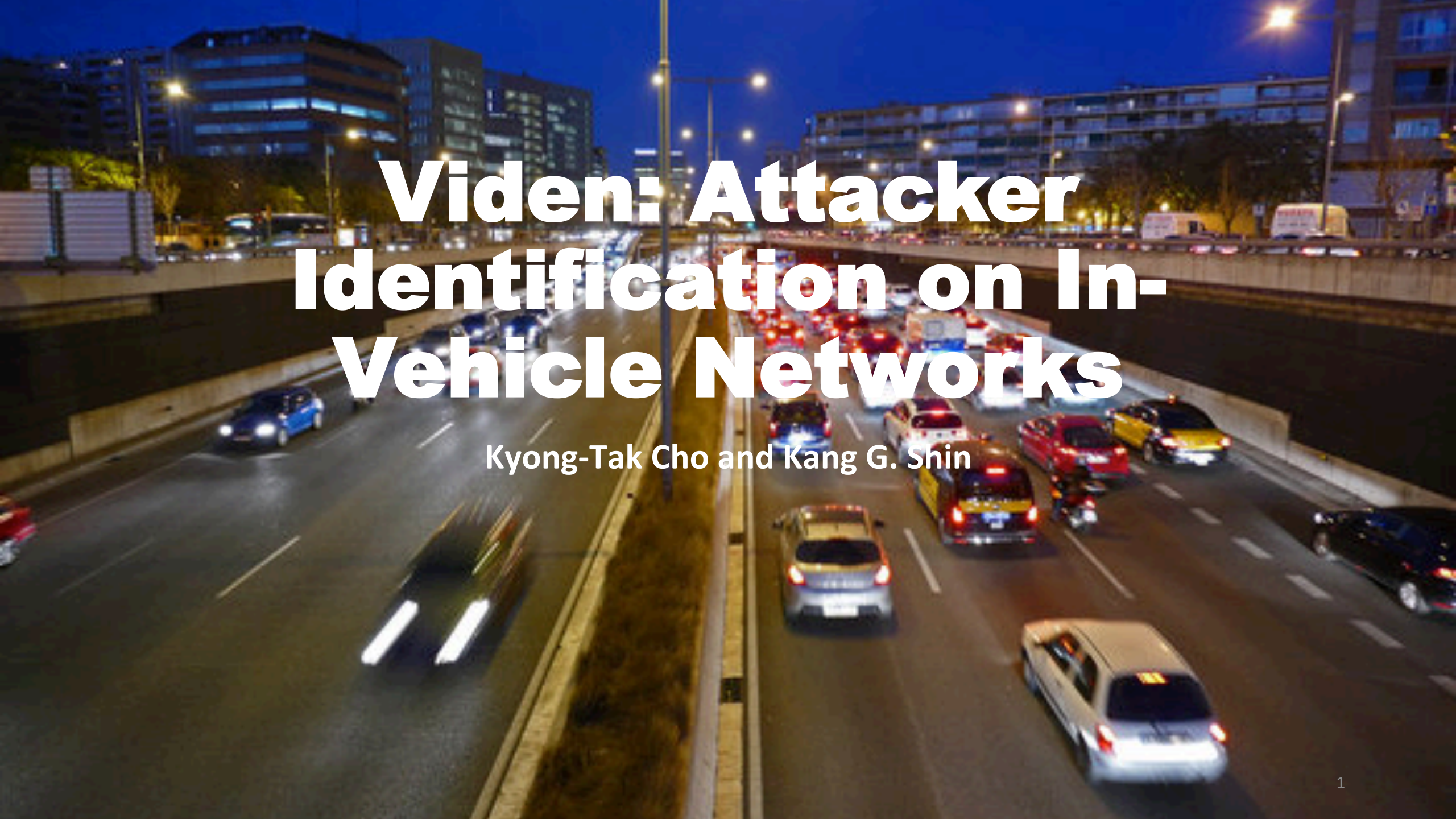


Viden: Attacker Identification on In-Vehicle Networks

Kyong-Tak Cho and Kang G. Shin

Content

- Motivation
- CAN
- Viden
- Evaluation
- Drawback
- Future Work

Content

- Motivation
- CAN
- Viden
- Evaluation
