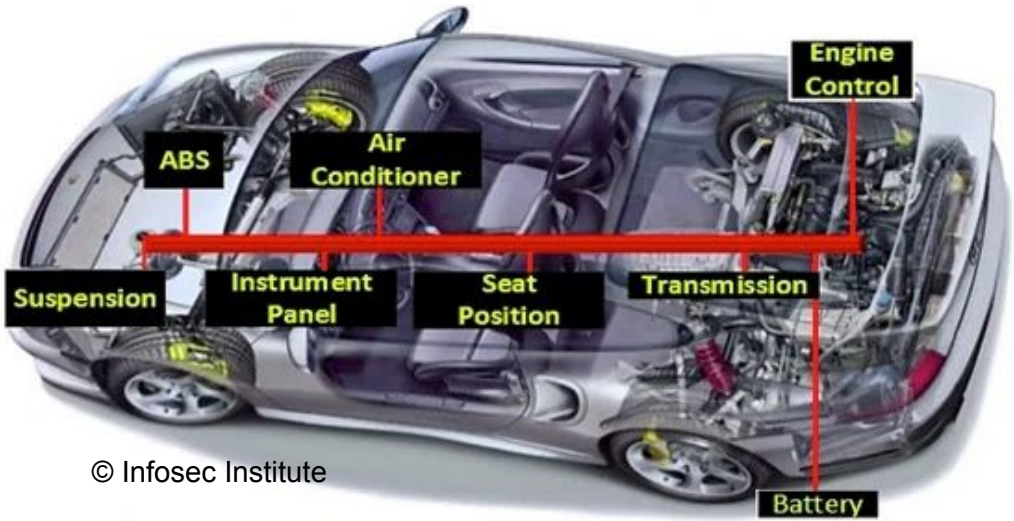
EdgeTDC: On the Security of Time Difference of Arrival Measurements in CAN Bus Systems

Marc Roeschlin, Giovanni Camurati, Pascal Brunner (ETH Zurich),
Mridula Singh (CISPA Helmholtz Center for Information Security), Srdjan Capkun (ETH Zurich)

March 2, 2023, NDSS, San Diego, CA

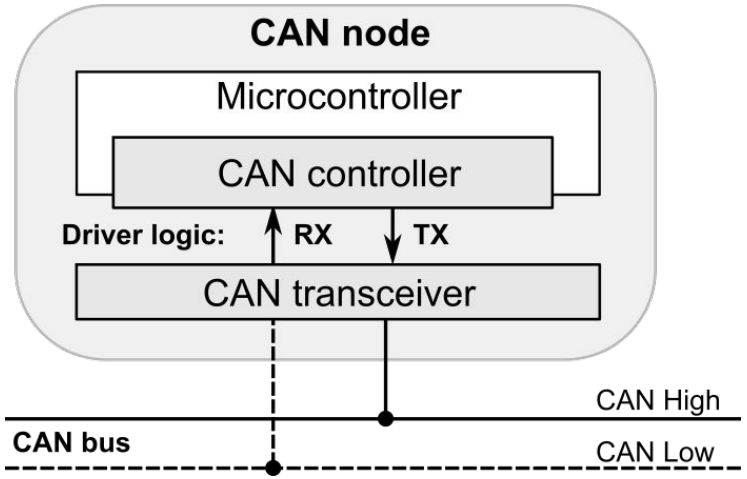
What is CAN Bus?

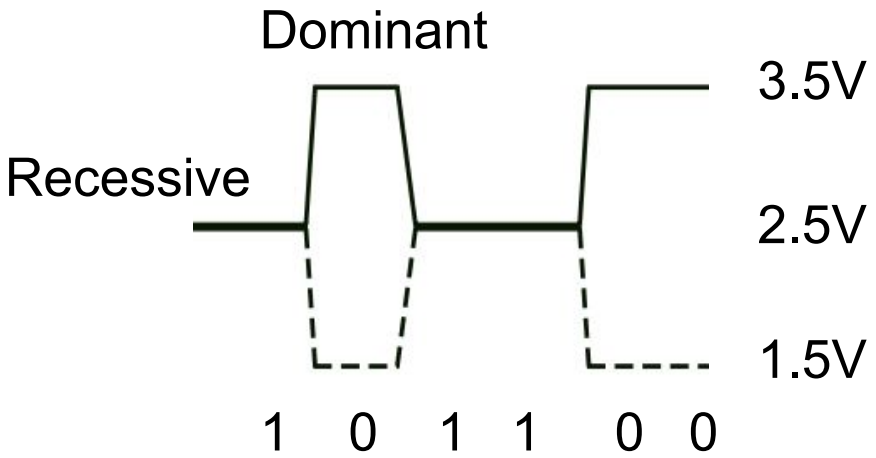
- Robust serial bus protocol
- Decade-old standard for intra-vehicle communication
- Electronic Control Units (ECUs) but also multimedia and other systems



