Distributed Systems Group – Institute of Computer Science
University of Osnabrück

CAN't – An ISOBUS Privacy Proxy for Collaborative Smart Farming

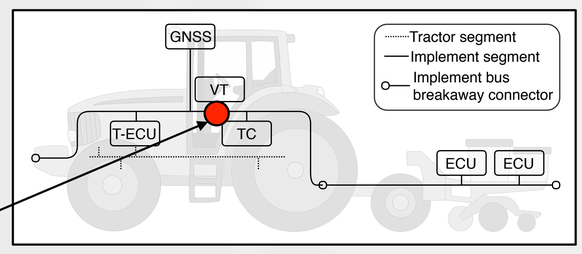
René Helmke, Jan Bauer, Alexander Bothe, Nils Aschenbruck

Introduction & Motivation

Nowadays, agricultural machines and implements are equipped with multiple embedded sensors and actors continuously producing extensive data streams. For data communication, an internal vehicle bus called ISOBUS is used. ISOBUS is based on the machine's Controller Area Network (CAN). However, neither CAN nor ISOBUS communication takes privacy or data sovereignty issues into account. For example, a small maximum payload size of 64 bit prevents proper deployment of well-established cryptographic techniques to ensure secure end-to-end communication. Furthermore, data frames are generally transmitted via broadcast. This implies that each connected node is able to inject or extract arbitrary information. With the increasing interconnectivity of agricultural machines and their integration into farm management information systems, the aforementioned issues become a non-negligible threat in terms of security, safety, and privacy. For selected agricultural scenarios, we propose *CAN't*, an ISOBUS privacy proxy.

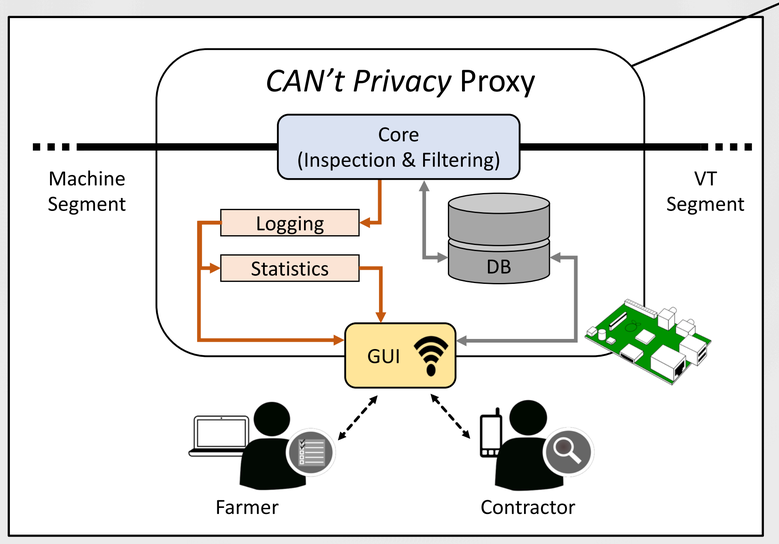
CAN't

CAN't is a data protection framework that enables enforcing technical aspects of a given privacy policy. By acting as man-in-the-middle between a logging node and the remaining network, it filters and manipulates selected CAN data streams. Thus, all actors involved in the agricultural value chain, e.g., farmers, contractors, and employees, can contractually agree on the type and information level of data they want to exchange.



