TCAN: Authentication Without Cryptography on a CAN Bus Based on Nodes Location on the Bus

Eli Biham, Sara Bitan, Eli Gavril

Computer Science Dept., Technion

* Patent Pending

Introduction

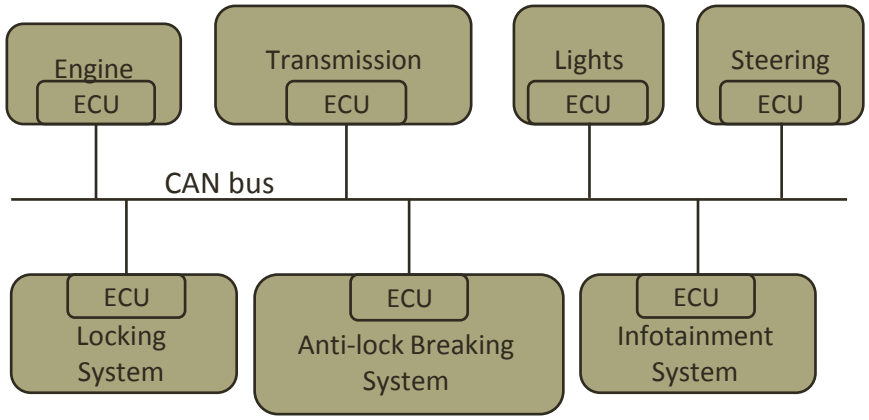
- Cars have become extremely sophisticated in recent years.
- They contain dozens of computerized systems:
  - Anti-lock braking system (ABS)
  - Tire pressure monitoring system (TPMS)
  - Cruise control
  - Backup assist
  - Infotainment
  - And many more…

- Some of these systems are also connected to the internet.

- All of these system communicate with each other through networks
  - the main one is the CAN bus.

The CAN Bus

- In-vehicle systems are connected to the CAN bus via Electronic Control Units (ECUs):



- The ECUs communicate with each other by sending CAN messages:

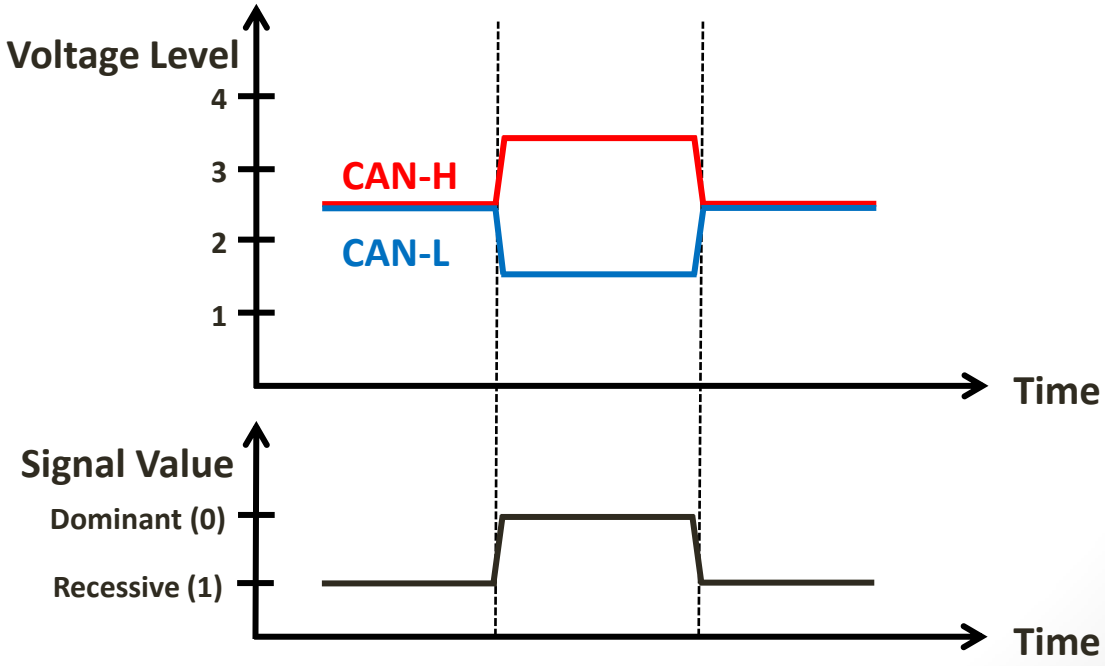
Start of frame (1 bit)	Arbitration (12 bits)	Control (6 bits)	Data (0-64 bits)	CRC (16 bits)	ACK (2 bits)	EOF (7 bits)

