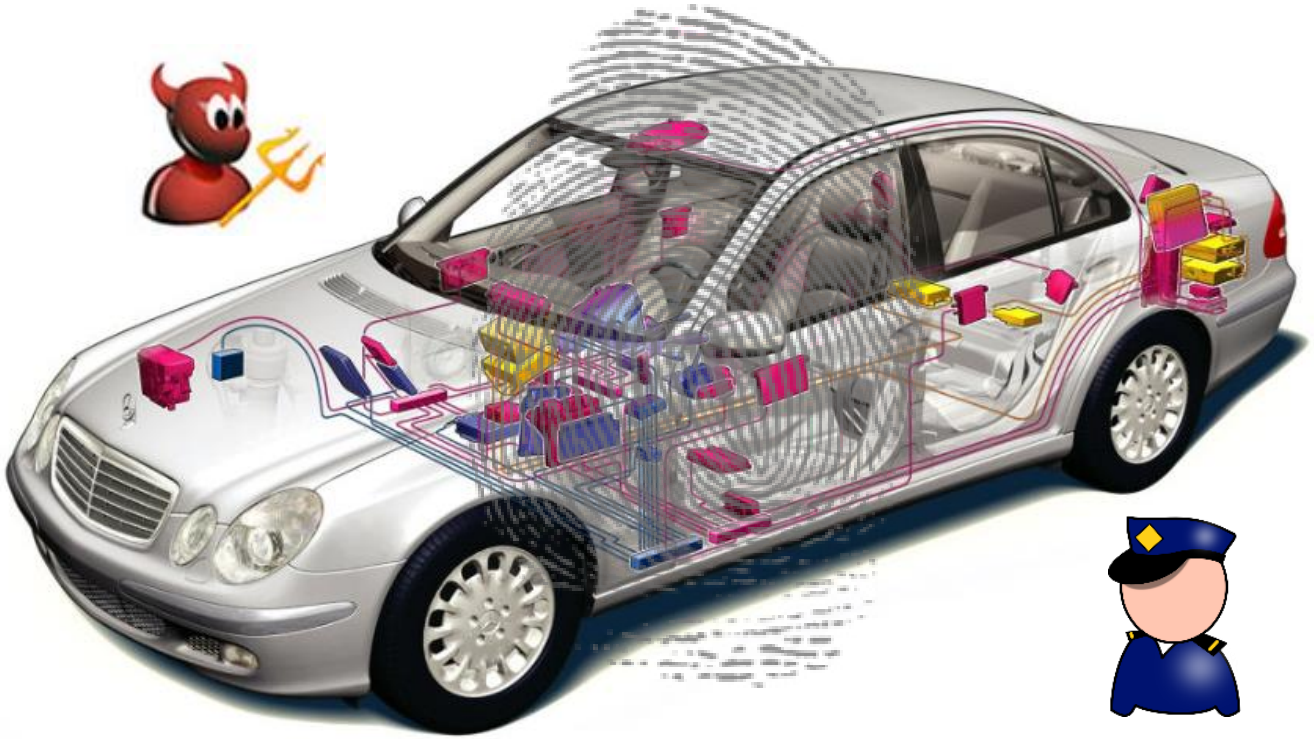
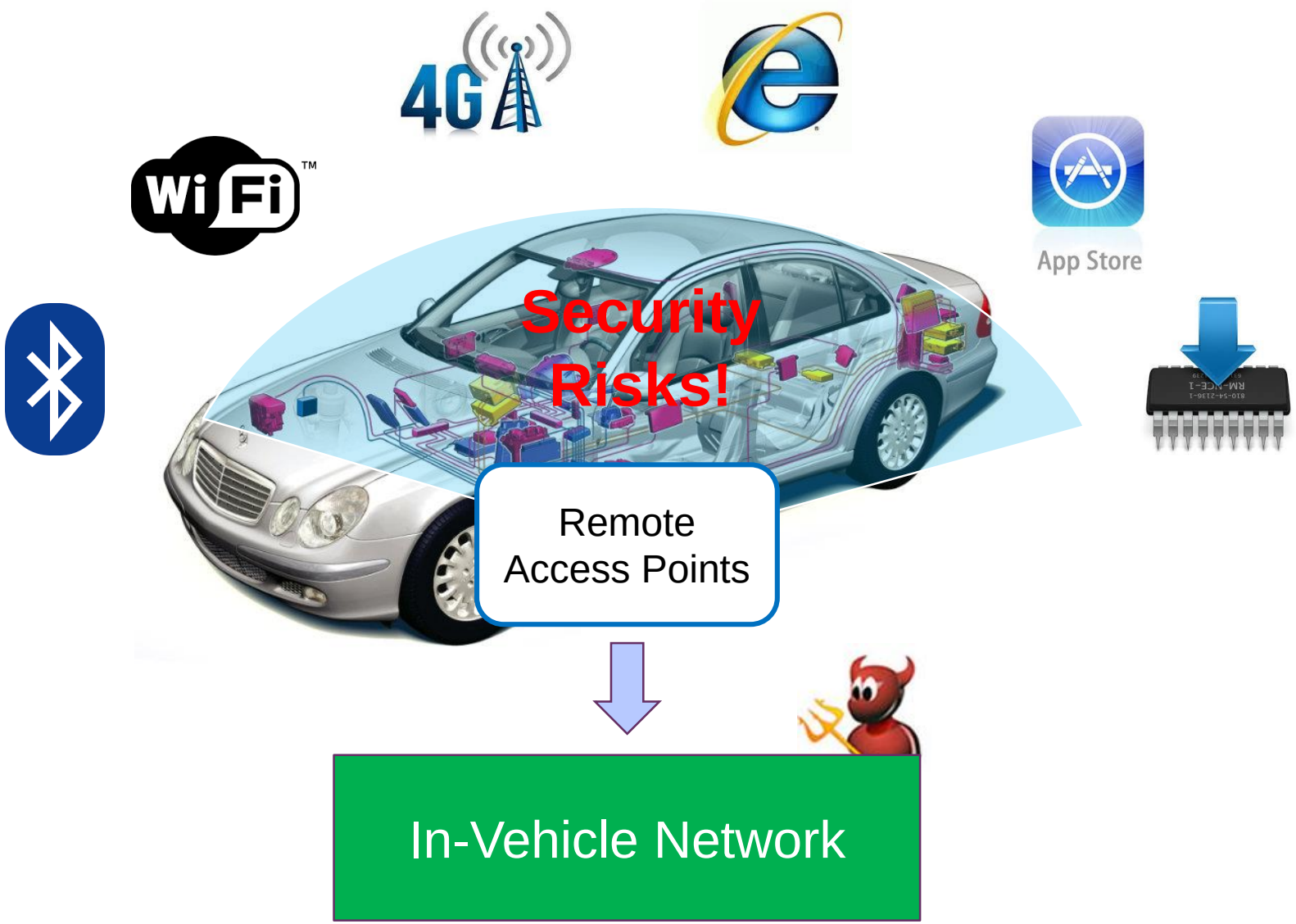
Fingerprinting Electronic Control Units for Vehicle Intrusion Detection



Kyong Tak Cho and Kang G. Shin
The University of Michigan

UNIVERSITY OF MICHIGAN

Vehicle Cyber Attack

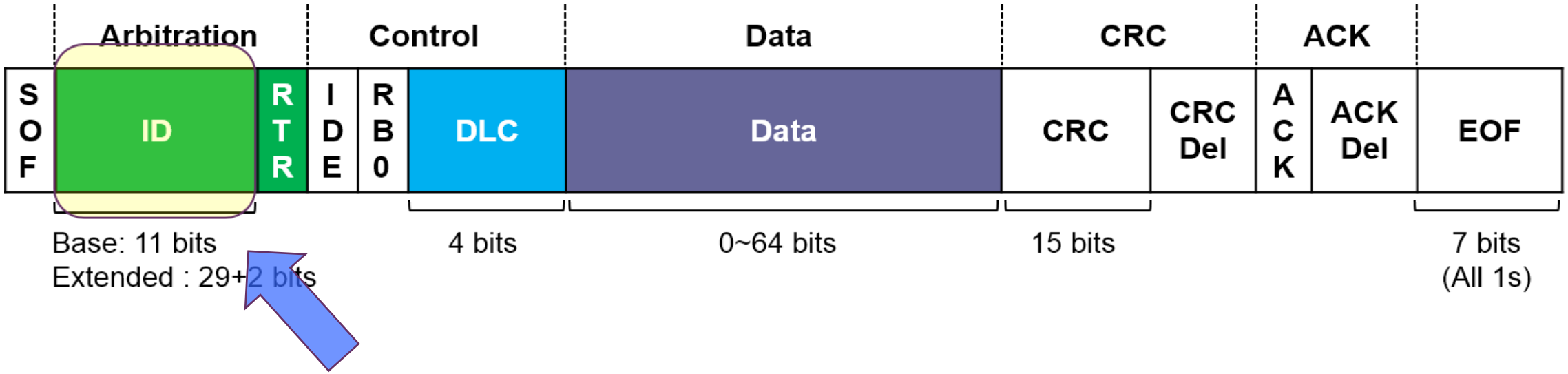


Vehicle attacks are real!

Source: K. Koscher *et al*, “Experimental Security Analysis of a Modern Automobile”, IEEE S&P’10

CAN (Controller Area Network)

CAN Message Format



- Message-oriented addressing
  - ID represents message contents
  - No info who sent the message.