- Drawback
- Future Work

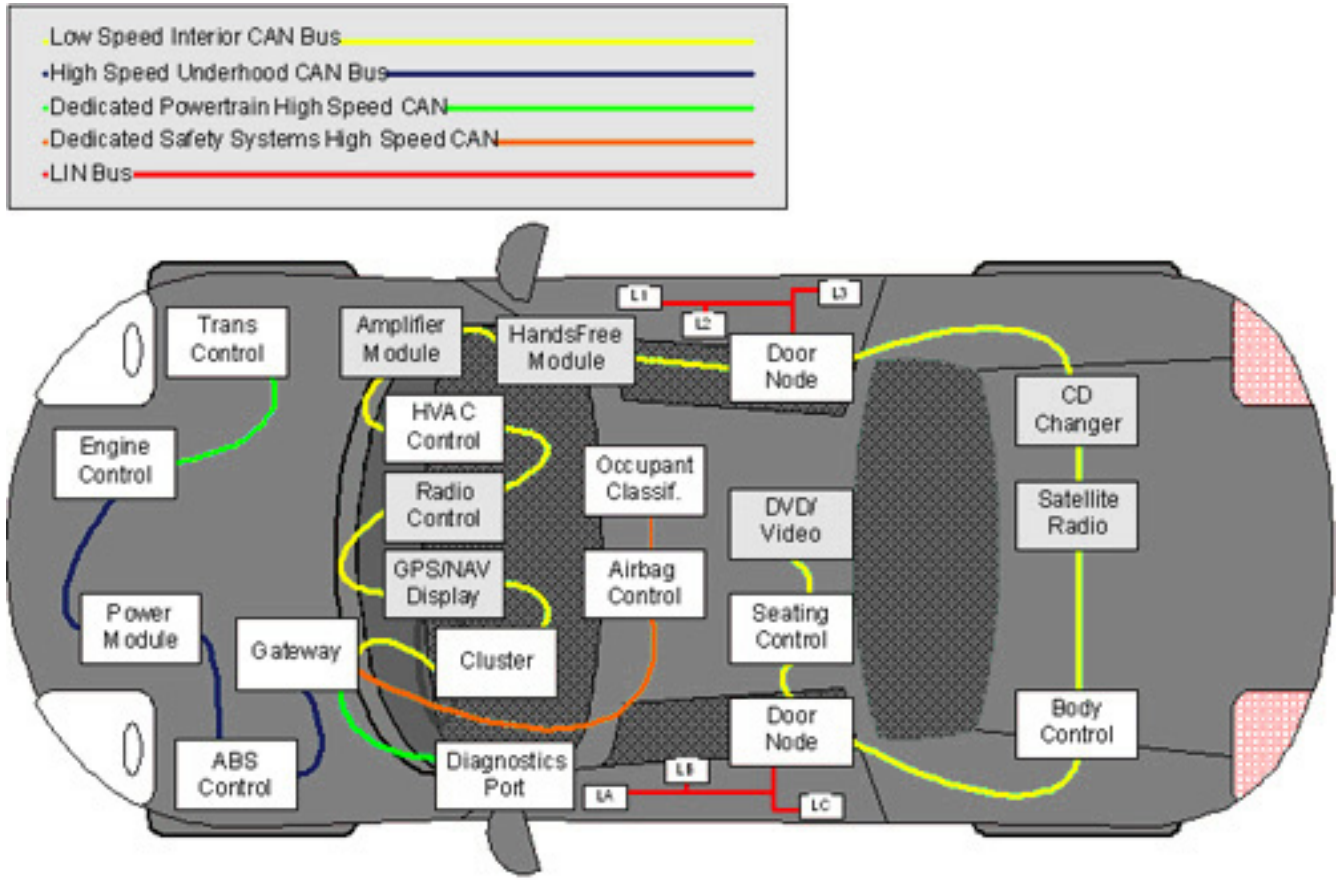
Motivation

- ✓Advancements in Automotive Technology
- ✓Drawbacks in Present Defense Schemes

What is ECU?

- Electronic Control Unit(ECU)
- Types of ECU’s
- Threats

What is ECU?