Cancellation of Messages

- A Message can be invalidated during transmission by transmitting an error frame over it.
- The error frame is transmitted by an ECU upon detection of a bus error.
- The error frame starts with 6 to 12 consecutive dominant bits.
  - The CAN protocol uses bit stuffing to ensure that no six consecutive dominant bits occur in a CAN message.
- The last chance to transmit an error frame is over the EOF field.

CAN Data Transmission

- The ECUs on the bus are connected by two wires: CAN-H and CAN-L.
  - When voltage levels of CAN-H and CAN-L are equal, the signal on the bus is recessive (i.e., 1).
  - When voltage difference between CAN-H and CAN-L is above a certain threshold, the signal on the bus is dominant (i.e., 0).



The Problem

- The CAN bus has no built-in security mechanisms.
- Any ECU on the bus can send a malicious message
  - with a forged message type to another ECU.
- For example,
  - the infotainment system can send a steering message.

The Problem

- In 2014 two researchers showed how to remotely hack a Jeep Cherokee.
  - They managed to remotely gain access to the CAN bus, and
  - Send malicious messages.
  - They managed to physically influence the vehicle.
- They discovered how to
  - kill the engine
  - disable the brakes
  - influence the steering
  - etc.

Attack Model

- Our attack model consists of an attacker that manages to compromise ECUs on the CAN bus.

- The compromised ECUs can send:
  - Messages that appear to be sent from other ECUs.
  - Or any signal.

- We do not address the issue of an attacker that has physical access to the vehicle.

CAN Bus Authentication

- In order for the CAN bus to be secure, CAN messages need to be authenticated.
- Authentication requirements:
  - Verifying the true sender of the message
  - Verifying that the message has not been tampered with
- Message integrity is supported by the built-in collision detection in the CAN bus.
- Verification of the sender is typically achieved using cryptography.

Existing Solutions

CAN+ and CANAuth

- CAN+ is a protocol that allows inserting 120 additional bits of data to each message.

- The additional bits are transmitted in a “gray zone”
  - A period of time within a CAN bit in which a signal change may be possible without causing errors.

CAN+ and CANAuth

- CANAuth uses CAN+ to send key establishment data and message signatures.

- For each message type or a group of message types
  - a session key is established
  - and distributed to the relevant ECUs.
  - The session key is used by the ECUs to authenticate messages of the corresponding types.

- The problem:
  - If an ECU is compromised then so are all of its session keys.
  - Thus, it can send any message type that it usually just receives.

CaCAN

- CaCAN saves the need of each ECU to authenticate received messages.
- Instead, it uses a special “Monitor” node that checks authentication.
  - And cancels invalid messages by sending an error frame.
- A sending ECU attaches an authentication tag to the message.
  - Containing a counter and a MAC .
  - Computed under a secret shared key of the ECU and the Monitor.
- The problem : an 8-bit MAC is not secure enough.
  - Also, the MAC and counter consume 16 bits of the message.

CMI-ECU

- A Monitor detects malicious messages by using dedicated detection algorithms
  - Typically employ pattern matching or heuristic detection filters.
  - When a malicious message is detected, the Monitor invalidates it by transmitting an error frame.

- Drawbacks
  - Detection algorithms cannot detect all the malicious messages.
  - An attacker may be able to deceive the detection algorithms.