CAN Bus Physical Layer

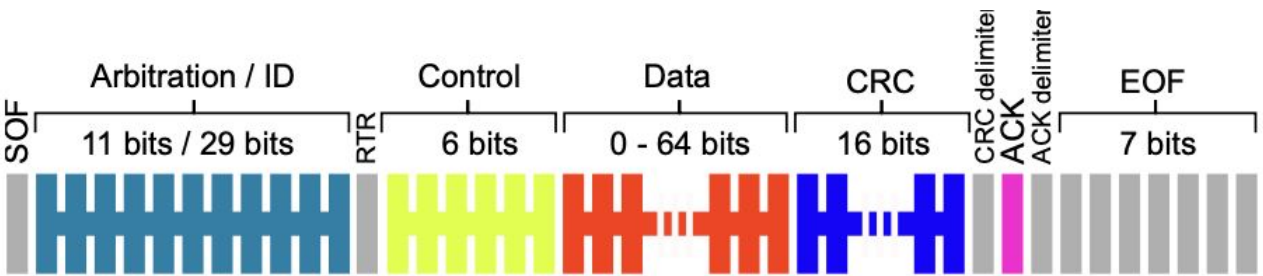
- Twisted pair with multiple nodes
- Differential (dominant/recessive)
- Wired-or: dominant if at least one node is dominant





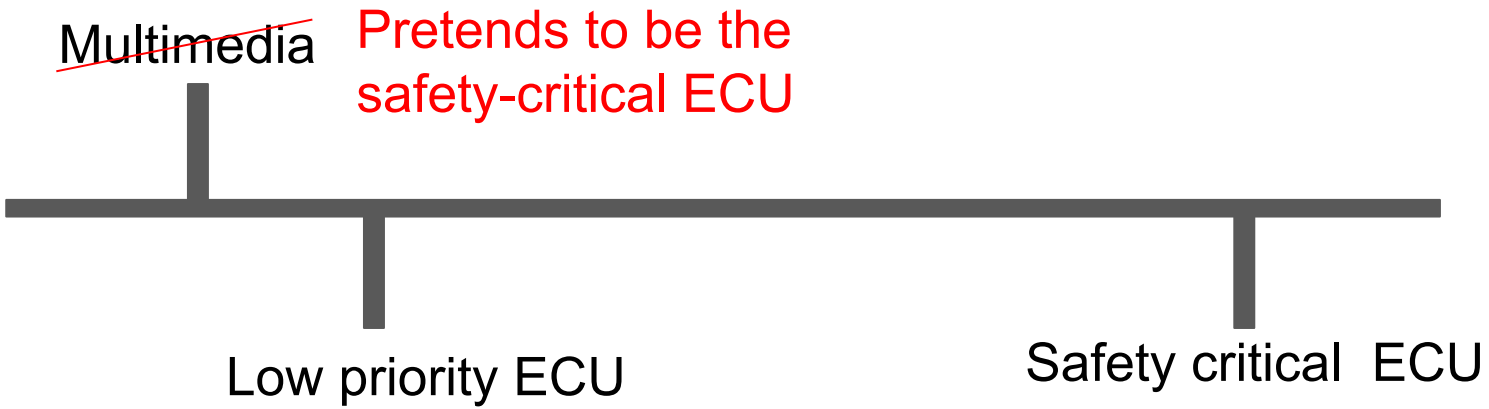
CAN Bus Frames

- Nodes/ECUs only transmit when bus is idle
- Synchronization is achieved through arbitration
  - Dominant bit = higher priority
- Safety-critical messages have higher priority



