2016

iGP: Autonomous Car

iGP Module: Automotive Intrusion Detection/Prevention System (IDS/IPS) and Cyber-security Vulnerability Tool

Lead Supervisor: Prof. Sherif Hammad and Dr. Mohamed Sobh

Introduction:

In-vehicle LIN and CAN networking appeared to minimize wiring cost and to add more comfort. Nowadays, the number of electronic control units increased dramatically, while adding more mission critical functionalities. Wireless communication channels are used with broad lines of applications. Safety (human lives) comes first in designing all kinds of vehicles. It implies new challenges in securing vehicle functionalities against hackers whose numbers are increasing lately.

Objectives:

Students are required to overview automotive networking architecture, configurations, and standards. Understanding all kinds of cyber security possible attacks, to automotive mission critical modules, is essential. Embedded and desktop system design, implementation, and testing will be deeply addressed. Software tool reports attacks. Embedded systems emulate, detect and prevent possible malicious attacks.

Outcomes/Deliverable

1. Vulnerability and penetration/breaches testing software tool that studies ECU immunity against malicious attacks.
2. Embedded software library that detects and protects against malicious attacks.