+ Attack Model : “Attacker”

Strong

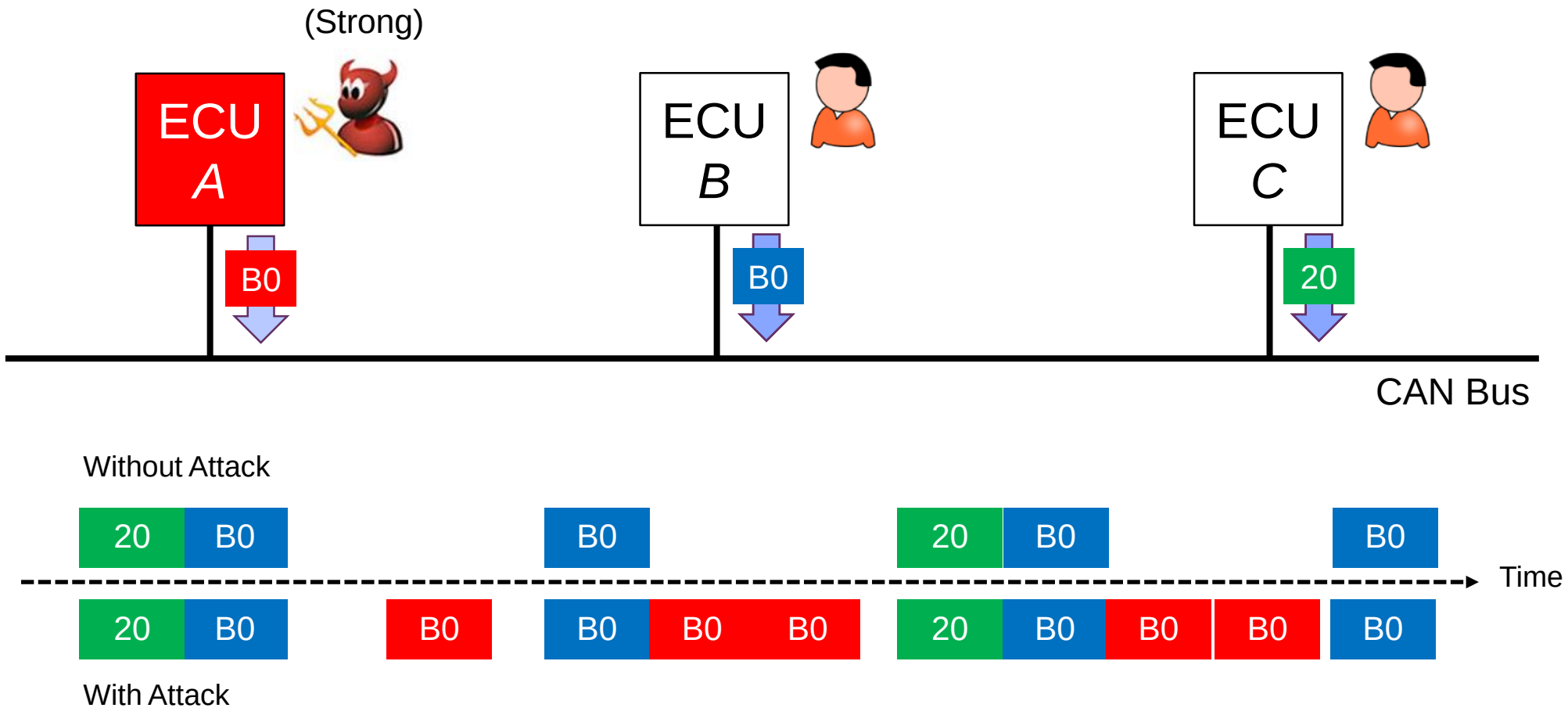
Start + Stop
Tx

Weak

~~**Start +**~~ **Stop**
Tx

Attack Model

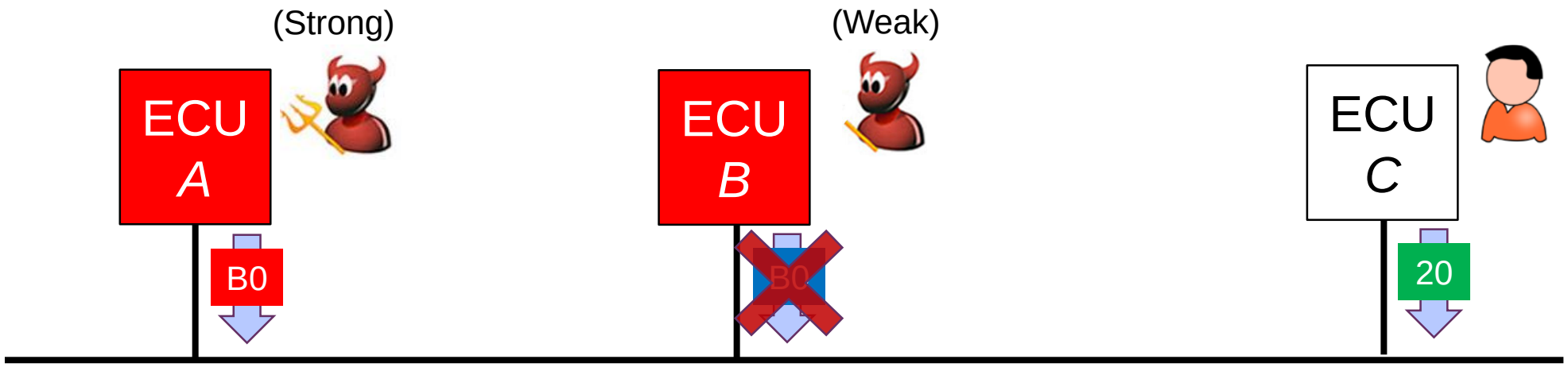
Method 1 & 2: *Fabrication* and *Suspension* attack

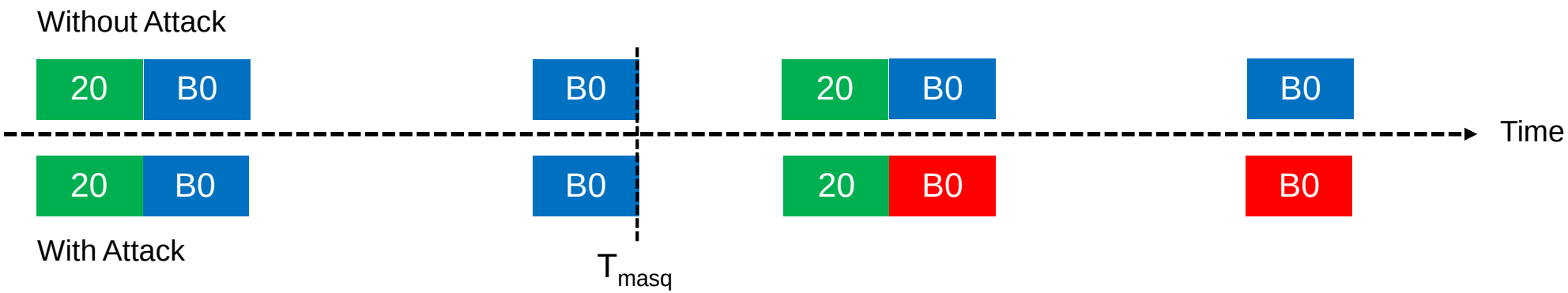


Source: K. Koscher *et al*, “Experimental Security Analysis of a Modern Automobile”, IEEE S&P’10