Low Speed Interior CAN Bus
High Speed Underhood CAN Bus
Dedicated Powertrain High Speed CAN
Dedicated Safety Systems High Speed CAN
LIN Bus
Trans Control
Amplifier Module
HandsFree Module
Door Node
CD Changer
Engine Control
HVAC Control
Occupant Classif.
Radio Control
DVD/ Video
Satellite Radio
GPS/NAV Display
Airbag Control
Power Module
Gateway
Cluster
Seating Control
Door Node
Body Control
ABS Control
Diagnostics Port
L1
L2
L3
LA
LB
LC

Related Work

- Clock based Intrusion detection system
  - Clock Skews
  - Works only in Periodic message
  - Attacker information evaded –a periodic messages
- Mean square voltage measurements
  - Works only with slow speed (10kbps)
- Supervised Batch learning Algorithm
  - Not practical

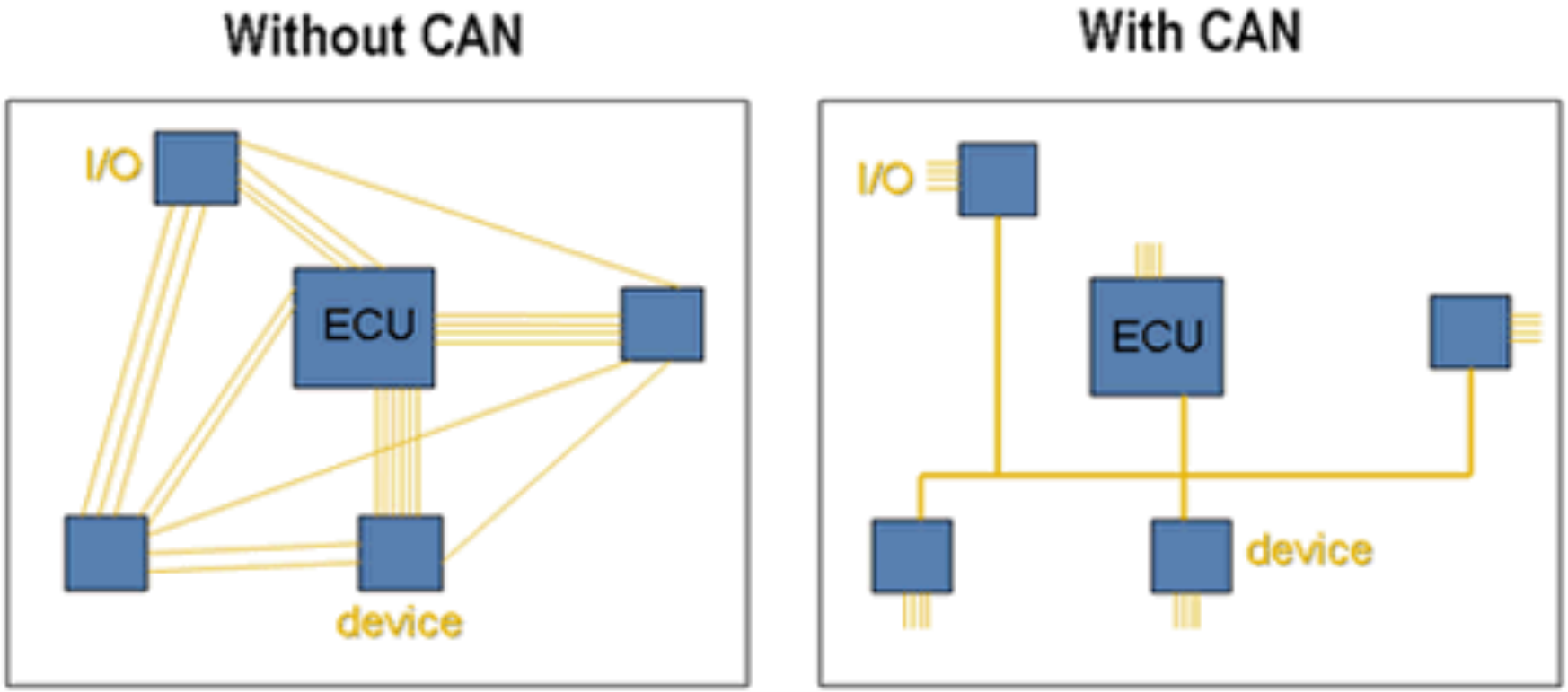
VIDEN: Voltage based attacker IDENtification