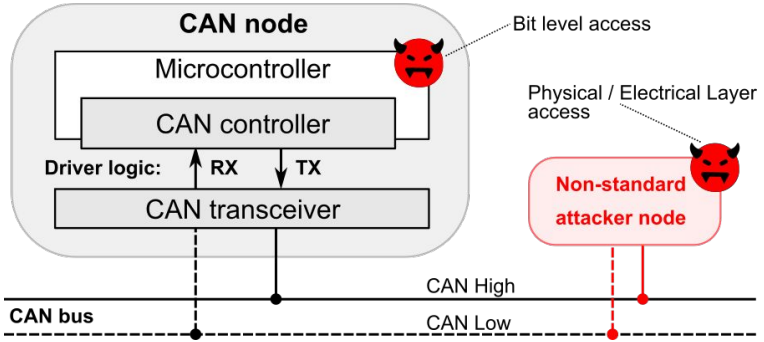
No authentication ⇨ Masquerade attacks!

- CAN Bus messages are **not authenticated**
- **Masquerade attacks**:
  - Low priority node is compromised (e.g., via wireless interface)
  - It impersonates a safety-critical node (e.g., ECU)



Threat Model(s)

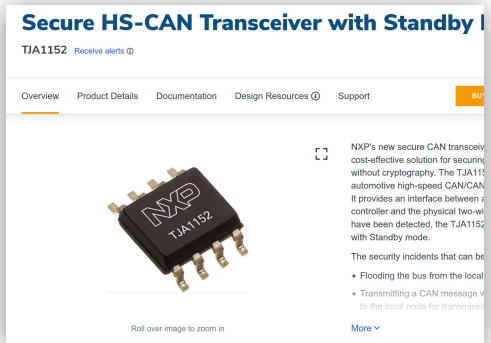
- **Remote attacker**
  - Commonly found in CAN bus literature
  - Attacker gains control over one or more ECUs exploiting another vulnerability, e.g., in Bluetooth
  - Attack vectors limited to interface provided by CAN controller
- **Physical layer attacker**
  - Attaches own proprietary devices to the bus
  - At different locations (OBD, tow hitch, dash, etc.)



Possible solutions

- Cryptographic
  - Many proposals to introduce encryption or authentication
  - None has found adoption in automotive industry
- Quite the opposite:
  - *security without cryptography* announced by NXP
- Network segmentation
- Physical-layer intrusion detection
  - Voltage, timings, …
  - Time Difference of Arrival (TDoA)

Today's topic

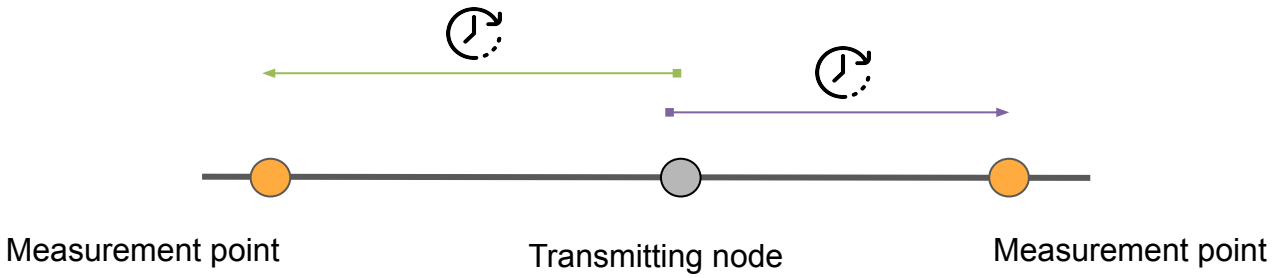


Intrusion Detection Systems for CAN

- As an alternative to authentication, IDS have been proposed
- Extract features from messages transmitted on the bus
  - Physical layer features
  - Voltage, clock, …
- Train a model to detect anomalies
  - Online **(re-)training** required
  - Vulnerable to poisoning attacks

Bhatia et al. *"Evading Voltage-Based Intrusion Detection on Automotive CAN"* NDSS 2021

Time Difference of Arrival to the Rescue?



