Security Vulnerabilities of Autonomous Platoons

Master thesis project at RISE SICS Västerås.

Description
This thesis work is defined in the scope of the SafeCOP (Safe Cooperating Cyber-Physical Systems Using Wireless Communication) (www.safecop.eu) and ELECTRA projects. SafeCOP is a European project that targets cyber-physical systems-of-systems whose safe cooperation relies on wireless communication and the aim of ELECTRA is to investigate the challenges and communication needs of a safe, secure and efficient integration of the platoon into a broader C-ITS context. Platooning is a challenging example of cooperative Cyber-Physical Systems that require a tight coordination between different system components, including sensors, actuators, and controllers. Truck platoons include two to three trucks that are driven as a group to reduce the air drag and therefore increase the fuel efficiency. The challenge arising is to share relevant data among vehicles without much delay, or to be more accurate, with predictable delay to provide for new services. Since failure of communication system in CPS environment can endanger human life or the environment, or may lead to a large financial loss, before the practical deployment of vehicular platoons, the communication system needs to be analyzed in the presence of attackers. Therefore, a structured and comprehensive study of security threats, vulnerabilities and security services is required.

This thesis is suitable for 1-2 students. The thesis would involve the following tasks (can be adjusted to research interest of the candidate(s)):

- Survey the state-of-the-art on security threats, vulnerabilities and security services.
- Implement and simulate impacts of some common and dangerous attacks.
- Propose methods for real-time detection of attacks.

Qualifications
To be successful in this thesis work the candidate(s)would need the following:

- Programming skills in C/C++.
- Other preferable programming languages Python or Java is a plus.
- Knowledge and experience on vehicular ad hoc network and security is a plus.
- Good spoken and written English skills are required.
- Knowledge of network simulators, such as NS-2, NS-3 and OMNeT++ is a plus.

Contact Person
Ali Balador (ali.balador@ri.se), Senior Researcher at RISE SICS Västerås.

Application
To apply please send your CV along with the list of courses you have taken and their grades to ali.balador@ri.se. In your CV provide a short description of previous projects that you have done.

About RISE SICS Västerås
RISE SICS Västerås is a research institute with the aim to strengthen the innovation system in the Mälardalen region by offering applied research to both private and public organizations. Our projects typically involve a team of researchers and focus on delivering tangible results that create immediate and long-term value, based on the latest research results. We are constantly growing and are looking for researchers who enjoy the challenge of working in close collaboration with industry. SICS Västerås has a flexible organization that develops and applies methods and solutions in close collaboration with industrial, public and academic partners. Our core values are to be open-minded, value-driven, research-oriented, and to have fun! Read more about us at www.sics.se

ID: 1581

RISE RESEARCH INSTITUTES OF SWEDEN
Division ICT
RISE SICS

ADRESS
Expectrum, Kopparbergsvägen 10
722 13 Västerås

KONTAKT
info.sics@ri.se, www.ri.se/sics