# Intrusion Detection on the CAN Bus—A Systematic Literature Mapping Study

Bachelor's or Master's Thesis


**Supervisor:** Prof. Dr. Alexander Pretschner
**Advisor:** Thomas Hutzelmann
**Email:** {alexander.pretschner, t.hutzelmann}@tum.de
**Phone:** +49 (89) 289 - 17830
**Starting date:** now (Oktober 2020)



Fakultät für Informatik
Lehrstuhl 4
Software & Systems Engineering
Prof. Dr. Alexander Pretschner

Boltzmannstraße 3
85748 Garching bei München

Tel: +49 (89) 289 - 17830
https://www4.in.tum.de


## Context

In the automotive domain, formerly isolated, embedded systems are now extended and partially replaced with modern computers. The focus of recent developments is utilizing an internet connection and will shift to providing autonomous driving functionalities in the near future. However, to fulfill the basic driving capabilities, old components and structures are left mostly unchanged. This combination of legacy systems and modern components implies several questions and problems.

For instance, especially the network communication between these systems has unique requirements, for example, strict safety properties and a rigidly limited budget on the used resources. Therefore, classical cryptography cannot be used to prevent attacks. As an alternative approach, intrusion detection systems can be deployed inside the network that should raise alarms if they observe "suspicious" behavior. Their design and implementation are in the focus of current research. Nonetheless, this research area has been dispersed until now, and there is no holistic overview and comparison available of different detection strategies across the literature. This raises the need for a systematic literature review that provides insights about previously proposed intrusion detection approaches, their strengths and weaknesses, and the performed evaluation and core quality attributes.

We already build some previous artifacts that will build the foundation for this thesis. First, a big pool of literature that is relevant for Intrusion Detection on the can bus. For this, we started with all papers listed by several libraries for an initial search query for "CAN bus" and "intrusion detection". With a multi-step filter process and forward- and backward-snowballing, we systematically identified all papers that are relevant for this topic. Second, we elicited an initial structure representing the core peculiarities of intrusion detection in general as well as network intrusion detection in particular. Each peculiarity focuses on one specific aspect of the IDS—namely the protected system, the detectable intrusions and assumptions about the attacker— and provides several options for potential realizations. This work resulted in a questionnaire structuring the information provided in the papers as well as forming a framework for the automotive domain to identify promising approaches during the requirements engineering of the bus network.

For this thesis, we will filter this list and select the core publications (e.g. the highly cited) about detection approaches on the CAN bus. You will read these papers thoroughly to extract and structure the information that is required by the questionnaire. Afterward, you will analyze this structured mapping statistically to identify weaknesses inside the questionnaire as well as to spot non-considered peculiarity realizations as gaps in the literature. Finally, we will compose the findings to a holistic overview of the current state-of-the-art.

If this work is conducted as a Bachelor's thesis, a few simplifications will apply: The selection criteria on the publications will be more narrow, there is less need for reflecting about the structure, and finally, suggestions about the improvement of the structure are not mandatory.

## Goal

In this thesis we will conduct a systematic literature mapping study. You will be included in the initial setup, the literature analysis and be part in the writing of the final publication.

*(continuation on next page)*

## Working Plan

1. Familiarize yourself with the procedure of mapping studies
2. Understand and comprehend the initial structure with corresponding background literature
3. Participate in the voting procedure and paper selection
4. Analyze selected literature about:
   (a) Used network architectures and attacker models
   (b) Mechanics used for detection
   (c) Performance and weaknesses
   (d) Means and quality of evaluation
   (e) Used toolchains and data sets
5. Conduct a statistical analysis of the coverage in each peculiarity
6. Use these findings of this analysis to suggest improvements on the questionnaire
7. Write a Report about findings on research questions

## Deliverables

- Participation in the literature voting and filter process
- Structured summaries of the analyzed literature
- Final report written in conformance with TUM guidelines.

## References


**[1]** Kitchenham et al., Systematic literature reviews in software engineering – A systematic literature review, 2009

**[2]** Wohlin, Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering

**[3]** Miller and Valasek, CAN Message Injection, 2016

**[4]** Tomlinson et al., Towards Viable Intrusion Detection Methods For The Automotive Controller Area Network, 2018

**[5]** Loukas et al., A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles, 2019


## If you are intersted . . .

Please fill out the application form of our chair (`https://wiki.tum.de/x/OQrlGw`) and we will arrange a in person meeting to discuss the thesis in detail.


Fakultät für Informatik
Lehrstuhl 4
Software & Systems Engineering
Prof. Dr. Alexander Pretschner

Boltzmannstraße 3
85748 Garching bei München

Tel: +49 (89) 289 - 17830
https://www4.in.tum.de