- TDoA = Difference between arrival times
- TDoA ↔ Position ↔ Identity

Biham et al., *"Tcan: Authentication without cryptography on a CAN bus based on nodes location on the bus",* Embedded Security in Cars 2018.
Moreno et al., *"Sender Authentication for Automotive In-Vehicle Networks through Dual Analog Measurements to Determine the Location of the Transmitter",* ICISSP 2019.
Murvay et al, *"TIDAL-CAN: Differential Timing Based Intrusion Detection and Localization for Controller Area Network"*, IEEE Access, vol. 8, pp. 68 895–68912, 2020

Novel attacks on TDoA

- TDoA is a physical quantity
  - Previous work assumes it cannot be altered
  - Especially by a remote attacker

- We show
  - **TDoA can be manipulated**
  - Even by a **remote attacker**
  - Leading to successful **masquerading attacks evading TDoA IDS**

- Types
  - **Spoofing:** the attacker alter its own TDoA
  - **Poisoning:** the attackers alter the victim's TDoA during re-training

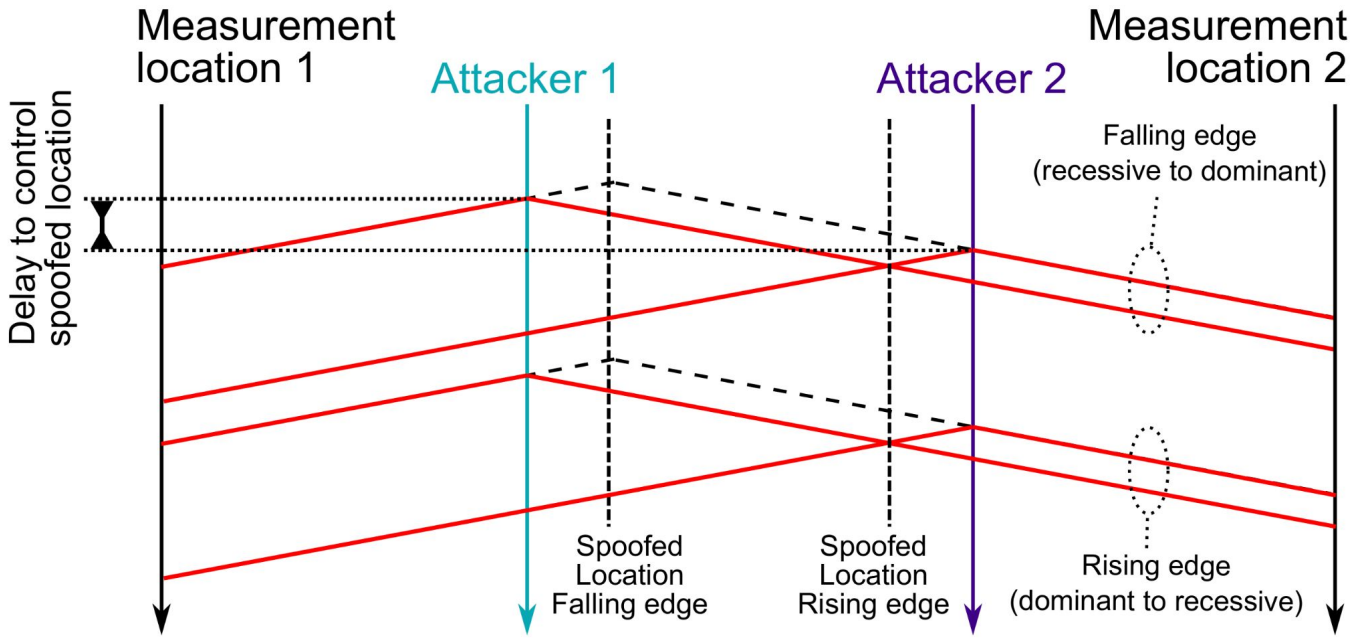
- How?