Attack Model

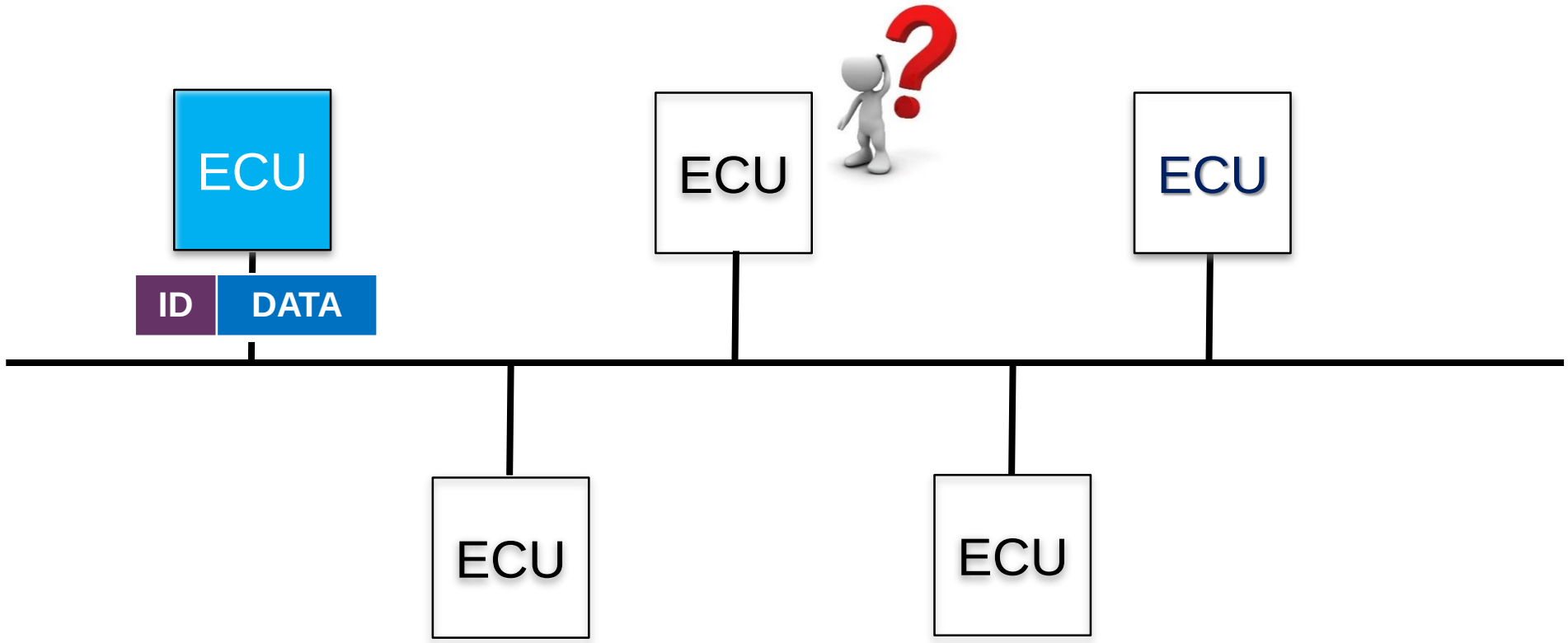
Method 3: *Masquerade* attack





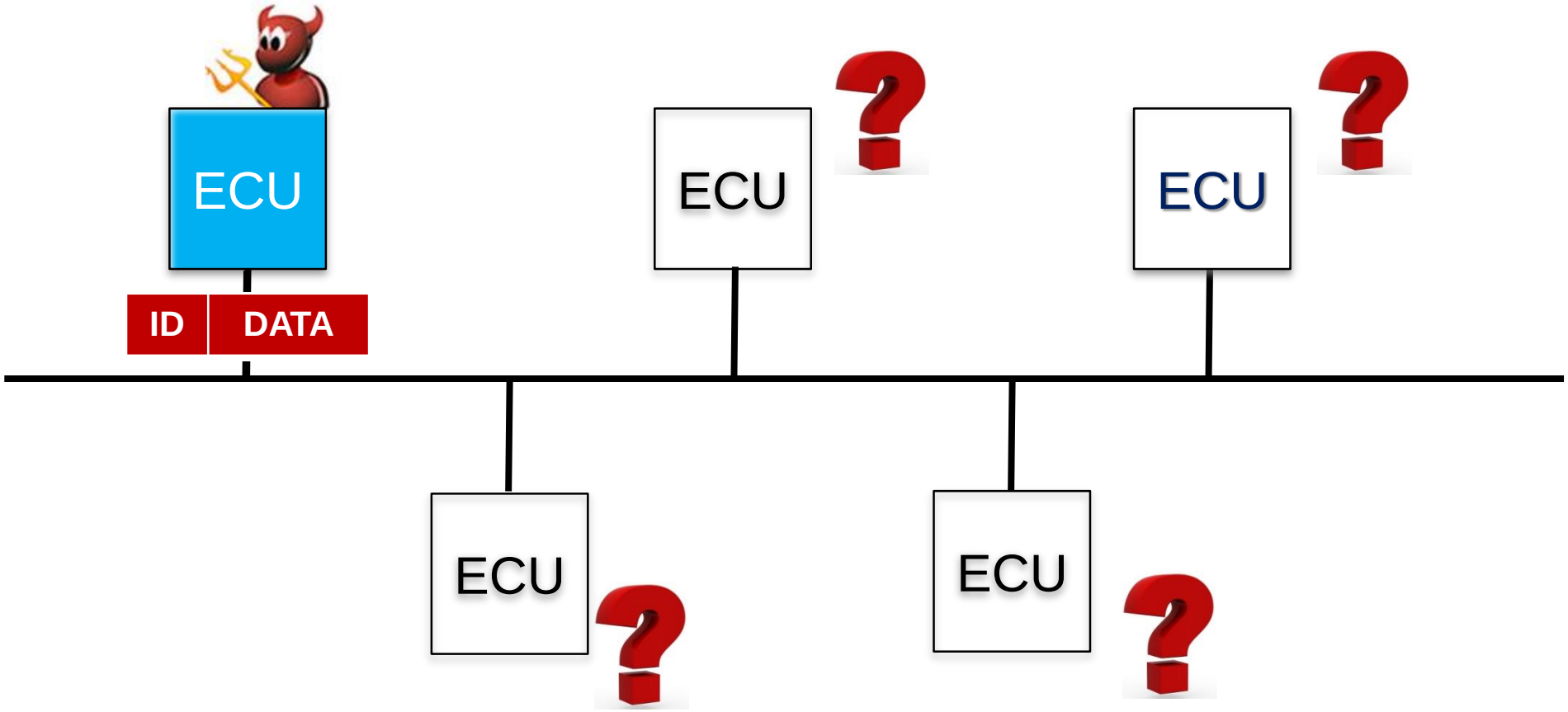
Problems

1. ***No authenticity***: Which ECU sent the message?



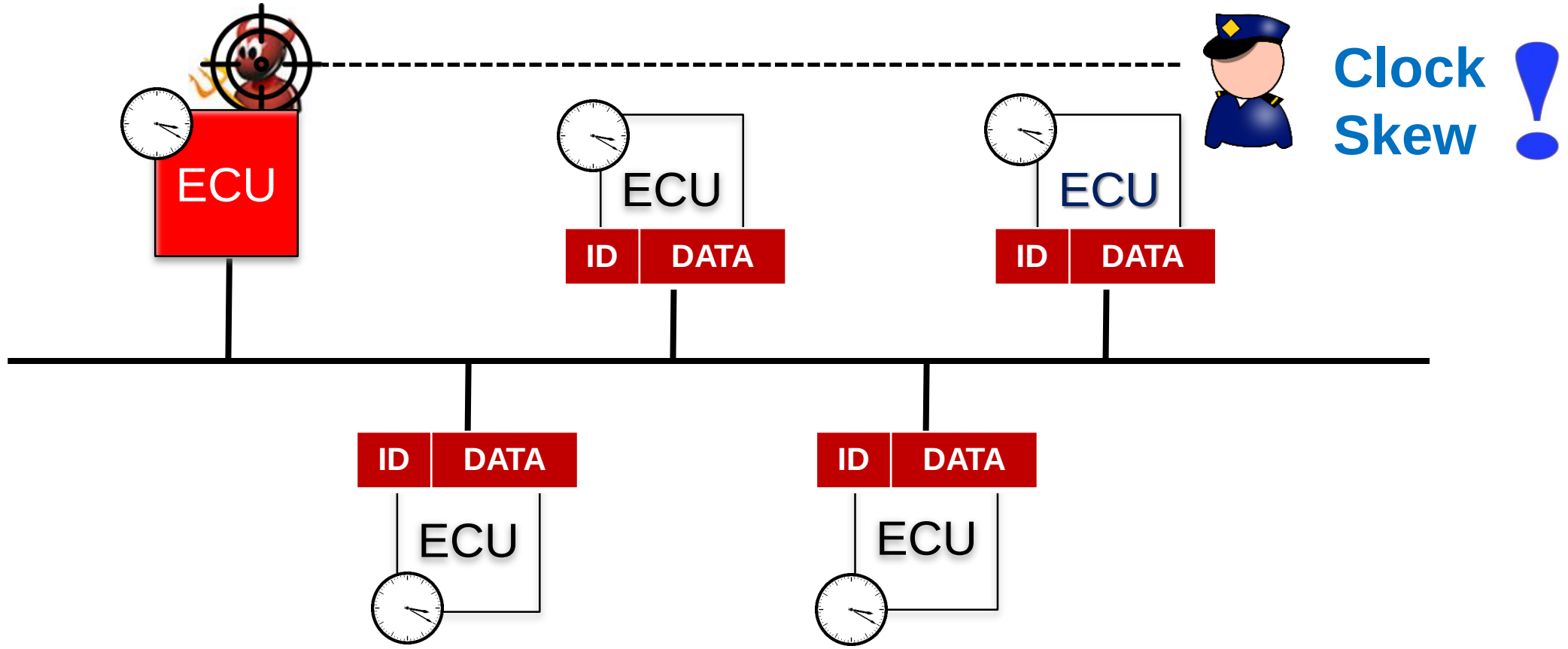
+ Problems

***2. Root-cause Analysis**: Who attacked?*

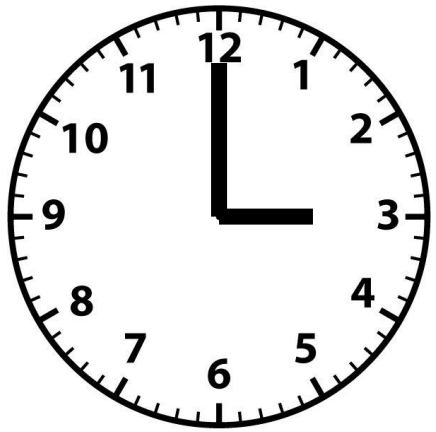


CIDS: Clock-based IDS

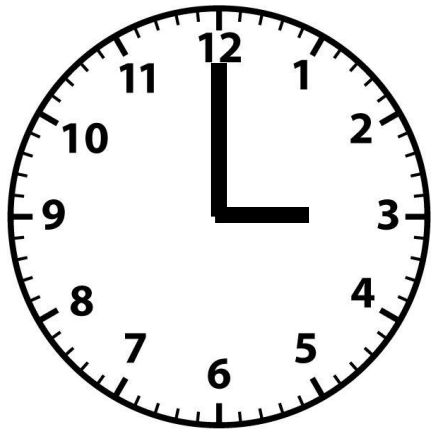
Objective: *Fingerprint ECUs for Intrusion Detection*



