Proposal for Master Thesis on
"Automotive Driving Security: Risk Assessment of Radar Communications"

Department of Electrical Engineering (E2) and Computer Science (CSE)

Description

A state-of-the-art proposed solution for Intelligent Transportation System safety and efficiency is the combination of mmWave radar and communications, called as joint radar-communications (RadCom), which reuses radar hardware for wireless vehicle-to-vehicle (V2V) communication [1]. RadCom is expected to become an inevitable technology for autonomous driving, since it offers not only reduced hardware, but also efficiency in spectrum and energy consumption. However, *we do not know how secure it will be to replace the current radar and V2V communications by RadCom units and how to deploy security mechanisms to RadCom systems*. Radar and communication systems are prone to different security threats, which offers that combining these two systems in an intelligent way, might enhance security. In this thesis, we will discover the answer in a scientific methodological method. The outcome of the security risk assessment for an automotive RadCom system, will be used to develop appropriate security mechanisms for future RadCom systems.

Objectives

In this thesis, we are interested in conducting a security risk assessment [2] of a specific type of automotive RadCom protocol [3], called as RadChat. We will deploy security mechanisms into the protocol RadChat to improve its security level and simulate its performance by modifying an already developed Matlab-based RadCom simulator for vehicular networks. The thesis will include & target the following steps:

1) *Risk assessment:* The threats and their impact levels will be discovered to attain the security level of the RadChat protocol according to the method in [2], and compared with the current separate radar&V2V communication system.
2) *Deployment of security mechanisms:* Security mechanisms will be identified to be deployed to the RadChat protocol, which will increase its security level. A finite-state-machine of the secure RadChat protocol will be defined.
3) *Performance evaluation:* Performance with and without security mechanisms for RadCom will be simulated to evaluate various performance metrics (such as safety/security metrics, communication data rate, latency, etc.).

Project Group

This is a thesis suitable for a group of *two* students, preferably one student from CSE and one from E2 Departments. Matching will be done by the supervisor if the students wish so.

Prerequisites

Programming background for C or Matlab. Familiarity with object-oriented programming is beneficial, but not required.

Specific outcomes

Students will be exposed to problems about the state-of-the-art radar communications technology regarding autonomous driving. Meanwhile, students will learn about vehicular network simulations, security and protocol development.

Fig.1: Example for a radar communication (RadCom) system.

Contact

Supervisor: Canan Aydogdu, canan@chalmers.se
(main contact for additional information)
Examiner: Henk Wymeersch (E2), Tomas Olovsson (CSE)

References

[1] A. R. Chiriyath, B. Paul and D. W. Bliss, "Radar-Communications Convergence: Coexistence, Cooperation, and Co-Design," in IEEE Transactions on Cognitive Communications and Networking, vol. 3, no. 1, pp. 1-12, March 2017.

[2] Islam, M.M., Lautenbach, A., Sandberg, C., & Olovsson, T. (2016). A Risk Assessment Framework for Automotive Embedded Systems. CPSS '16.

[3] C. Aydogdu, M. F. Keskin, N. Garcia, H. Wymeersch and D. W. Bliss, "RadChat: Spectrum Sharing for Automotive Radar Interference Mitigation," in IEEE Transactions on Intelligent Transportation Systems, 2019.