- Voltage measurements output by transmitter ECU
- Creates Voltage profiles (Fingerprints) based on voltage instance
- Adaptive signal processing(Online learning)
- Defense mechanism against
  - Naïve adversary
  - Timing-aware adversary
  - Timing-voltage-aware adversary

Content

- Motivation
- CAN
- Viden
- Evaluation
- Drawback
- Future Work

Controller Area Network Protocol



CAN typical application Schematic

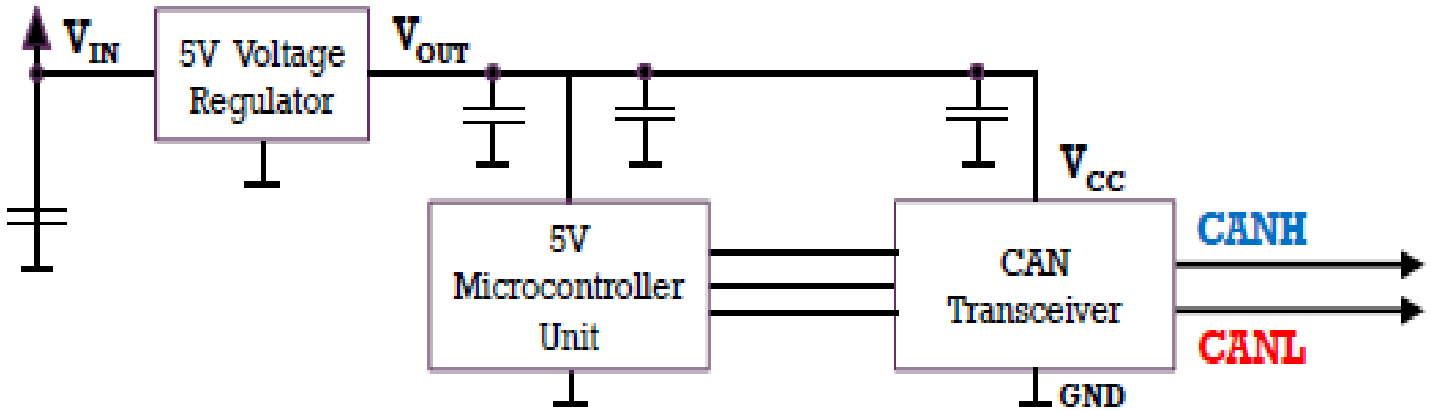
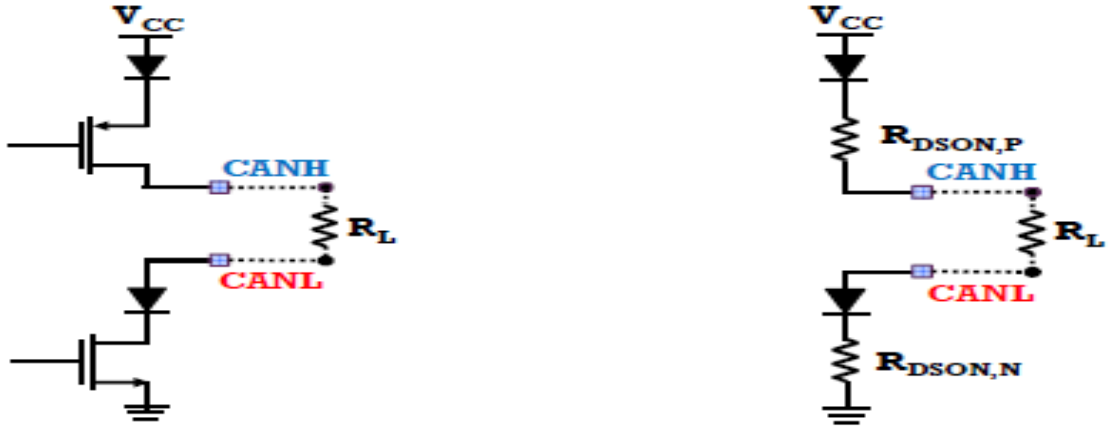


Figure 4: CAN typical application schematic.

