Hamdan S., Hudaib A., Awajan A., 2019. Detecting Sybil Attacks in Vehicular Ad Hoc Networks. International Journal of Parallel Emergent and Distributed Systems. TAYLOR & FRANCIS (ISI) DOI: 10.1080/17445760.2019.1617865

Abstract

Ad hoc networks are vulnerable to numerous attacks due to its infrastructure-less nature, one of these attacks is the Sybil attack. Sybil attack is a severe attack on vehicular ad hoc networks (VANET) in which the intruder maliciously claims or steals multiple identities and uses these identities to disturb the functionality of the VANET network by disseminating false identities. Many solutions have been proposed in order to defend the VANET network against the Sybil attack. In this research a hybrid algorithm is proposed by combining footprint and privacy-preserving detection of abuses of pseudonyms (P2DAP) methods. The hybrid detection algorithm is implemented using the ns2 simulator. The proposed algorithm works as follows. P2DAP acts better than the footprint algorithm when the number of vehicles increases. On the other hand, the footprint algorithm acts better when the speed of vehicles increases. The hybrid algorithm depends on encryption, authentication and on the trajectory of the vehicle. The scenarios will be generated using SUMO and MOVE tools.