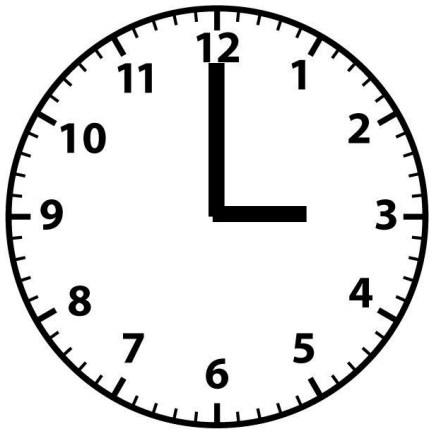
CIDS: Clock-based IDS



3:59 PM



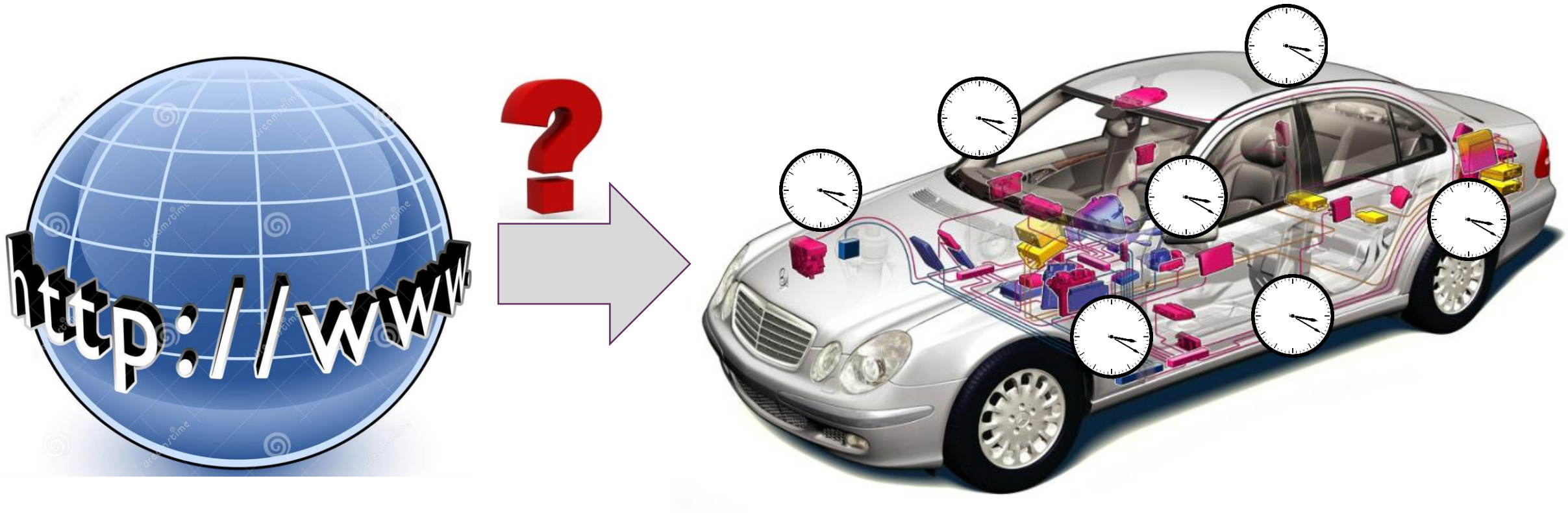
4:01 PM



4:00 PM

	Node 1	Node 2	Node 3
Clock Offset	-1 min	+1 min	0 min
Clock Skew	-1/60	+1/60	0

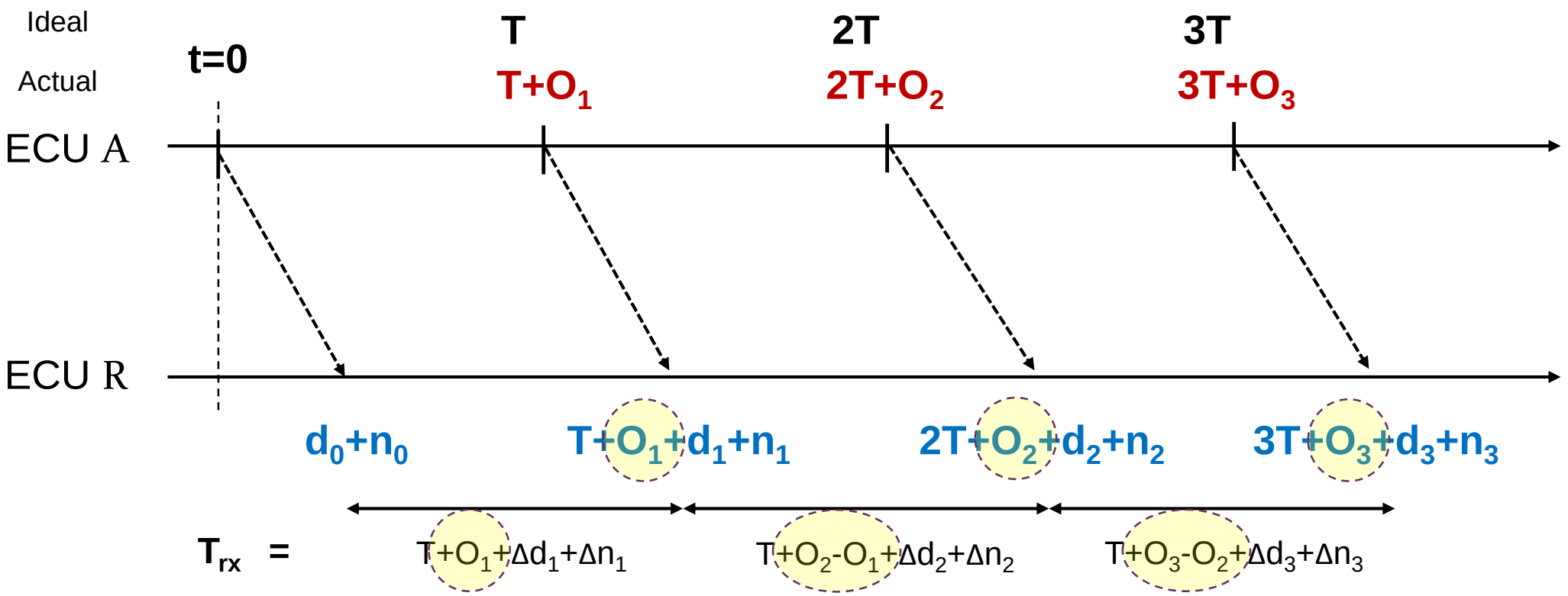
+ CIDS: Clock-based IDS



Determine ECUs' "**Clock Skew**" !

How? Exploit the fact that most messages are "**Periodic**"

CIDS: Clock-based IDS

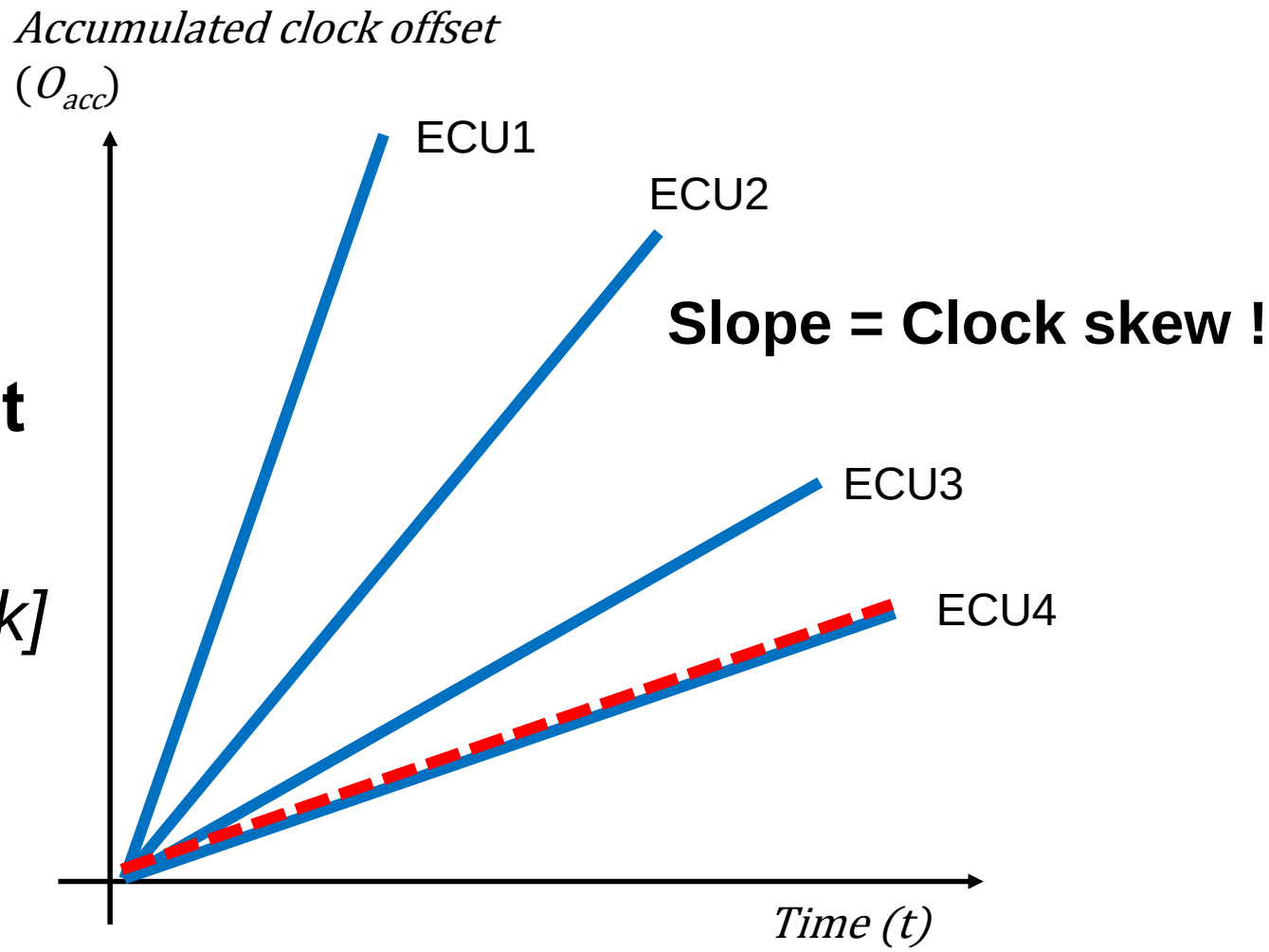


Transmitter's clock information is hidden in the message arrival timestamps and intervals!

CIDS: Clock-based IDS

“Recursive Least Square (RLS)”