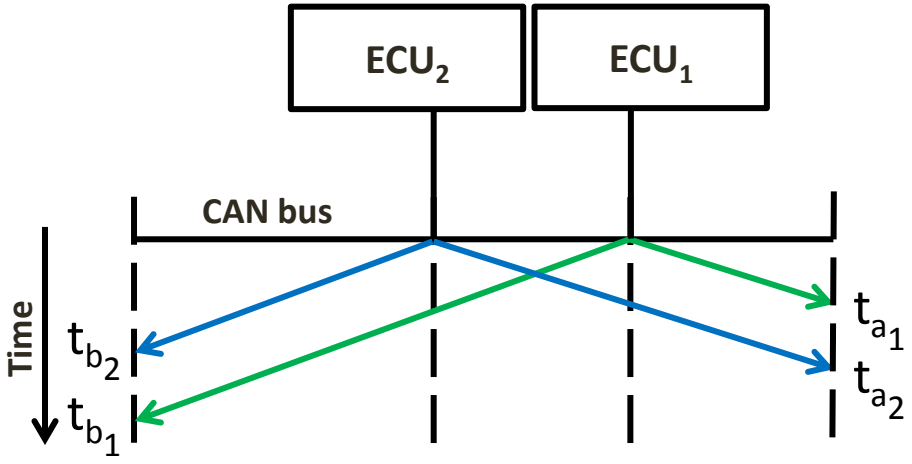
Other Protocols

- TESLA
- Parrot
- etc.

TCAN

Correlation Between Location and Arrival Time

- Consider a signal sent by an ECU
  - And consider its arrival times to the two ends of the bus.
    - We term them t_a and t_b.
- We observe that the location of an ECU on the bus is correlated to the arrival time difference.



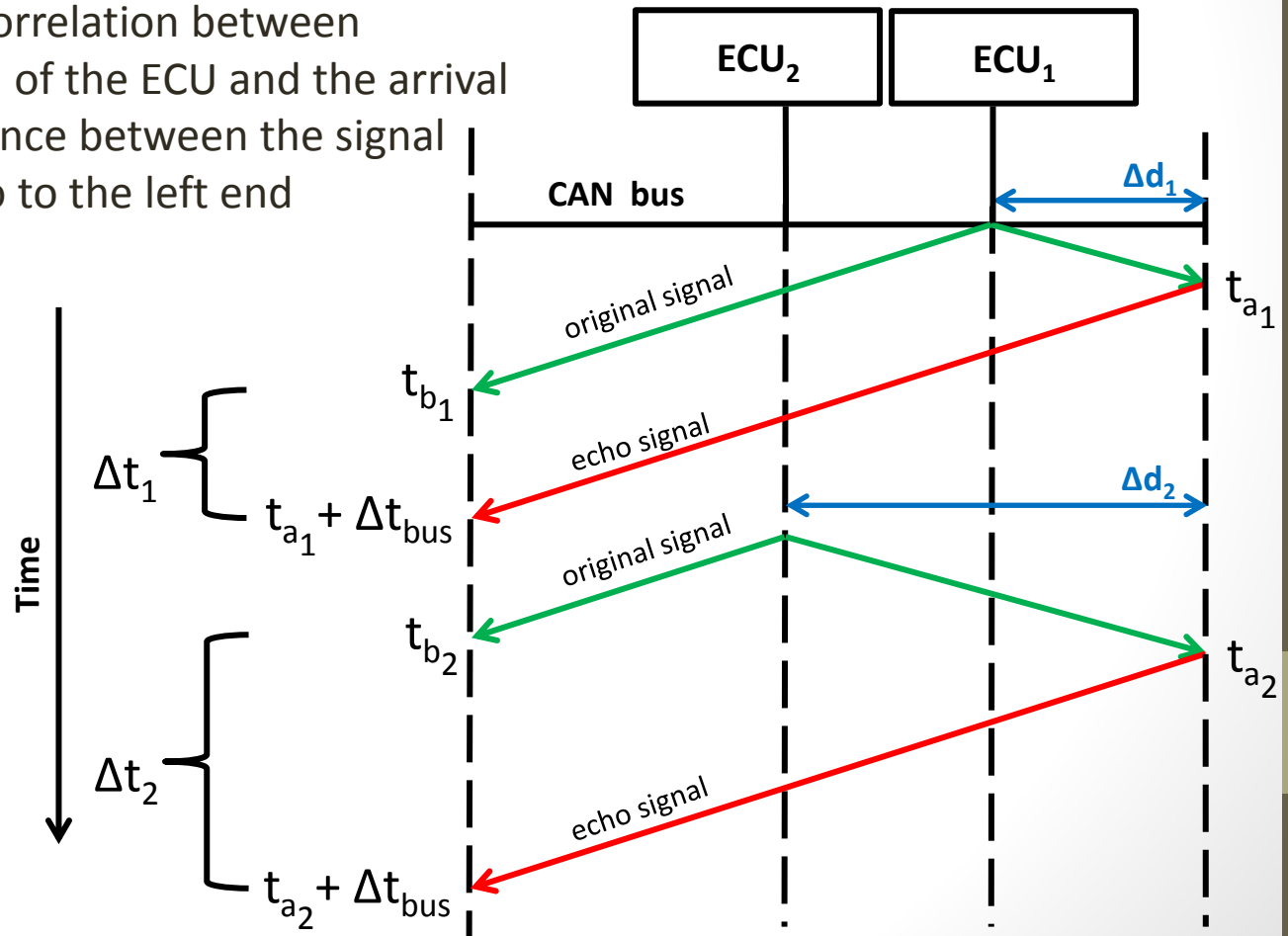
- If we were to know the arrival time difference $t_a - t_b$ of a signal,
  - we would be able to deduce the location of the sender.

