Abstract

Vehicular ad-hoc networks (VANETs) are renowned form of mobile ad-hoc networks. In VANET, wireless device sends information to nearby vehicles, and messages can be transmitted from one vehicle to another vehicle or roadside infrastructure. So, using VANET can increase safety and traffic optimization. Similar to other technologies, in VANET there are some important and noticeable issues. One of the most important of them is Security. Since the network is open and accessible from everywhere in the VANET radio range, it is expected to be an easy target for malicious users. Therefore there is a need for optimizing the Security of vehicular Ad-hoc networks by Mitigating malicious attacks. This paper presents a review of security requirements, attacks and security challenges to implement the security measures in the VANET. Existing solutions proposed by different researchers are also reviewed and compared to find out the research gaps and scopes in the field of VANET security.


Index Terms

Computer Science  Networks

Keywords

VANET, Security, Attacks, RSU, Attack, Blackhole, Grayhole, DOS, Illusion, Wormhole, Sinkhole