CAN Bus: Security Issues

S. Venkatesan

Acknowledgement: The contents, example scripts and some figures are copied from various sources.
Thanks to all authors and sources made those contents public and usable for educational purpose

Issues

- It has no security features.

- Is vulnerable to all kinds of attacks – Many are inconceivable when CAN was created in 1986.

Accessing CAN

- Attack surface
  - Physical access to the wiring.
  - Splicing in a device (used today to override emissions controls in trucks) through subverting wireless access points (not just Bluetooth or WiFi but also sensors for TPMS)
- Impact
  - Hijack a device connected to CAN (most commonly a car’s infotainment system but ECUs and other control systems can be hijacked too).

Types of Attack

- Confidentiality [Less required].
- Integrity
- Availability

Attacks

- Janus attack
- Frame spoofing (simple, timed and Error Passive variants)
- Error attack
- Double Receive attack
- Freeze Doom Loop attack

Attacks

- **The Double Receive Attack**. This is where a transmitter’s CAN controller is made to re-send a frame so that other CAN controllers receive it multiple times.

- **The Freeze Doom Loop Attack**. This is where the CAN bus can be silently frozen after a frame is sent, and held in that state for an arbitrary time by the attacker.

- **The Janus Frame Attack**. This is where bit glitching is used to attack the very lowest parts of the CAN protocol to send a single frame with different contents to different receivers.

Solutions

- Segmentation
- Encryption
- Authentication
- Intrusion Detection System

CAN-HG

- The CAN-HG protocol augments existing CAN with Higher speed data and provides bus Guarding support to stop spoofing and denial-of-service attacks.

- The CAN-HG header tags a frame with details of where it came from. An Intrusion Detection Prevention System (IDPS) uses this to instantly spot a spoofed frame.

