Low-Cost Information Transfer System Between Vehicles on Roads

Authors: Amelec Viloria, Omar Bonerge Pineda Lezama, Noel Varela

Published in: Advances in Electrical and Computer Technologies

Abstract

The authentication process is a key component to increase security in a vehicle network. Most of the authentication protocols proposed in the literature are based on asymmetric cryptography, and specifically on the use of the RSA algorithm. In addition, the use of digital certificates and a public key infrastructure is considered. Therefore, the authentication process is often complex. In order to propose a secure solution, without the use of digital certificates and the RSA algorithm, a mutual authentication protocol based on the Diffie-Hellman algorithm is presented to establish a session key between vehicle (OBU) and road unit (RSU). From the session key, a secure communication channel can be established to transmit the identifier of each participant and the respective security parameters. To perform the authentication process, the entities perform low-cost computational operations such as hash and XOR functions. Once the mutual authentication protocol is completed, the vehicle and the road unit can exchange messages securely.