CAN output Voltage

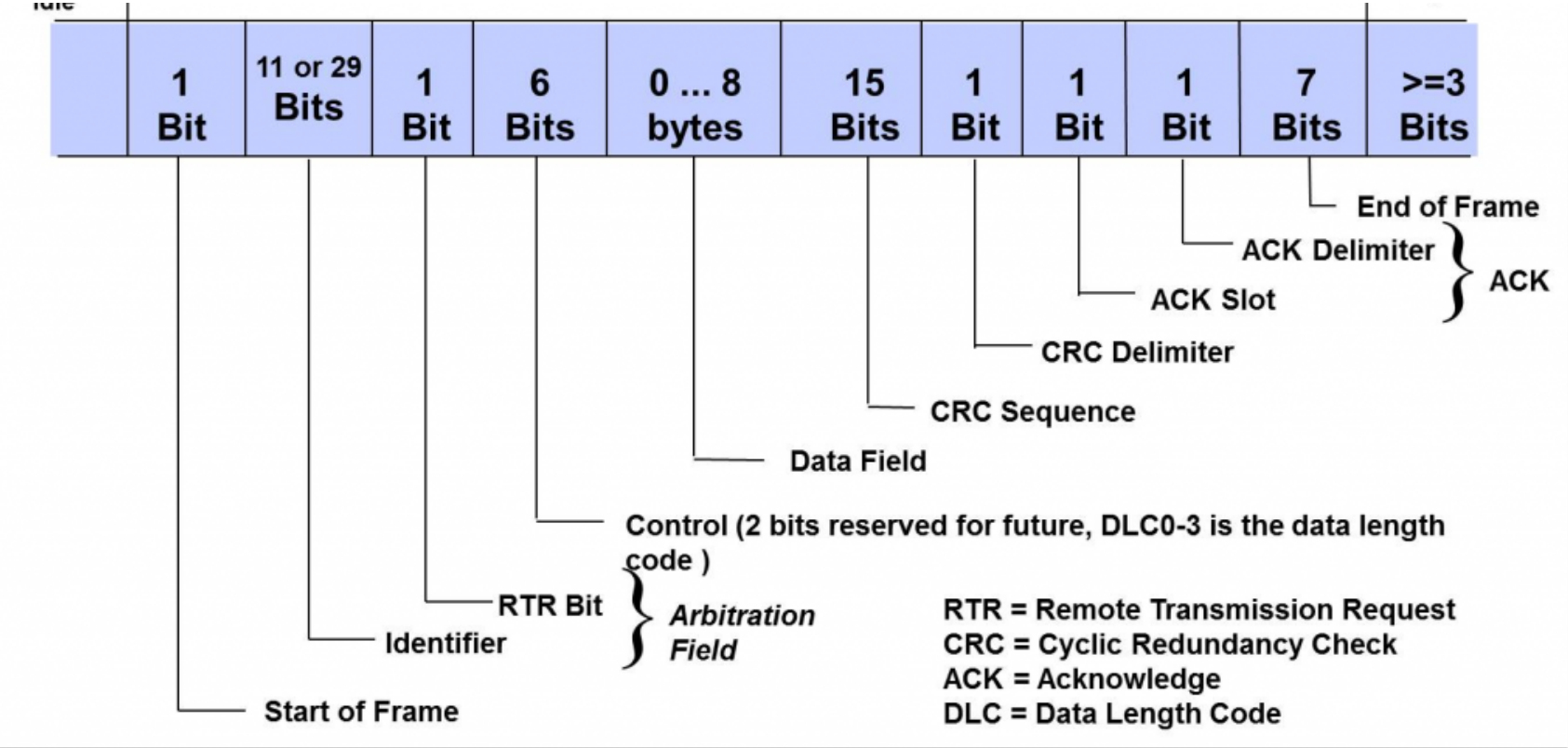
(b) CAN output voltages when sending a message.



(a) Transceiver schematic. (b) When sending a 0-bit.

Figure 2: Output schematics of a CAN transceiver.

CAN Data Frame



Content

- Motivation
- CAN
- Viden
- Evaluation
- Drawback
- Future Work

System and Threat model

CAN bus consideration for system model

- Fingerprinting device- IDS, timing and voltage based
- ECU attached only through CAN bus

Threats involved are naïve, timing-aware and timing-voltage-aware adversaries

High-Level Overview of Viden

Involves Four Phases

- Phase 1: Learning ACK Threshold
- Phase 2: Derives Voltage instances
- Phase 3: Creates Voltage Profiles
- Phase 4: Verification