Correlation Between Location and Arrival Time

- Consider that any signal that reaches the right end of the bus is immediately echoed back.
  - There is a correlation between the location of the ECU and the arrival time difference between the signal and its echo to the left end of the bus.

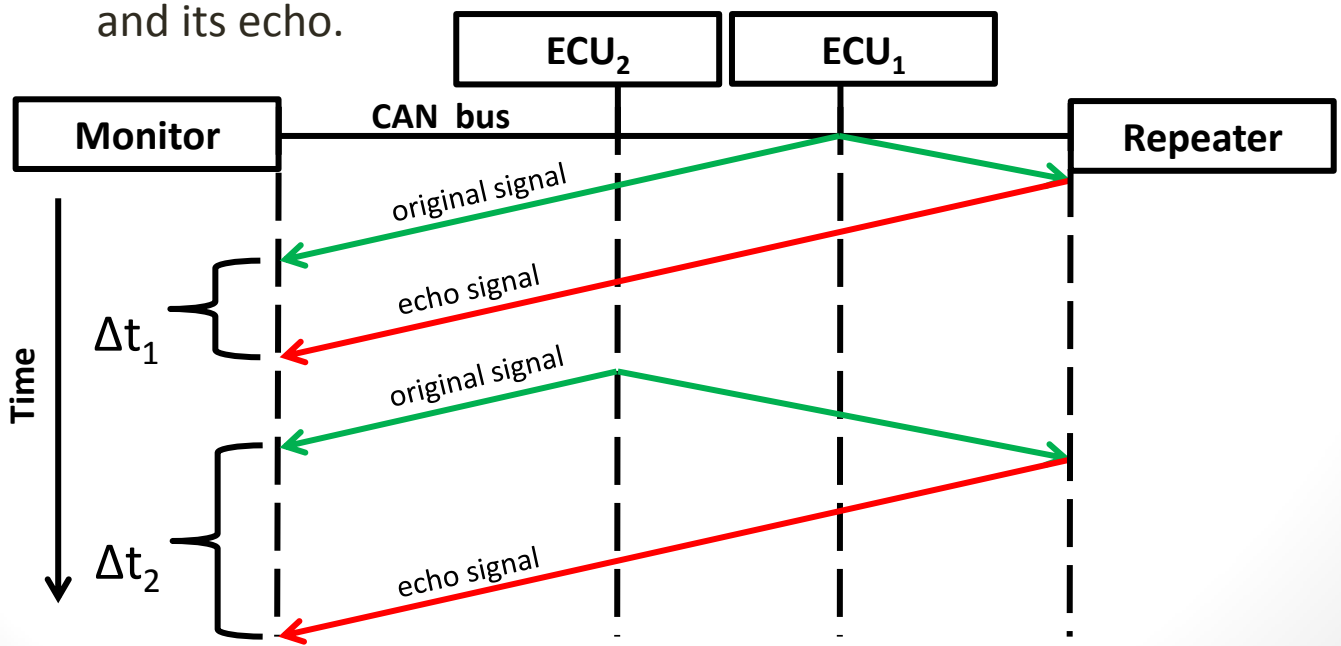
$$\Delta d_1 = \Delta t_1 \cdot c/2$$

$$\Delta d_2 = \Delta t_2 \cdot c/2$$



The Repeater and Monitor

- We install two new nodes at the ends of the bus:
  - A repeater at one end, and a monitor at the other end.
  - The Repeater echoes a signal
    - when it receives messages on the bus.
  - The Monitor deduces the physical location of a sending ECU
    - by measuring reception time difference between a message signal and its echo.



Authenticating the Message

- The Monitor contains an **Authentication Table**
  - a table that contains legal pairs of location and message type.
- The Monitor reads the message type of the message