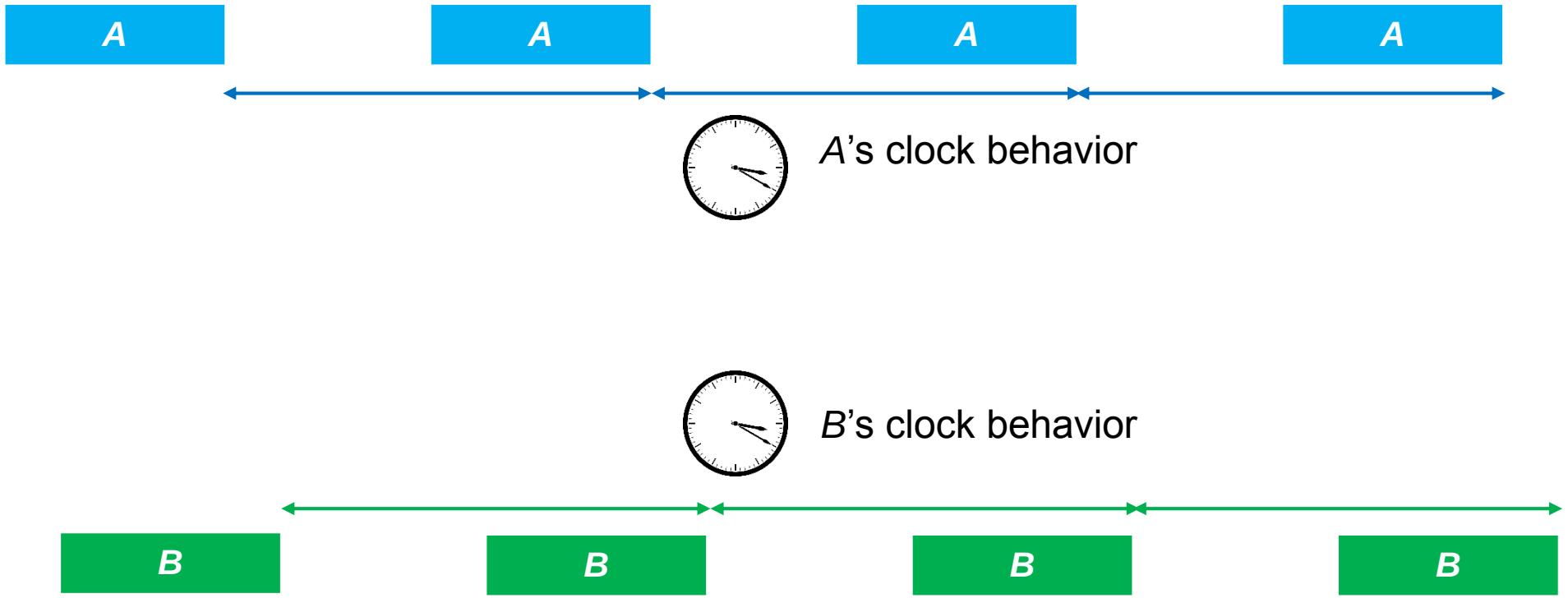
$O_{acc}[k] = S[k]t[k]+e[k]$



CIDS: Clock-based IDS

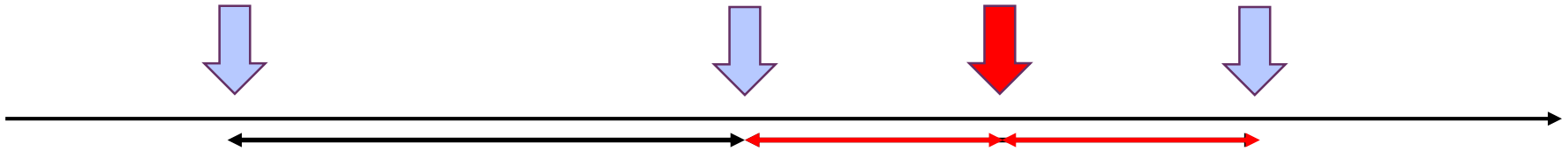
1. Per-message

2. Message-pairwise



CIDS: Per-message Detection

- Detection – Fabrication Attack

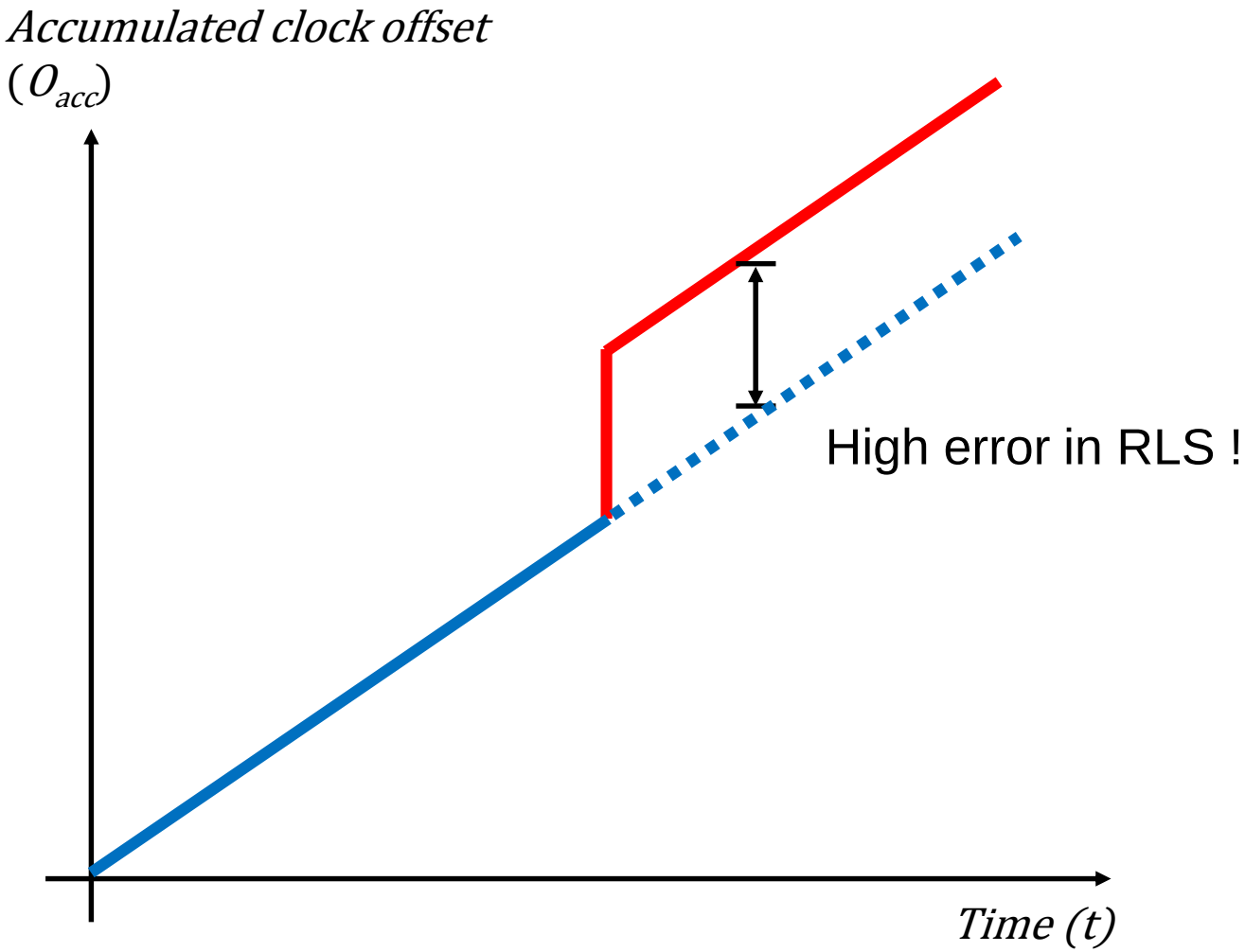


			1.5T+O_2+d_2+n_2	**2T**+O_3+d_3+n_3
Measured	d_0+n_0	$T+O_1+d_1+n_1$	$2T+O_2+d_2+n_2$	$3T+O_3+d_3+n_3$
Estimated		$E[T_{rx}]+d_0+n_0$	$2E[T_{rx}]+d_0+n_0$	$3E[T_{rx}]+d_0+n_0$
Difference	≈	**O_1+Δd+Δn**	**O_2+Δd+Δn**	**O_3+Δd+Δn**
			-0.5T+O_2+Δd+Δn	**-T+O_3+Δd+Δn**

|E[O_i]| Increases!