Phase 1: Learning ACK Threshold

- Measuring dominant voltages
- Extracting Non-ACK voltages

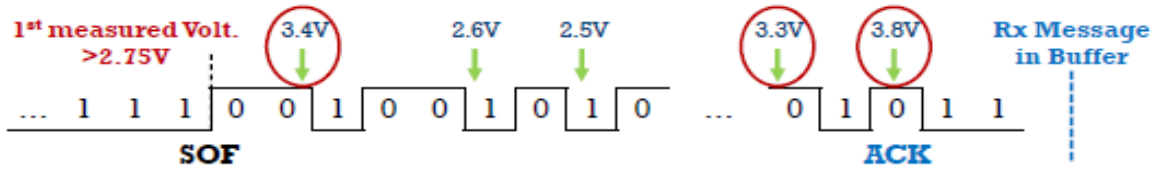


Figure 6: Viden measuring CANH voltages.

Phase 2: Deriving A Voltage Instance

Algorithm 1 Dispersion Update

function UPDATEDISPERSION(V, Λ, P^*)
    return $\Lambda \leftarrow \Lambda + \alpha(P^* - \frac{\#(V<\Lambda)}{\#V})^3$ ▷ Adjust tracking position
end function
if #measured CANH and CANL voltages both $\geq \kappa$ **then**
    $V_H, V_L \leftarrow$ {past κR CANH, CANL measurements}
    $F_3 \leftarrow$ UPDATEDISPERSION($V_H, F_3, 0.75$)
    $F_4 \leftarrow$ UPDATEDISPERSION($V_L, F_4, 0.25$)
    $F_5 \leftarrow$ UPDATEDISPERSION($V_H, F_5, 0.9$)
    $F_6 \leftarrow$ UPDATEDISPERSION($V_L, F_6, 0.1$)
end if

Phase 3: Attacker Identification

$$CVD_x[n] = CVD_x[n-1] + \Delta[n]\left(1 - \nu_x[n]/\nu_x^*\right),$$

$$\Psi[n] = \sum_{x=1}^{6} CVD_x[n].$$

$$\Psi_{accum}[n] = \sum_{k=1}^{n} \Psi[k]$$

Phase 4: Verification

- Birthday paradox
  - ✓ Voltage profile collision
  - ✓ Multiple ECUs can have same profile
  - ✓ Narrower set up of ECU to look at

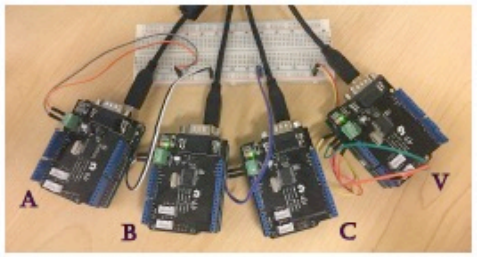
Target impersonation

- ✓ Further verification required to complement the Phase 1-3

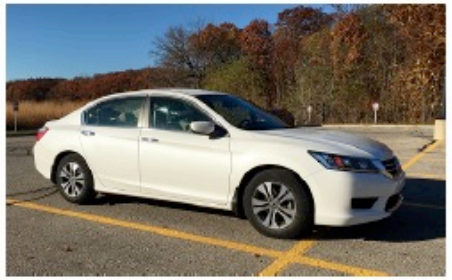
Content

- Motivation
- CAN
- Viden
- Evaluation
- Drawback
- Question

Evaluation

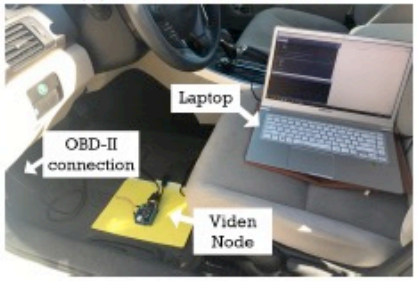


(a) CAN bus prototype.



(b) 2013 Honda Accord.

(c) 2015 Chevrolet Trax.



(d) Connection to the vehicle.

- Against Timing adversary
- Against Timing and Voltage adversary

Content

- Motivation
- CAN
- Viden
- Evaluation
- Drawback
- Question

Drawbacks

- Attack from another network ECU
- Atleast One Voltage profile
- No message send from the ECU – Inaccurate identification
- Voltage profile adjustments

Content

- Motivation
- CAN
- Viden
- Evaluation
- Drawback
- Question

Question

THANK YOU