CAN-HG hardware

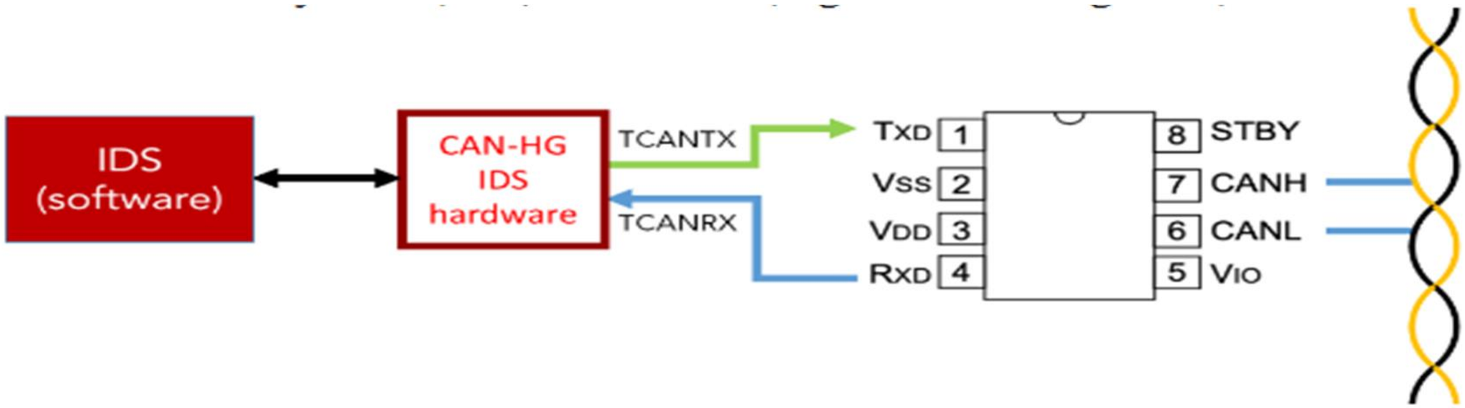


Figure 7: The central security node with CAN-HG IDS hardware

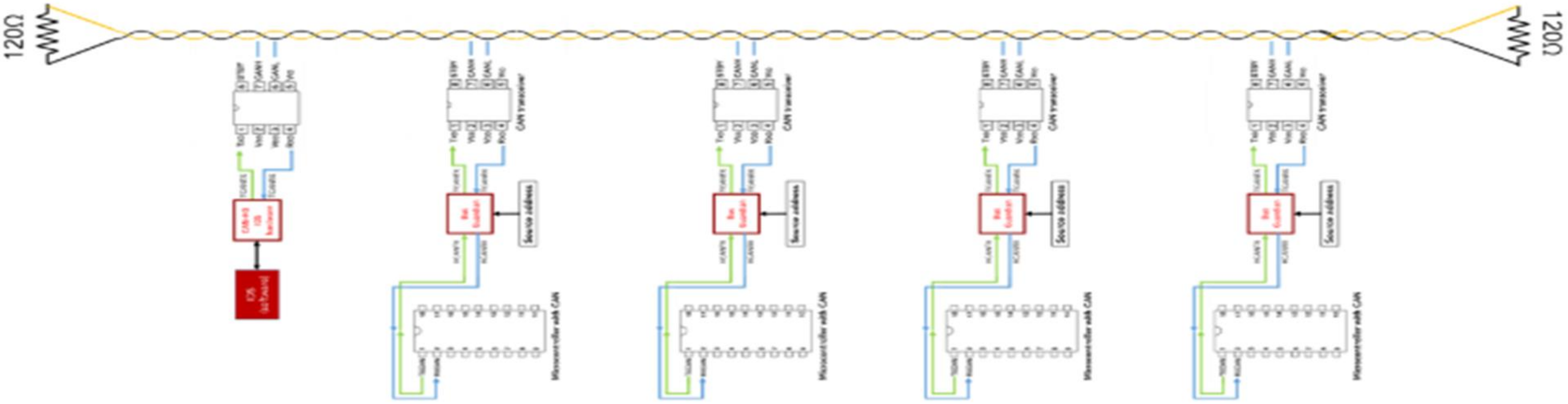
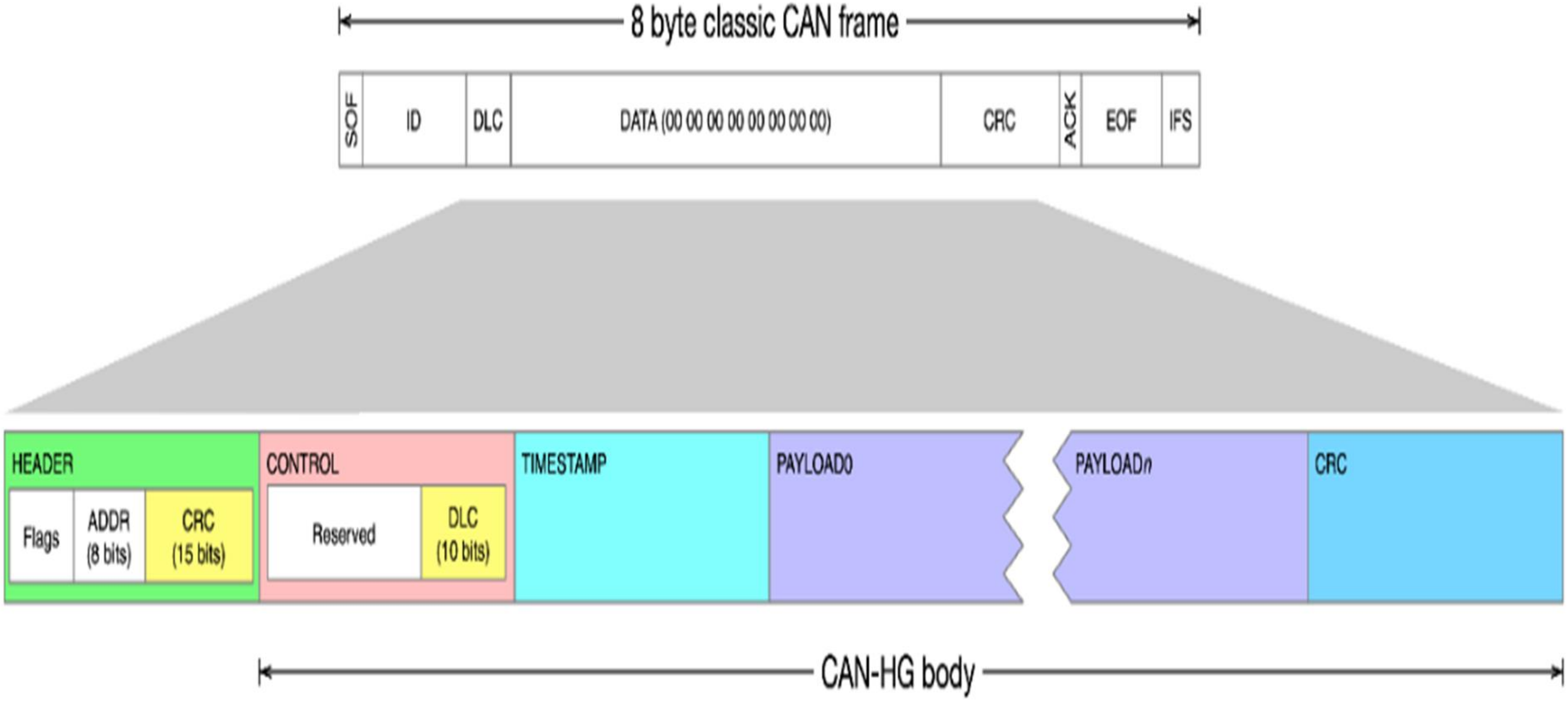