System Architecture [1]

- Man-in-the-middle proxy
- Packet inspection based on ISOBUS identifiers (PGN/SGN)
- Selective filtering, manipulation, and encryption
- Web-based GUI for wireless configuration

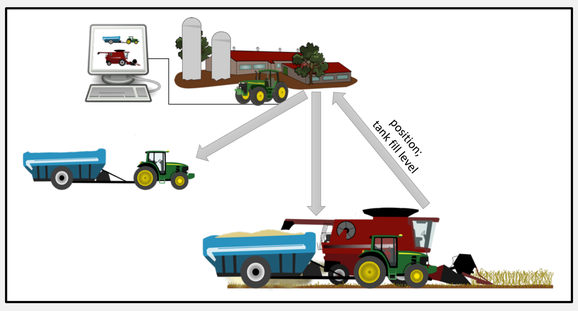


Implementation

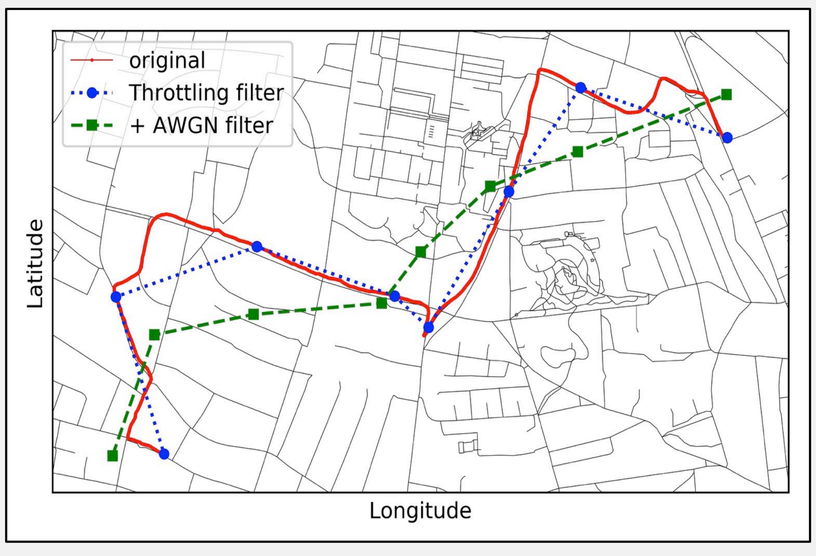
- Hardware
  - Raspberry Pi 3B PICAN DUO (MCP2551)
  - CAN 2.0B (250 kbit/s, 64 bit payload)
- Software
  - SocketCAN + Google Go
  - Demonstrative set of privacy filters

Scenario 1: Process Orchestration [2]

- Transport logistic during grain harvest
- Positions required for process optimization
- **Privacy threat**:
  - Boundless tracking of employees in road traffic



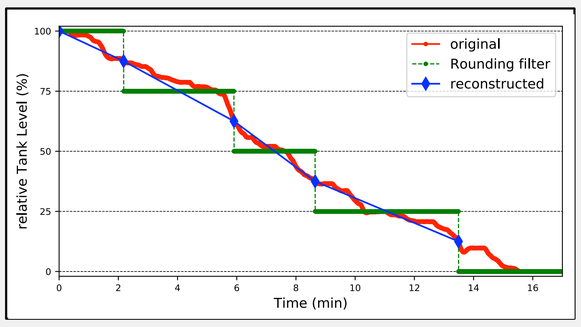
Manipulation of GNSS Traces



Scenario 2: Field Sensing

- Business sensitive information sensed during field operations (e.g., yield data or application rates)
- **Data sovereignty threat**:
  - Data gathering by contractors or 3rd party implements

Coarsening of Tank Level Information



References:

[1] Jan Bauer, René Helmke, Alexander Bothe, Nils Aschenbruck
"CAN't track us: Adaptable Privacy for ISOBUS Controller Area Networks"
Elsevier Computer Standards & Interfaces, Vol. 66, Article 103344, Oct. 2019.

[2] Jan Bauer, Nils Aschenbruck
"Measuring and Adapting MQTT in Cellular Networks for Collaborative Smart Farming"
Proc. of the 42nd IEEE Conference on Local Computer Networks (LCN), Singapore, Oct. 2017.

Download & Further Information:

https://sys.cs.uos.de/cant

Part of the Project: DiL https://www.odil-projekt.de

Sponsored by the: Federal Ministry of Education and Research

Managed by the: PTKA Project Management Agency Karlsruhe, Karlsruhe Institute of Technology