Master 2016

Anantmurti Mahabaleshwar Hegde

Software-Based Synchronization for Plug-and-Secure for CAN.

ABSTRACT - Masterthesis

The trend towards connected devices and IoT includes automobile vehicles along with all other devices. With this, it has become possible for hackers to control cars and remotely manipulate the communication within the car. Recently a new, novel approach named Plug and Secure for CAN has been developed to establish and refresh symmetric cryptographic keys between two CAN nodes in a CAN network. With this, the unauthorized manipulation of the CAN messages can be prevented.

The focus of the thesis is to synchronize different such nodes with a software-based communication technique. A step by step approach is considered to achieve the synchronization. First, the key establishment process is made reliable. Then, the hardware-based synchronization is achieved. The actual CAN transmission is encrypted and decrypted at different nodes using the generated keys. Later, the synchronization method is shifted to software using the identifier field to synchronize two separate nodes in the network.