# On the detection of grey hole and rushing attacks in self-driving vehicular networks

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

**Abstract:**

Vehicular ad hoc networks play an important role in the success of a new class of vehicles, i.e. self-driving and semi self-driving vehicles. These networks provide safety and comfort to passengers, drivers and vehicles themselves. These vehicles depend heavily on external communication to predicate the surrounding environment through the exchange of cooperative awareness messages (CAMs) and control data. VANETs are exposed to many types of attacks such as black hole, grey hole and rushing attacks. In this paper, we present an intelligent Intrusion Detection System (IDS) which relies on anomaly detection to protect external communications from grey hole and rushing attacks. Many researchers agree that grey hole attacks in VANETs are a substantial challenge due to them having their distinct types of behaviour: normal and abnormal. These attacks try to prevent transmission between vehicles and roadside units and have a direct and negative impact on the wide acceptance of this new class of vehicles. The proposed IDS is based on features that have been extracted from a trace file generated in a network simulator. In our paper, we used a feed-forward neural network and a support vector machine for the design of the intelligent IDS. The proposed system uses only significant features extracted from the trace file. Our research, concludes that a reduction in the number of features leads to a higher detection rate and a decrease in false alarms.

**Keywords**

- [Vehicles](#),
- [Feature extraction](#),
- [Routing protocols](#),
- [Ad hoc networks](#),
- [Intrusion detection](#),
- [Roads](#)