On Gray-Hole Detection Ids Based On Machine Learning Algorithms In VANET

Arízaga-Silva, J., Rosales-Roldan, L.

Universidad Politécnica de Puebla - Department of Automotive systems
Doctor of Engineering
juan.arizaga@uppuebla.edu.mx

Faculty of Mechatronics, Electronics, Bionics and Aerospace – UPAEP
luis.rosales@upaep.mx

Abstract

Wireless communication technologies are significant elements in the development of intelligent transportation systems (ITS) and cybersecurity is today's primary concern in vehicular communications. Vehicles are now able to connect to road's infrastructure (V2I), other vehicles (V2V), or another element (V2X) spontaneously, vehicles are now nodes in a wireless network ready to interchange information. The exchange of information between nodes in these vehicular networks must remain secure, reliable, and available. The lack of infrastructure and centralized management makes vehicular ad hoc networks (VANET) vulnerable to irregular behaviours that significantly threaten different aspects of network security. In this paper, an intelligent Intrusion Detection System (IDS) is proposed to prevent Gray-Hole attacks in VANET. The advantage of the proposed IDS over existing systems is that it detects attacks before they cause considerable damage. Different Machine Learning algorithms were used to predict the behaviour of attacking nodes, being Random Forest the one that exhibited the best response to different performance metrics. Different simulations were developed using the NS-3 network simulator to demonstrate that the IDS achieves high detection accuracy.

Keywords

Ad hoc networks. Cyber-physical systems, Vehicle.