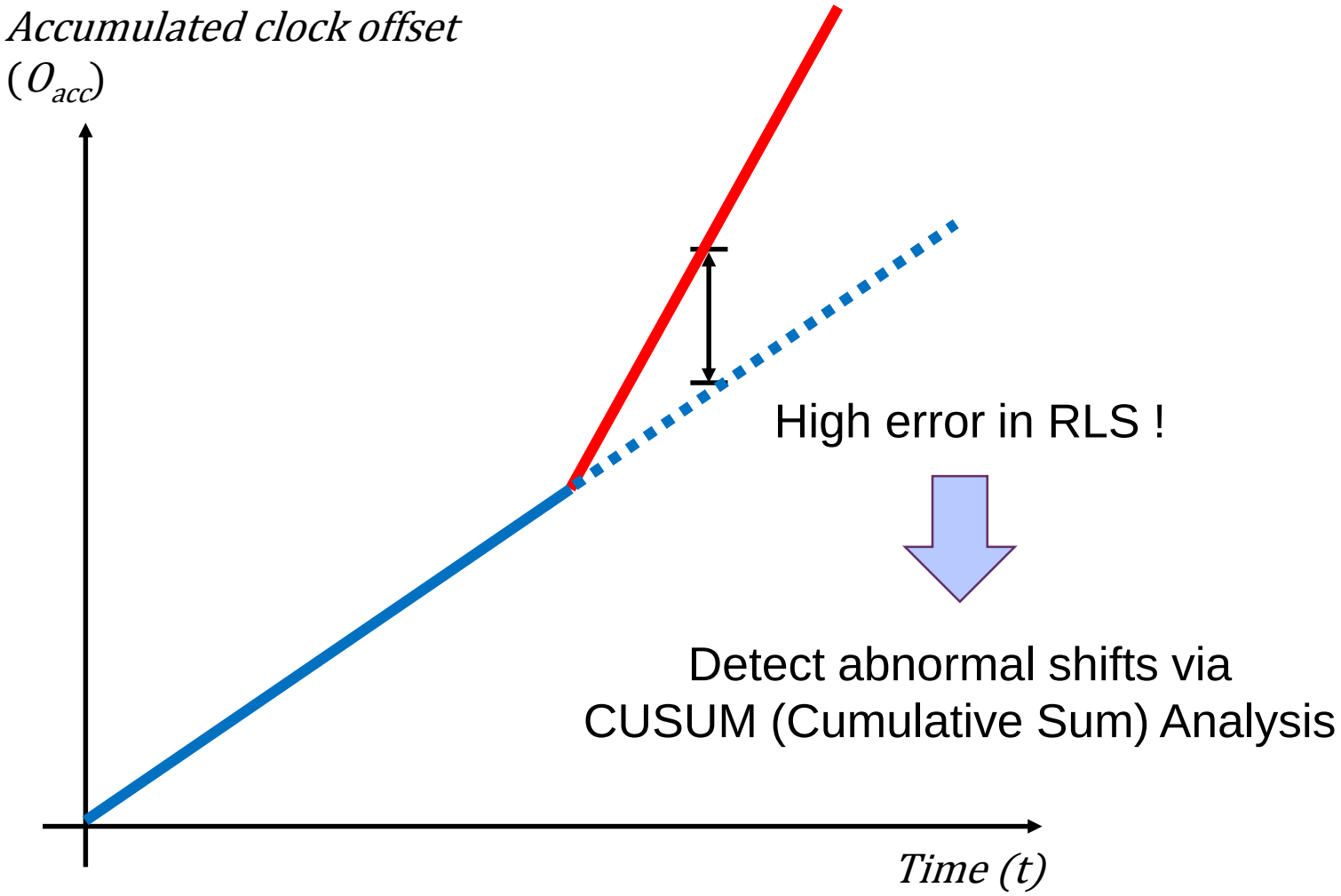
CIDS: Per-message Detection

- Detection: Fabrication Attack



CIDS: Per-message Detection

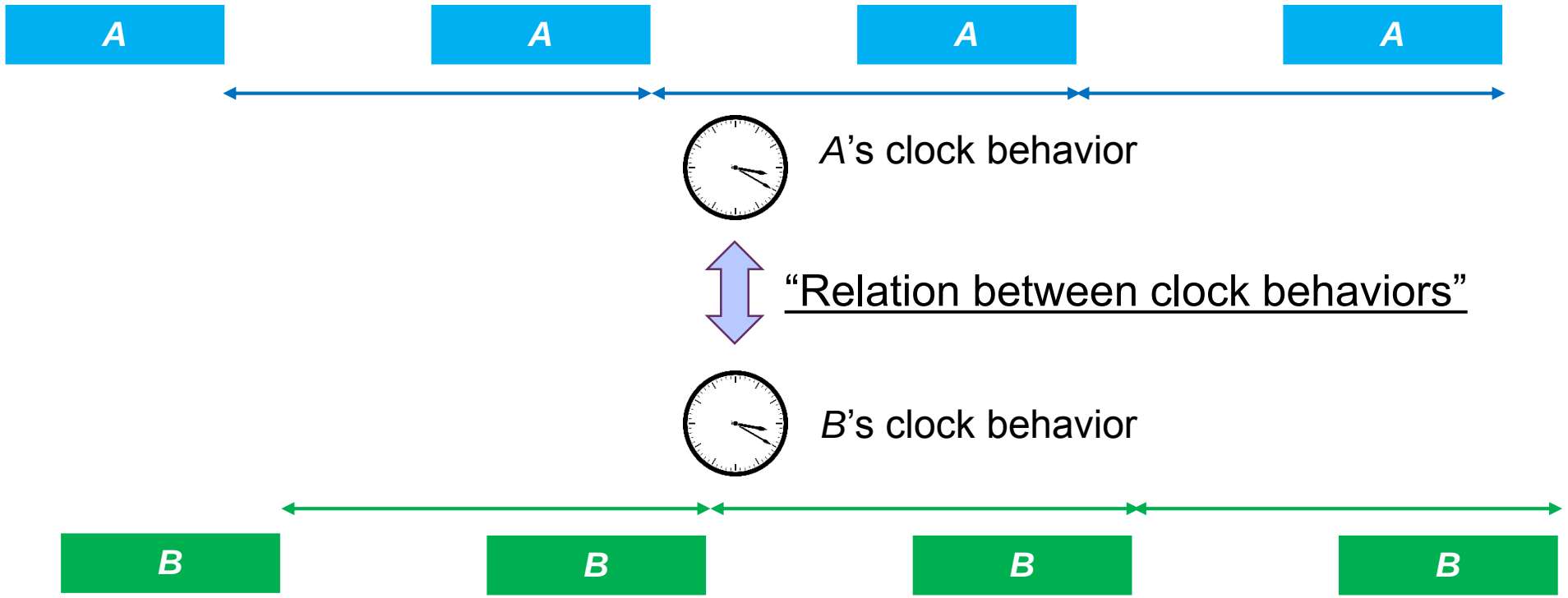
- Detection: Masquerade Attack



+ CIDS: Clock-based IDS

1. Per-message

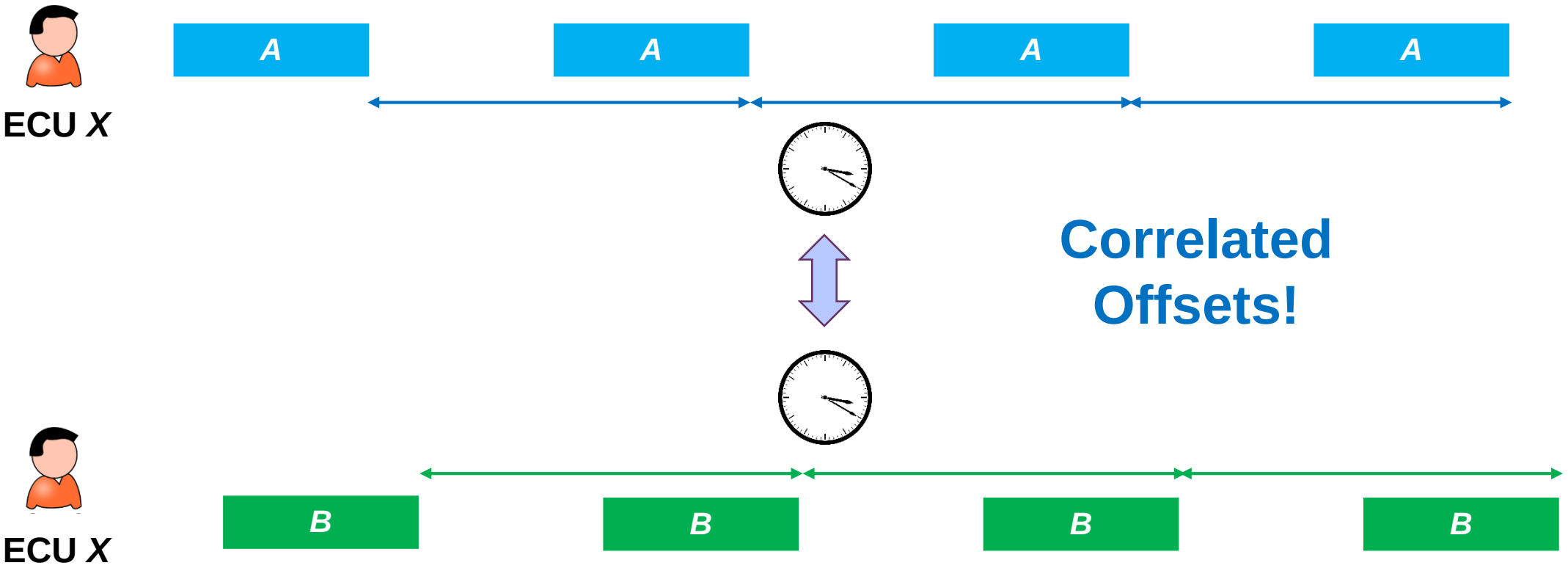
2. Message-pairwise



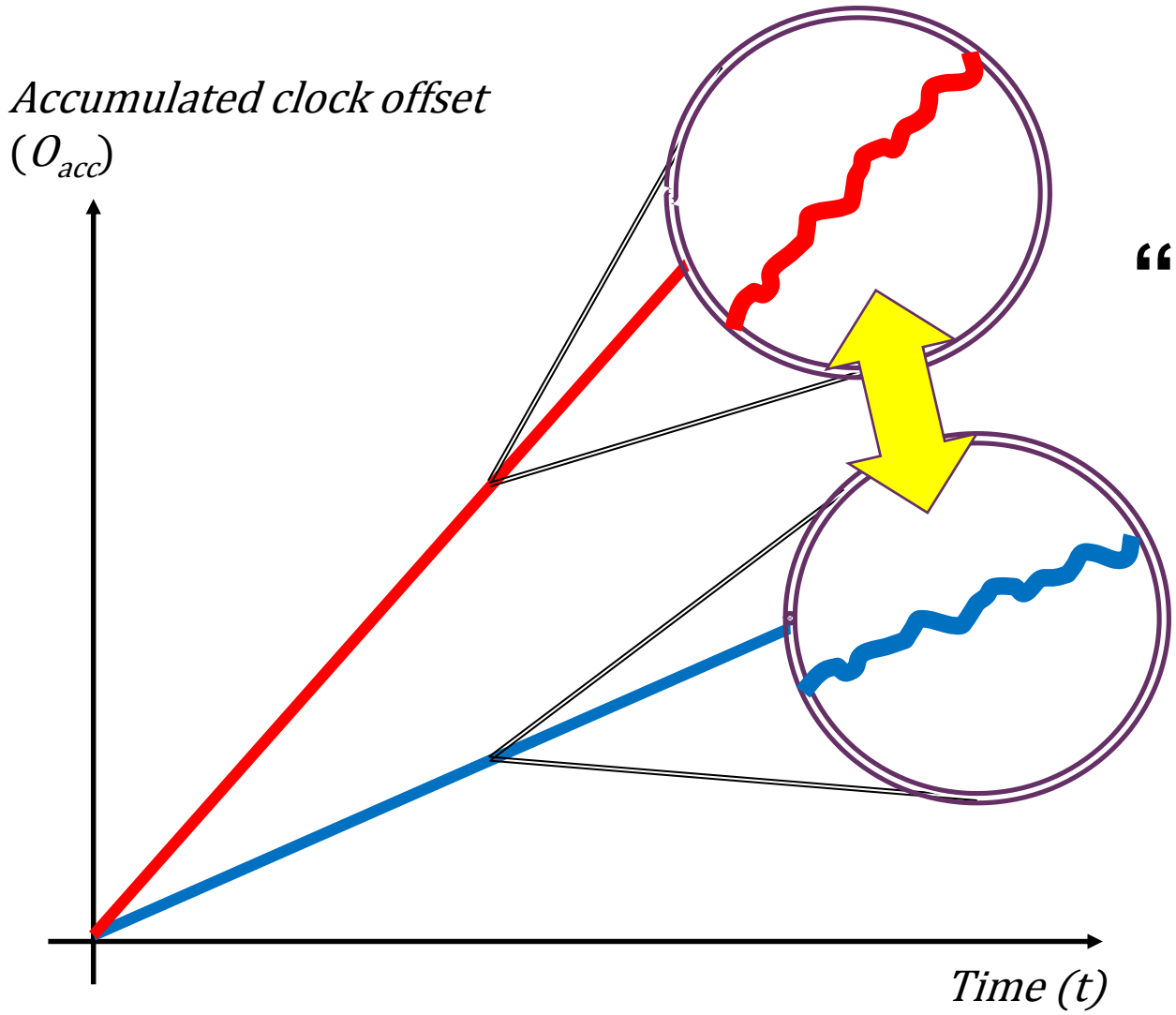
CIDS: Clock-based IDS

1. Per-message

2. Message-pairwise



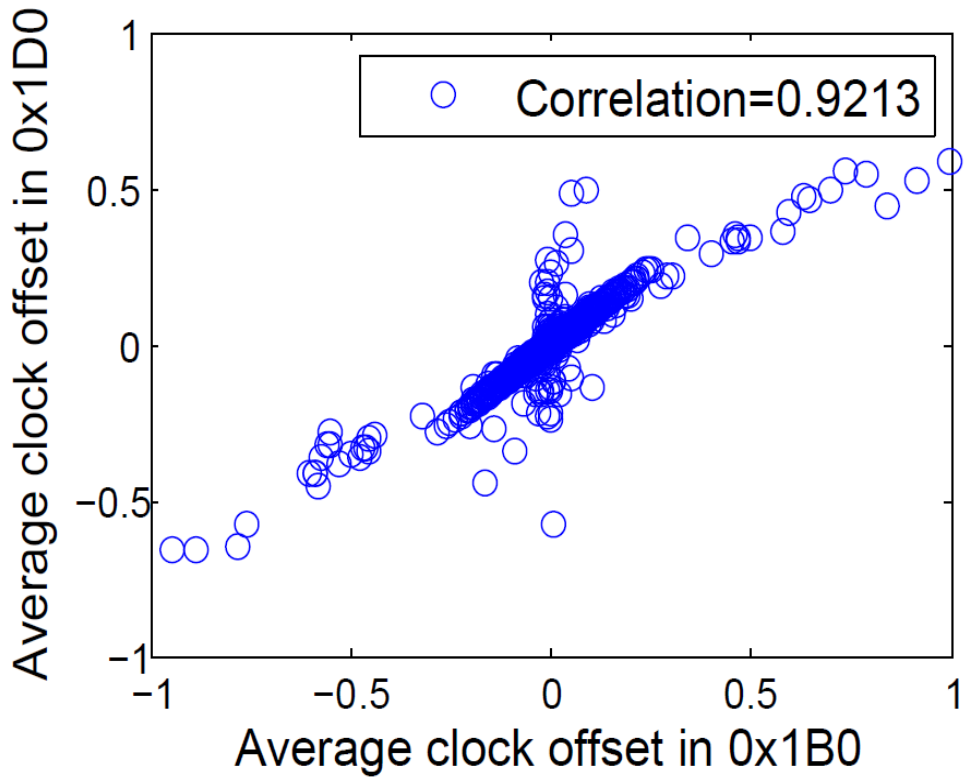
+ CIDS: Message-pairwise Detection



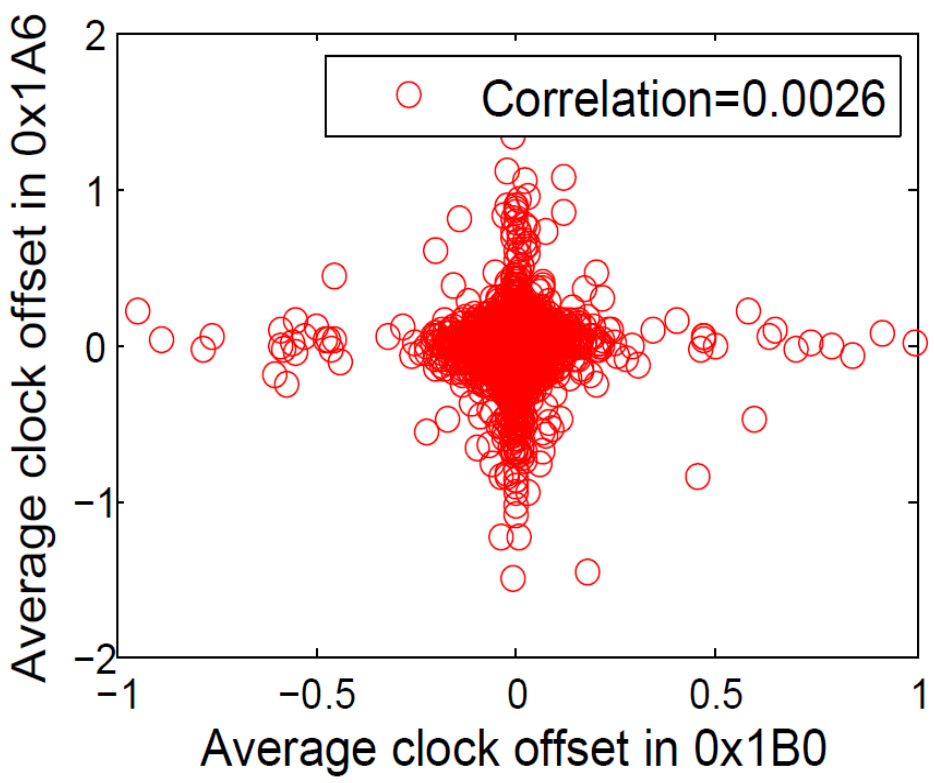
“Message-pairwise Detection”

