Crypto CAN't – Confidentiality and Privacy for CAN/ISOBUS Networks in Precision Agriculture

Jan Bauer [△], René Helmke [△], Till Zimmermann [△], Alexander Bothe [△], Michel Löpmeier[•], Nils Aschenbruck [△]

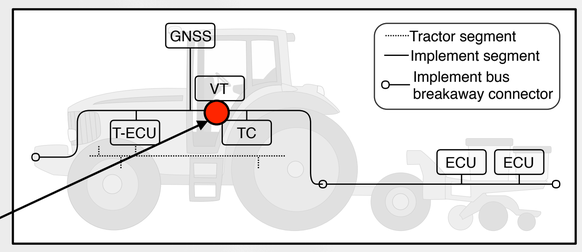
[△] Distributed Systems and [•]Competence Center ISOBUS e.V.

Introduction & Motivation

Modern agricultural machines and implements are equipped with numerous embedded sensors, producing extensive machine and environmental data, which often contains personal and privacy-sensitive information. Data streams are transmitted via ISOBUS, an internal vehicle bus that relies on the Controller Area Network (CAN) standard. However, neither ISOBUS nor CAN take privacy aspects into account. Thus, particularly with respect to the increasing interconnectivity of machinery, serious privacy concerns arise.

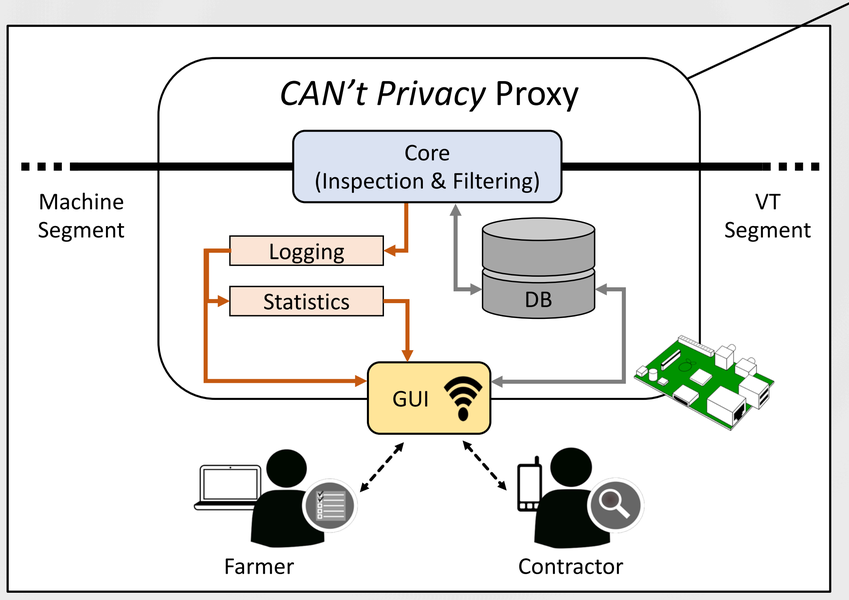
Crypto CAN't

Our data protection framework makes it possible to purposefully filter, manipulate, and encrypt CAN data streams for the sake of privacy and data sovereignty. Using CAN't, 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 during a certain process.



System Architecture [1]

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

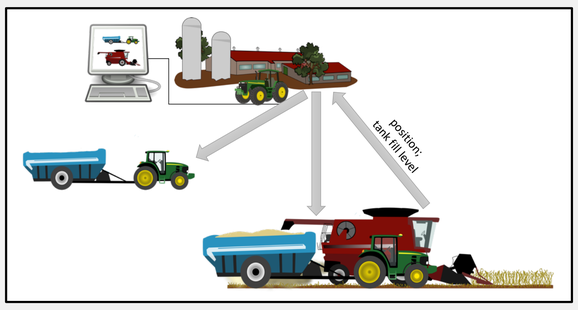


Implementation

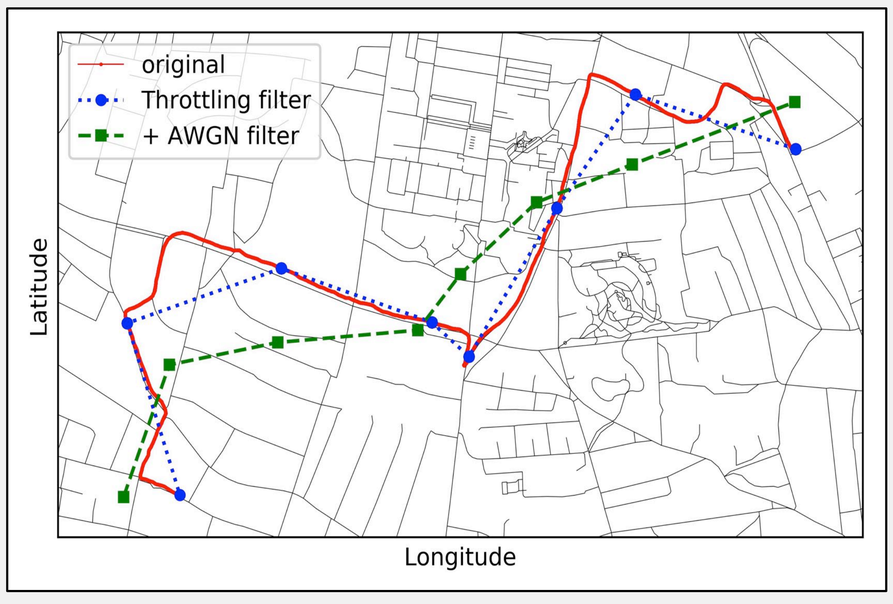
- Hardware
  - Raspberry Pi 3B PICAN DUO (MCP2551)
  - CAN 2.0B (250 kbit/s, 64 bit payload)
- Software
  - SocketCAN + Google Go
  - Basic set of privacy filters
  - Tiny Encryption Algorithm (XTEA)

Scenario 1: Process Orchestration [2]

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



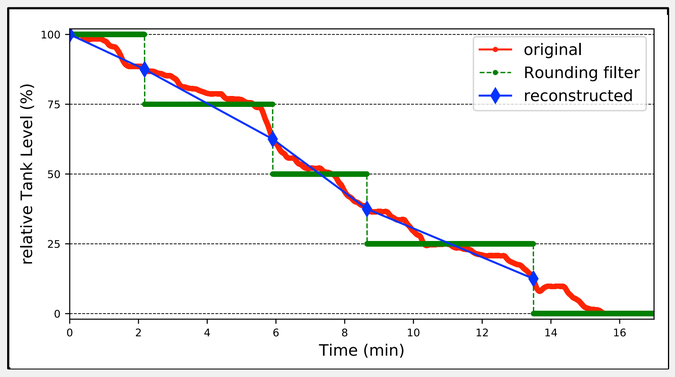
Manipulation of GNSS Traces



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