PURDUE INNOVATES | Office of Technology Commercialization

Securing Serial Communication Buses Using Interframe Spacing

This approach secures existing serial communication buses like CAN networks using trusted officer nodes to prevent attacks such as impersonation and message injection, without requiring hardware changes or consuming network memory.

Serial communication buses, including controller area network (CAN), are widely used to control factories, automotive and aerospace vehicles, elevators, and medical equipment. Despite their wide adoption in critical processes for society, they weren't designed with security features, opening the door for vulnerabilities to various forms of infrastructure. To address this, researchers at Purdue University have developed an approach to securing serial communication busses via a system of trusted officer nodes that have control over other agent nodes. While consuming no memory on the network, Purdue's system can secure against impersonation, message injection, error handling, and flooding. This communication approach can be used on existing serial networks, without the need for changes to existing hardware. This technology has applications in any system using CAN communication where it is necessary to eliminate security vulnerabilities without sacrificing performance.

Advantages

-Introducing security features to serial communication

-Preventing a variety of attack modes

-Versatile, low overhead

-Uses zero bytes of the CAN frame

-Does not use other cryptographic techniques

-Backward compatible

-Capable of instant detection and prevention

Applications

Technology ID
2024-XU-70376

Category
Robotics & Automation/Automation & Control

Authors
Zeynel Celik
Vireshwar Kumar
Khaled A Serag Alsharif
Dongyan Xu

Further information
Matt Halladay
MRHalladay@prf.org

Erinn Frank
EEFrank@prf.org

View online

-Automotive

-Avionics

-Medical equipment

-Factory automation

Technology Validation:

This technology was validated by successfully testing against various CAN vulnerabilities in an automotive vehicle. It achieved near-100% detection and prevention rates for common attacks.

TRL: 6

Intellectual Property:

Provisional-Gov. Funding, 2024-01-31, United States

Utility-Gov. Funding, 2025-01-31, United States

Keywords: CAN bus security, serial communication security, controller area network vulnerabilities, automotive cybersecurity, trusted officer nodes, message injection prevention, CAN network intrusion detection, CAN security solution, secure serial communication, factory automation security, can, Computer Technology, cyberattack, data security, resilience, serial communication, vulnerability