CIDS: Message-pairwise Detection

- 2013 Honda Accord



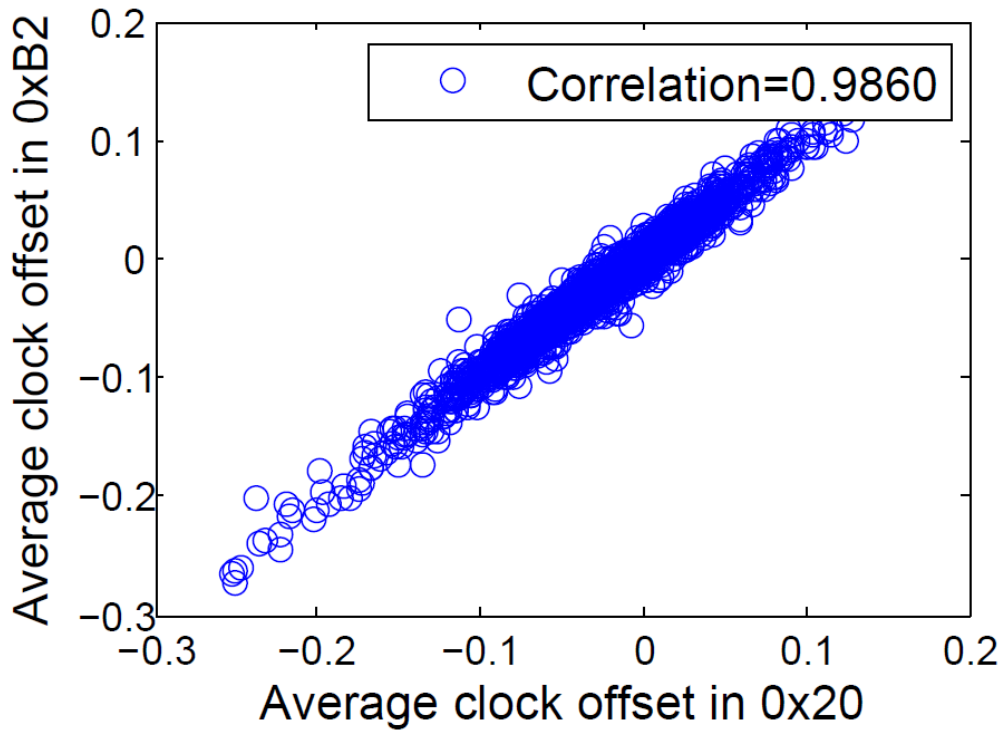
Same Txer



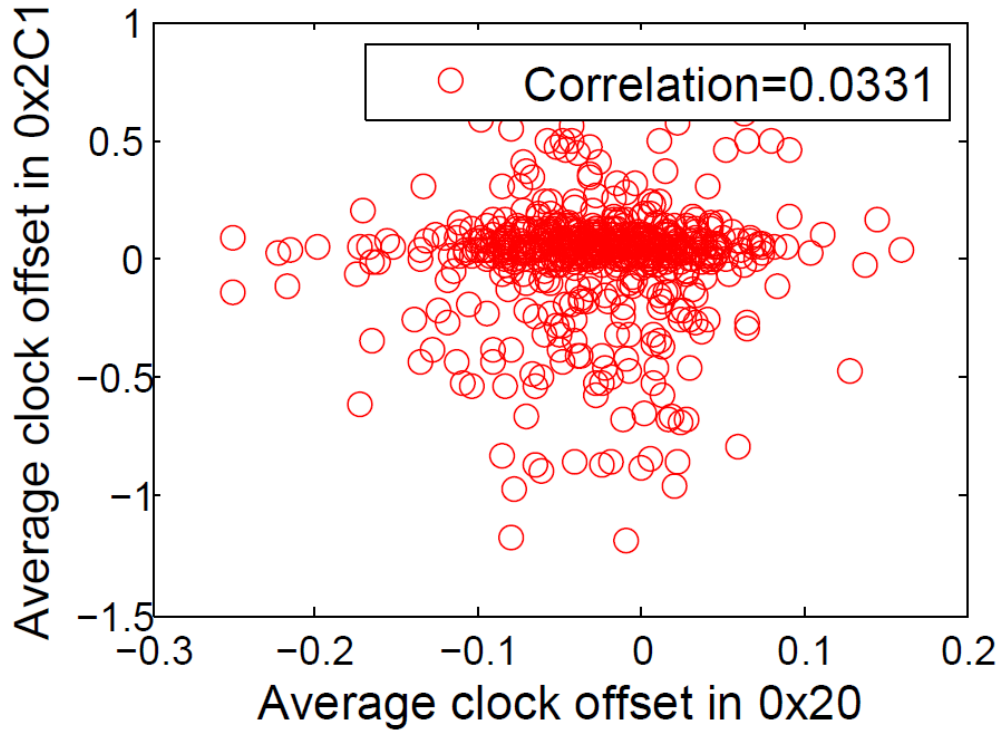
Different Txer

CIDS: Message-pairwise Detection

- 2010 Toyota Camry



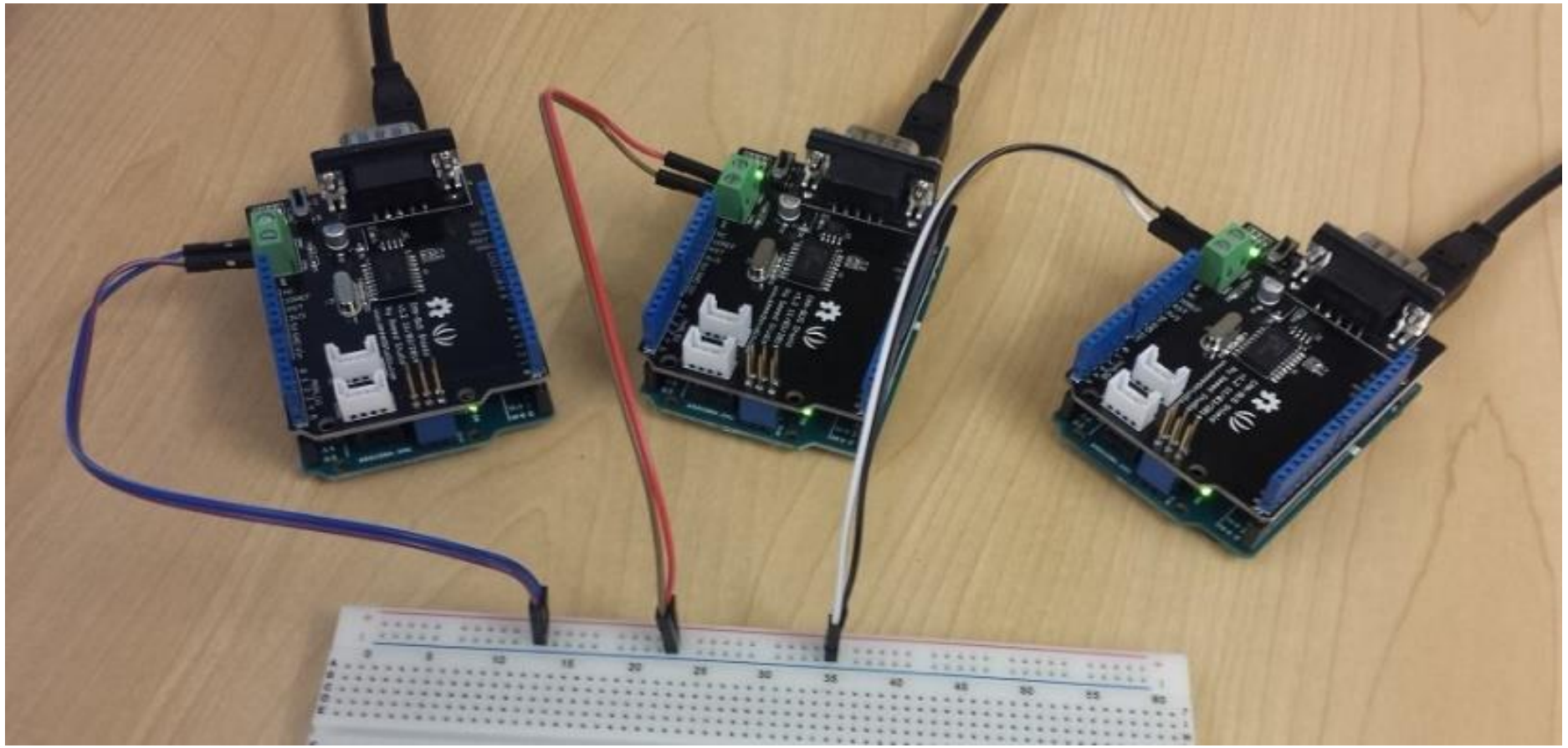
Same Txer



Different Txer

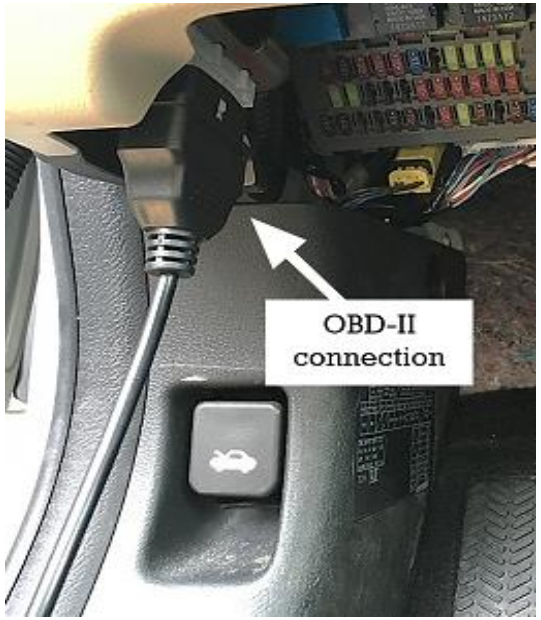
Evaluation

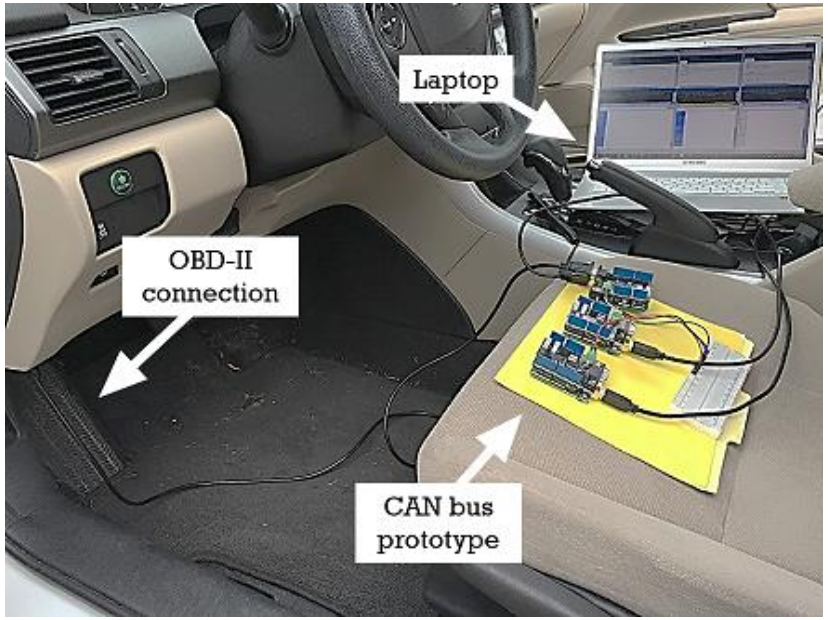
- Setting 1: CAN bus prototype



Evaluation

- Setting 2: Real Vehicle – 2013 Honda Accord