Message Overshadowing in CAN

- **Building block** for spoofing and poisoning
- Transmit at the same time to alter the TDoA
  - Spoofing: two colluding attackers
  - Poisoning: attacker on top of a victim
- Synchronization
  - Remote: exploit the CAN bus rules (see paper for details)
  - Physical: arbitrary synchronization precision
- Effect
  - The two nodes have two distinct values of TDoA
  - When transmitting together the perceived TDoA is from a node in between

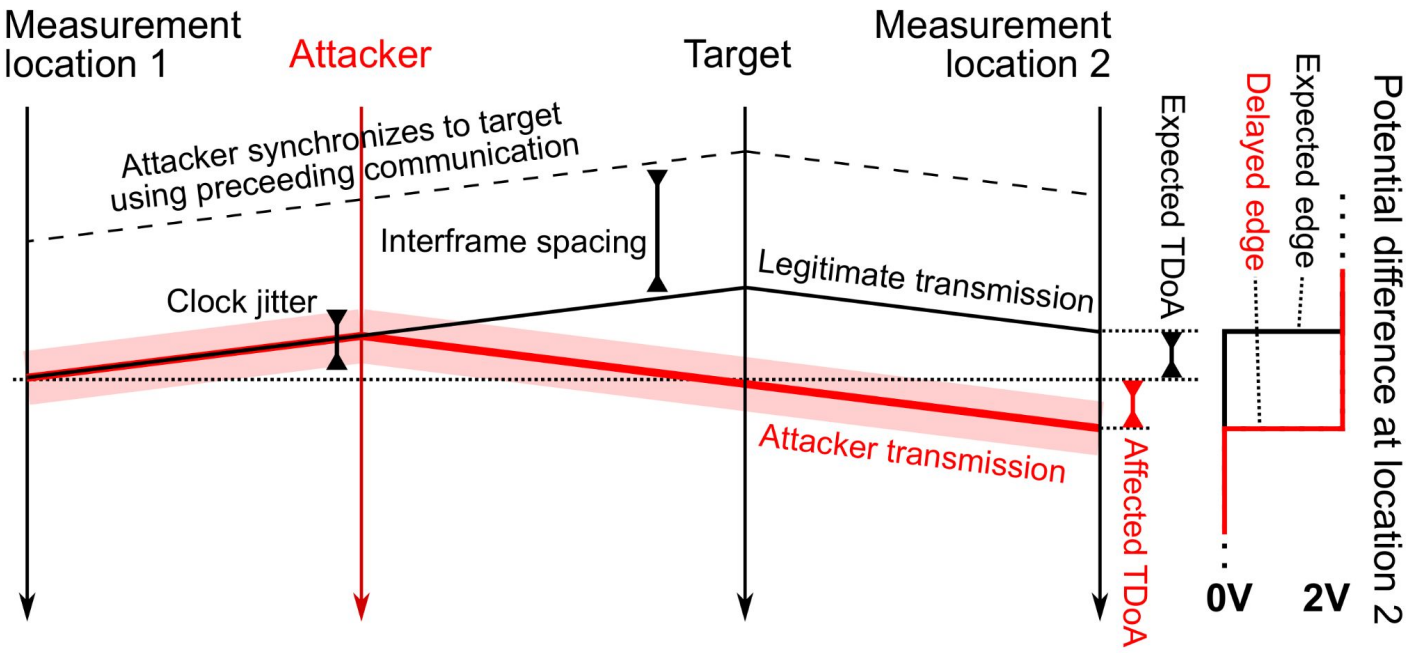
Spoofing Attack

Ex. Physical layer adversary controls at least two nodes able to transmit at the same time