  - and checks if the message type and the deduced physical location of the sender are a legal pair in the Authentication Table.
- If the pair is legal, the Monitor does nothing.
  - Otherwise, the Monitor invalidates the message by transmitting an error frame.

The Measurement Procedure

- Let S transmit a signal with a recessive-to-dominant edge .
- When the Repeater receives the signal from S, it immediately transmits an echo signal.
  - The echo signal should be identifiable by the Monitor but transparent to standard ECUs.
  - The echo signal has a predefined constant duration.
- The Monitor receives the signal from S and its echo from the Repeater, and measures their time difference Δt_s .
- The Monitor calculates the distance from S to the Repeater as

$$\Delta d_s = \Delta t_s \cdot c/2$$

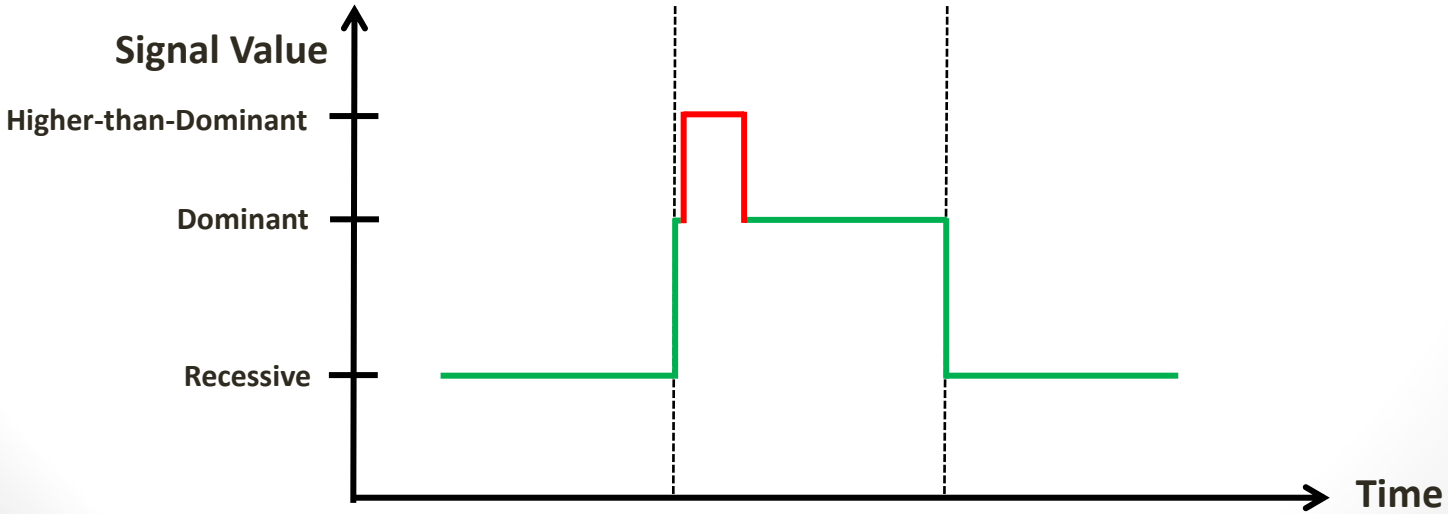
- The procedure returns with failure if one of the following occurs:
  - The echo signal is longer than a standard echo signal.
  - More than one echo signal is received.
- Otherwise, Δd_s is returned.