Figure 8: An example system of a central security node protecting a CAN bus of four other nodes

Source: Dr. Ken Tindell, CTO Canis Automotive Labs, CAN-HG overview
Augmenting Classic CAN for Performance and Security

Anatomy of a CAN-HG frame embedded inside a classic CAN frame



Source: Dr. Ken Tindell, CTO Canis Automotive Labs, CAN-HG overview
Augmenting Classic CAN for Performance and Security

Intrusion Detection and Prevention System

- Before the frame accepted by a CAN node, the IDPS alerts in case of spoofing.

- IDPS runs (typically in an interrupt handler) and examines the CAN ID of the partially received frame and the CAN-HG header.
  - If the source address in the header does not match the expected source address of the CAN ID, then the IDS software determines this frame is a spoof.

- The IDPS software destroys the frame by instructing the CAN-HG IDS hardware to raise an error (i.e. transmit an error flag of 6 dominant bits) to destroy the CAN frame.

Each bit sent in 2 microseconds, the CAN-HG will alert the user before complete delivery of packets

CAN-HG

- Integrity – Bus Guardian: Fast Bits encoding Address and CRC

- Availability – Bus Guardian: The central IDPS can broadcast a ‘cease’ command on CAN that causes the Bus Guardian to block the attacking host CAN controller’s signals until further notice.

- Confidentiality – Not addressed

References [Accessed on 21/08/2024]

- https://canislabs.com/cansecurity/
- https://kentindell.github.io/2020/01/20/new-can-hacks/
- https://canislabs.com/downloads/1905-2020-12-14-CAN-HG-overview.pdf
- A. Alfardus and D. B. Rawat, "Evaluation of CAN Bus Security Vulnerabilities and Potential Solutions," *2023 Sixth International Conference of Women in Data Science at Prince Sultan University (WiDS PSU)*, Riyadh, Saudi Arabia, 2023, pp. 90-97, doi: 10.1109/WiDS-PSU57071.2023.00030.