNC.2015.7158098

Publisher: IEEE

Conference Location: Las Vegas, NV, USA

Keywords

- Vehicles,
- Security,
- Artificial neural networks,
- Feature extraction,
- Training,
- Accuracy,
- Ad hoc networks