The Complete TCAN Protocol

- Given an authentication table,
- Let S transmit a message.
- Apply the measurement procedure to deduce the location of S
  - Following any recessive-to-dominant edge after the arbitration phase.
- If the procedure fails, the Monitor cancels the message
  - by sending an error frame.
- Otherwise, let the Monitor perform the following operations:
  - Fetch the message type from the message.
  - Verify that the pair (location, message type) exists in the authentication table.
  - If not, cancel the message by sending an error frame.

Echo Signal Implementation

- The Repeater waits for a recessive-to-dominant edge and sends an echo signal when such edge occurs.
  - The echo signal has a voltage difference which is higher than a regular dominant signal.
- The Monitor is fitted with high measurement capabilities
  - and is thus able to detect the echo signal.
  - Regular ECUs don’t notice the echo signal.



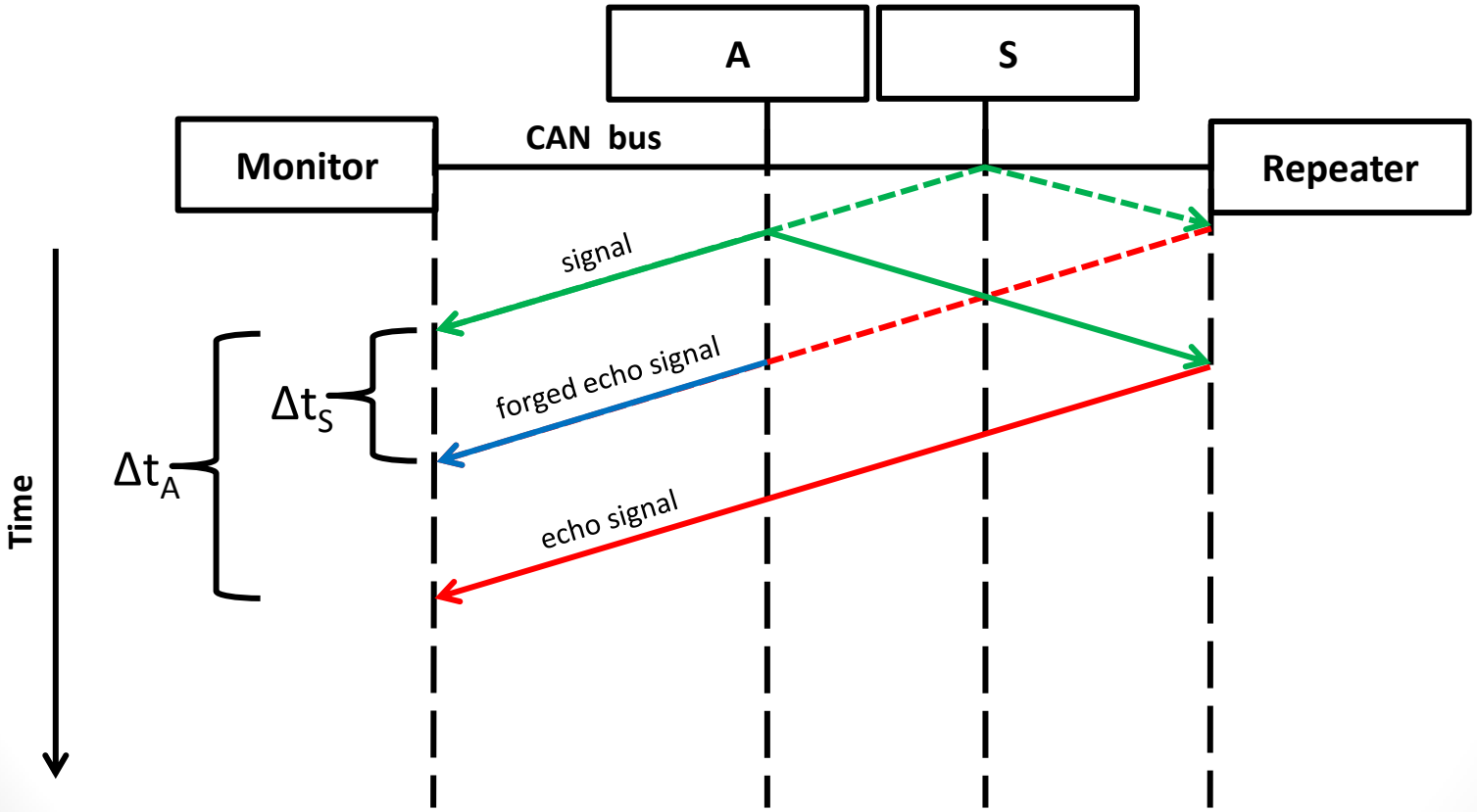
Echo-Forgery Attacks

- An attacker may try to send a forged echo signal in order to deceive the Monitor.

- In such attacks, the attacker wishes to cause the Monitor to deduce a legal origin of the signal,
  - Instead of deducing the location of the attacker,
  - By sending a carefully timed echo signal.