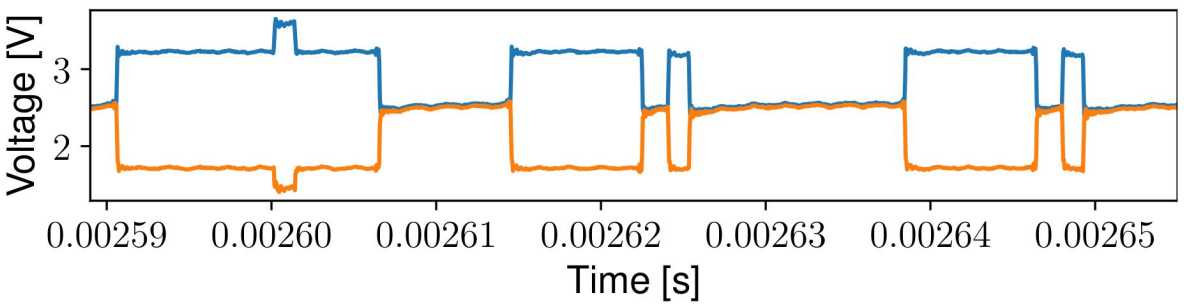
Poisoning Attack

Ex. Remote attacker synchronizes to target and performs overshadowing



Other Attack Types

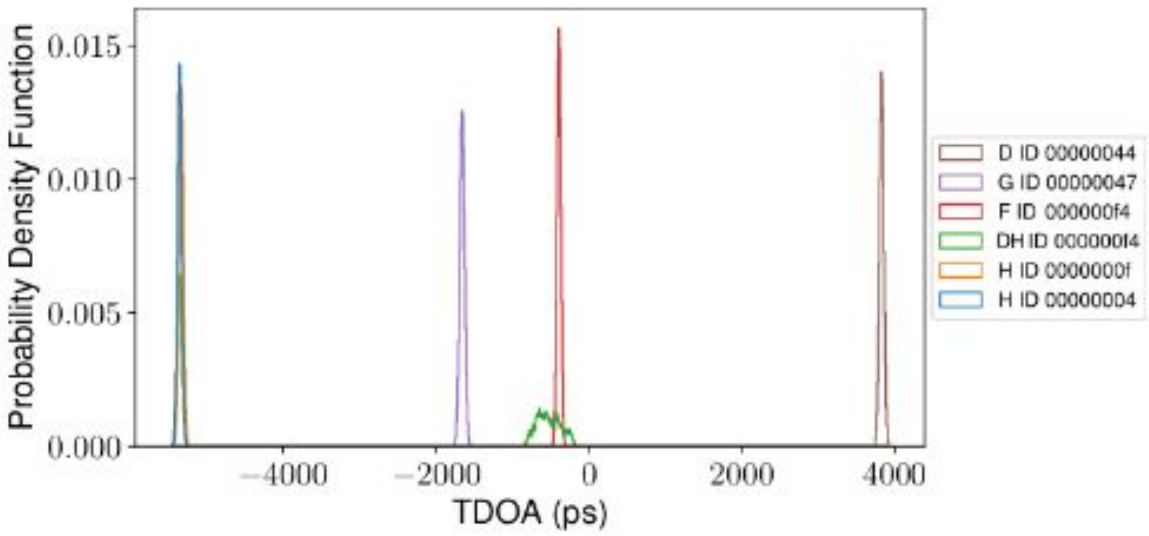
- Shown examples are based on overshadowing
  - Delay/anticipate edges
  - Recessive-to-dominant or dominant-to-recessive
- Plethora of other attack feasible
  - Increase bus load by adding resistance/capacitance
  - Inject extra pulses or noise

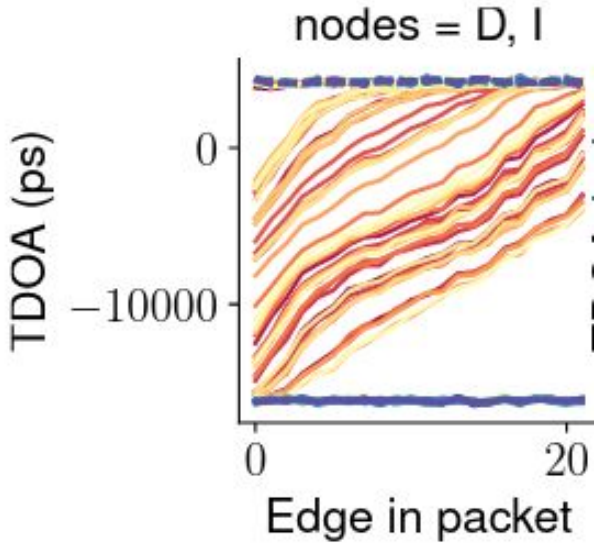


EdgeTDC: Our Approach for an IDS

- Decode CAN messages
  - *knowledge of bits and fields to measure*
- Measure TDoA for both rising and falling edges (except ID and ACK)
  - *increase accuracy*
  - *detect most spoofing/poisoning cases for which rising/falling TDoA is inconsistent*
- Measure intra-packet variance
  - *detect spoofing/poisoning (collusion of devices with different clock increases variance)*
- Check number of edges / number of bit transitions
  - *detect injection of edges at the physical layer*
- Knowledge of the topology and propagation speed, linear model
  - *detect poisoning that would alter the topology or measured propagation speed*
- Secure re-calibration with unpredictable messages from EdgeTDC at BUS ends
  - *prevent spoofing/poisoning during re-calibration*
- Measure TDoA at the output of the transceivers
  - leverage CAN bus hardware itself to filter noise
  - *TDoA measured on clean digital lines, not on the twisted pair*

