World Academy of Science, Engineering and Technology
International Journal of Transport and Vehicle Engineering
Vol:10, No:06, 2016

VANETs: Security Challenges and Future Directions

Authors : Jared Oluoch

Abstract : Connected vehicles are equipped with wireless sensors that aid in Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication. These vehicles will in the near future provide road safety, improve transport efficiency, and reduce traffic congestion. One of the challenges for connected vehicles is how to ensure that information sent across the network is secure. If security of the network is not guaranteed, several attacks can occur, thereby compromising the robustness, reliability, and efficiency of the network. This paper discusses existing security mechanisms and unique properties of connected vehicles. The methodology employed in this work is exploratory. The paper reviews existing security solutions for connected vehicles. More concretely, it discusses various cryptographic mechanisms available, and suggests areas of improvement. The study proposes a combination of symmetric key encryption and public key cryptography to improve security. The study further proposes message aggregation as a technique to overcome message redundancy. This paper offers a comprehensive overview of connected vehicles technology, its applications, its security mechanisms, open challenges, and potential areas of future research.

Keywords : VANET, connected vehicles, 802.11p, WAVE, DSRC, trust, security, cryptography
Conference Title : ICITS 2016 : International Conference on Intelligent Transportation Systems
Conference Location : New York, United States
Conference Dates : June 06-07, 2016