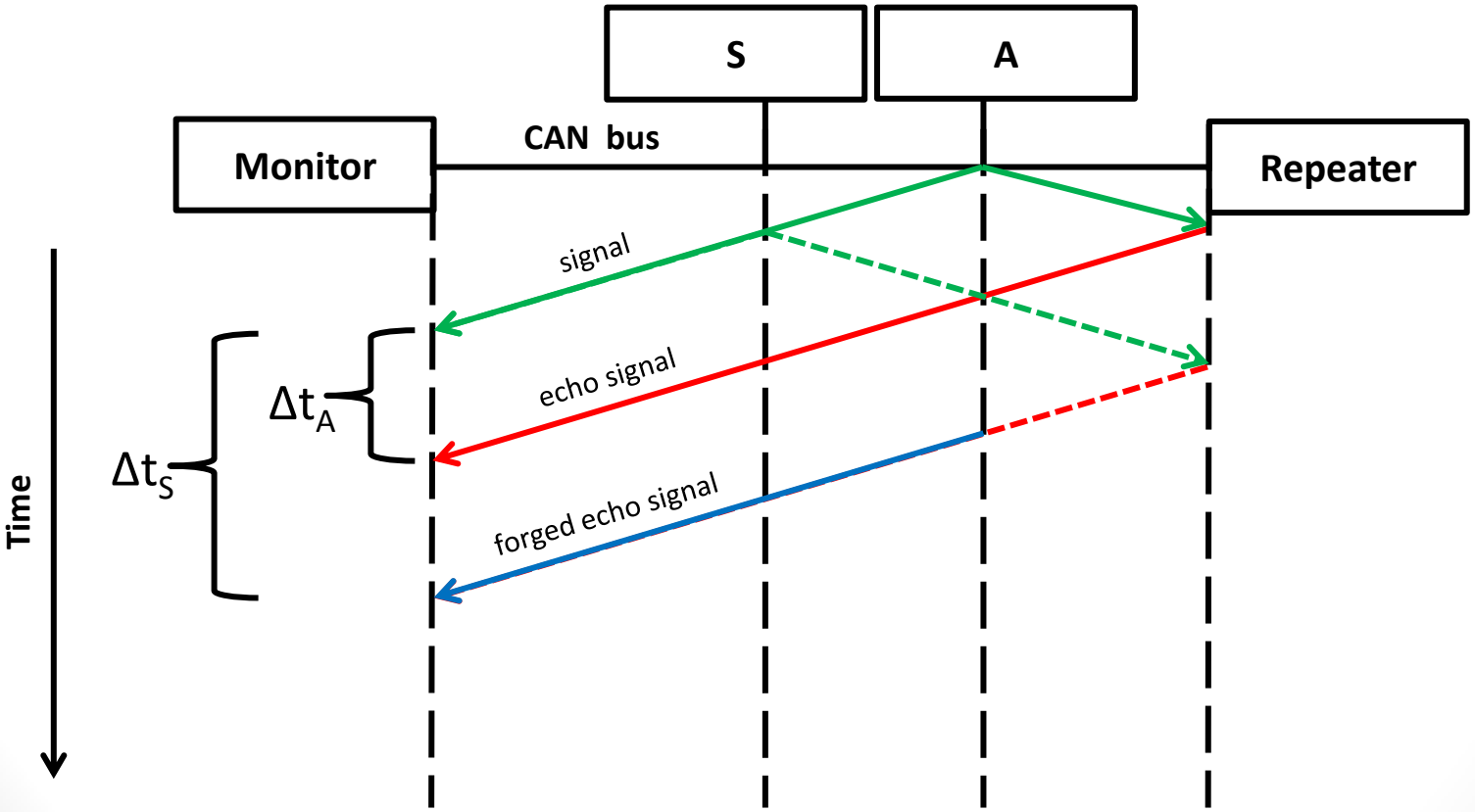
Echo-Forgery Attacks

- An attack from the left side of the legal sender:



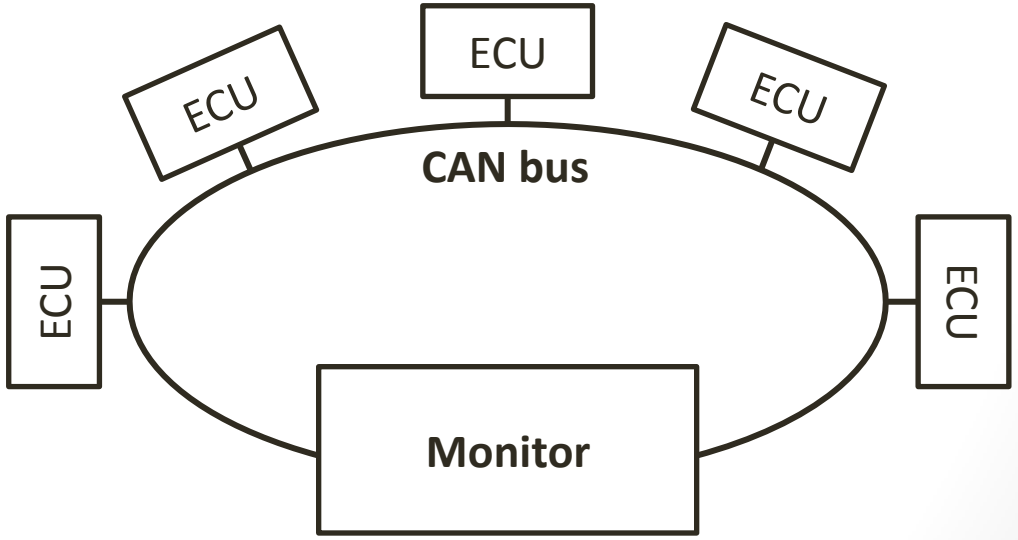
Echo-Forgery Attacks

- An attack from the right side of the legal sender:



Unified Monitor and Repeater

- In this alternative, both ends of the CAN bus are connected into a single device
  - It can monitor signals on both ends of the bus.
  - And can measure the time differences between the two ends.



- Advantages:
  - No echo signal.
  - The Monitor is passive.

Authentication Table Init

- The manufacturer of the car creates a hard-coded table for the Monitor.
  - Or lets the mechanic create/update the table.
  - It is completely cryptography-less.

- Alternatively, manufacturers may choose to automate the creation of the authentication table
  - Having each ECU carry out a cryptographic initialization protocol with the Monitor.
  - Cryptography is used in order to ensure security.
  - The main protocol still remains cryptography-less
    - During the entire ride.

Measurement Accuracy

- The Monitor deduces the location from the arrival time difference using the following equation:

$$\Delta d_s = \Delta t_s \cdot c/2$$

- Let N be the accuracy of measuring the time difference, in nanoseconds.

- The accuracy of Δd_s is therefore:

$$N \cdot c / 2[m] = N \cdot 0.3 / 2[m] = 0.15N[m]$$

Summary

- We presented the TCAN protocol
  - Authenticates messages on the CAN bus
  - Without using cryptography.
- We offered several implementation options.
  - E.g., echo signal.
- We further discuss practical and implementation issues in the paper.
- TCAN is patent pending.

The End