Example: Spoofing & Intra-packet Variance

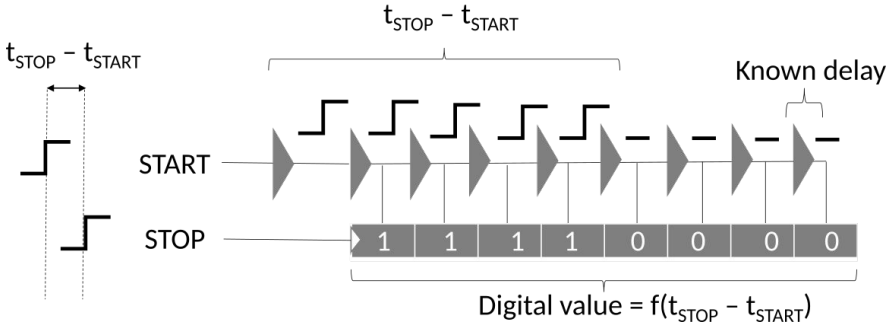


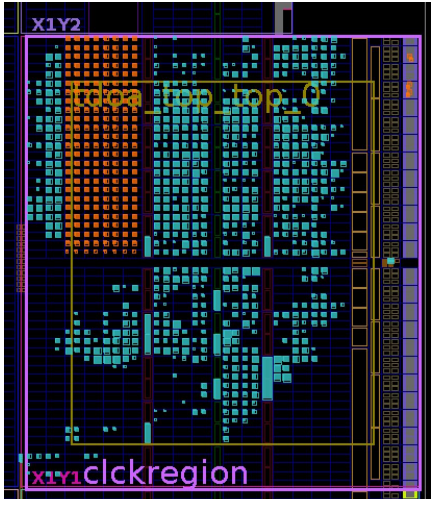


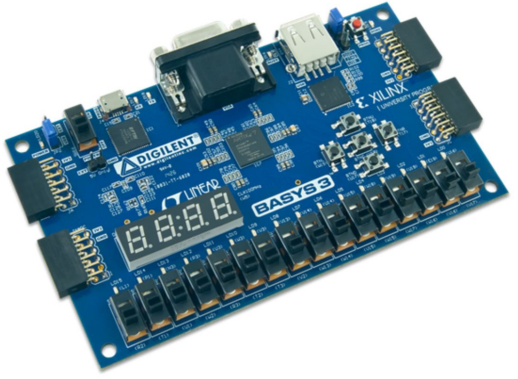
- Successful TDoA spoofing on both rising and falling edges
- But increased variance due to clock drift between the two colluding attackers

EdgeTDC: Implementation

- FPGA-based time-to-digital converter (TDC)
- Precision ~10 cm







EdgeTDC Performance

	Intra-packet variance	Both edges	Update	A1	A2	Victim	FAR	FRR
1	yes	yes	yes	D	H	F	0 %	0 %
2	yes	no	yes	D	H	F	0 %	0 %
3	no	yes	yes	D	H	F	100 %	0 %
4	no	no	yes	D	H	F	100 %	0 %
5	yes	yes	yes	L	E	F	0 %	0 %
6	yes	no	yes	L	E	F	17 %	60 %
7	yes	no	no	L	E	F	41 %	0 %
8	no	no	no	L	E	F	91 %	0 %
9	no	yes	no	L	E	F	0 %	0 %

TABLE III. ABLATION STUDY FOR TDOA SPOOFING.

Check the paper for more details

Conclusion

- CAN Bus is vulnerable to masquerade attacks (no authentication)
- TDoA is a promising feature to verify position/identity of the transmitter
- We show novel remote spoofing and poisoning attacks on TDoA
- We propose a novel and more resilient TDoA IDS (EdgeTDC)

Conclusion

- CAN Bus is vulnerable to masquerade attacks (no authentication)
- TDoA is a promising feature to verify position/identity of the transmitter
- We show novel remote spoofing and poisoning attacks on TDoA
- We propose a novel and more resilient TDoA IDS (EdgeTDC)

Discussion/Questions?