Collaborative detection of black hole and gray hole attacks for secure data communication in VANETs

ABSTRACT

Vehicle ad hoc networks (VANETs) are vital towards the success and comfort of self-driving as well as semi-automobile vehicles. Such vehicles rely heavily on data management and the exchange of Cooperative Awareness Messages (CAMs) for external communication with the environment. VANETs are vulnerable to a variety of attacks, including Black Hole, Gray Hole, wormhole, and rush attacks. These attacks are aimed at disrupting traffic between cars and on the roadside. The discovery of Black Hole attack has become an increasingly critical problem due to widespread adoption of autonomous and connected vehicles (ACVs). Due to the critical nature of ACVs, delay or failure of even a single packet can have disastrous effects, leading to accidents. In this work, we present a neural network-based technique for detection and prevention of rushed Black and Gray Hole attacks in vehicular networks. The work also studies novel systematic reactions protecting the vehicle against dangerous behavior. Experimental results show a superior detection rate of the proposed system in comparison with state-of-the-art techniques.