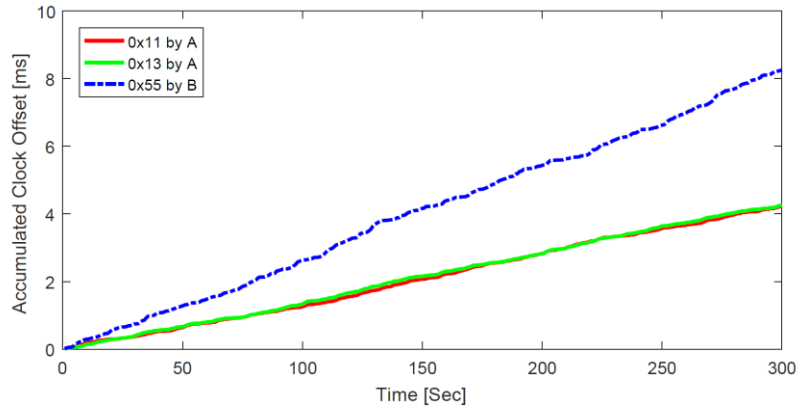




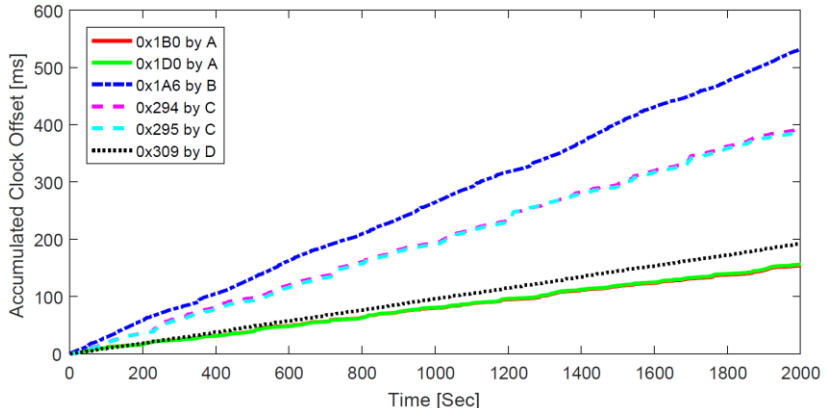
- Setting 3: CAN log data
  - 2010 Toyota Camry
  - 2010 Dodge Ram Pickup

Evaluation

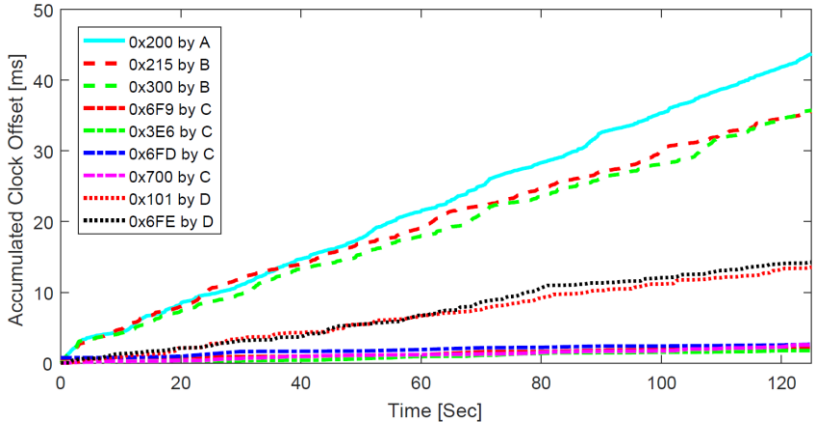
- Different Fingerprints



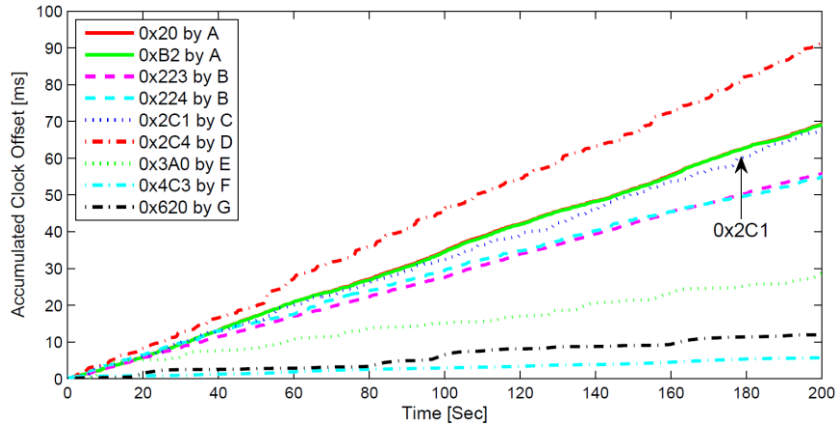
CAN bus prototype



2013 Honda Accord



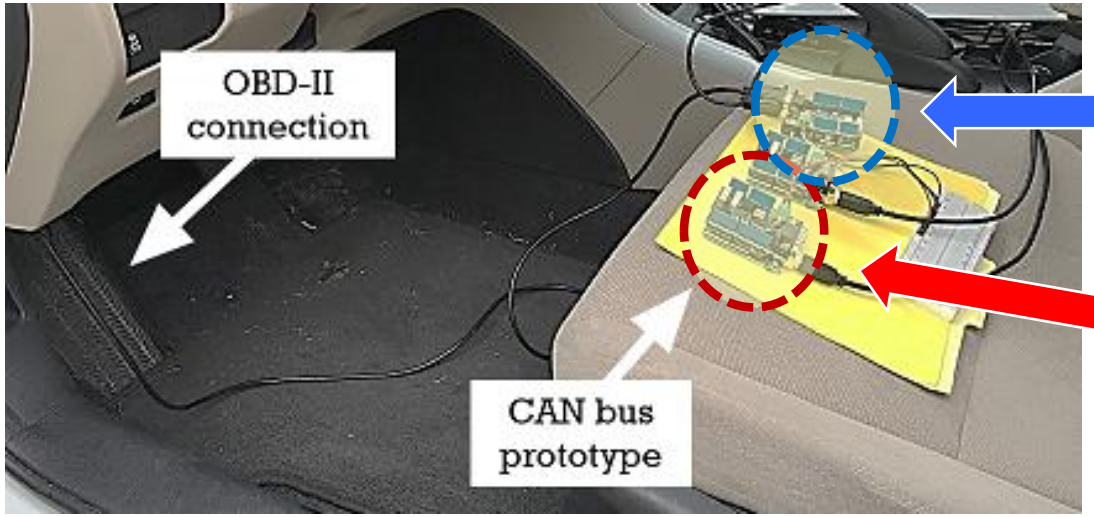
2010 Dodge Ram Pickup



2010 Toyota Camry

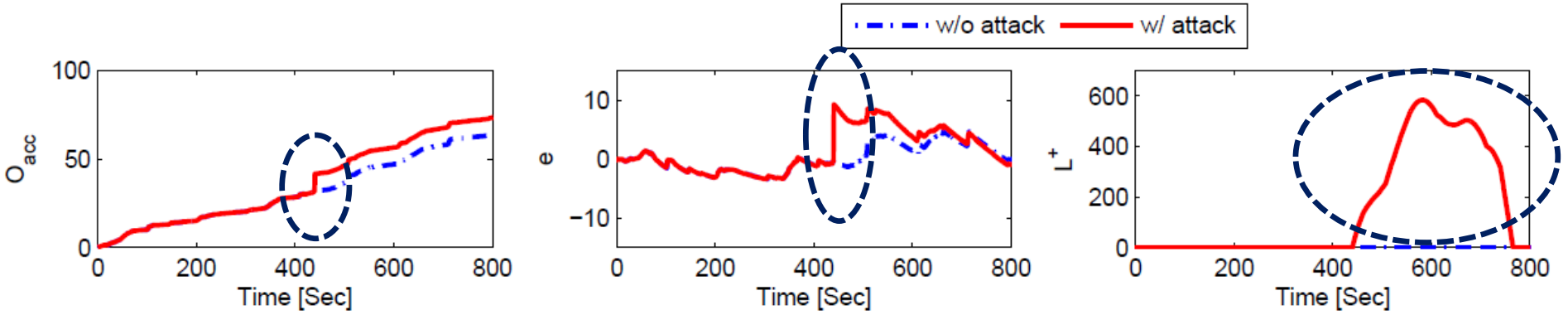
Evaluation

- Defending Fabrication Attack



CIDS

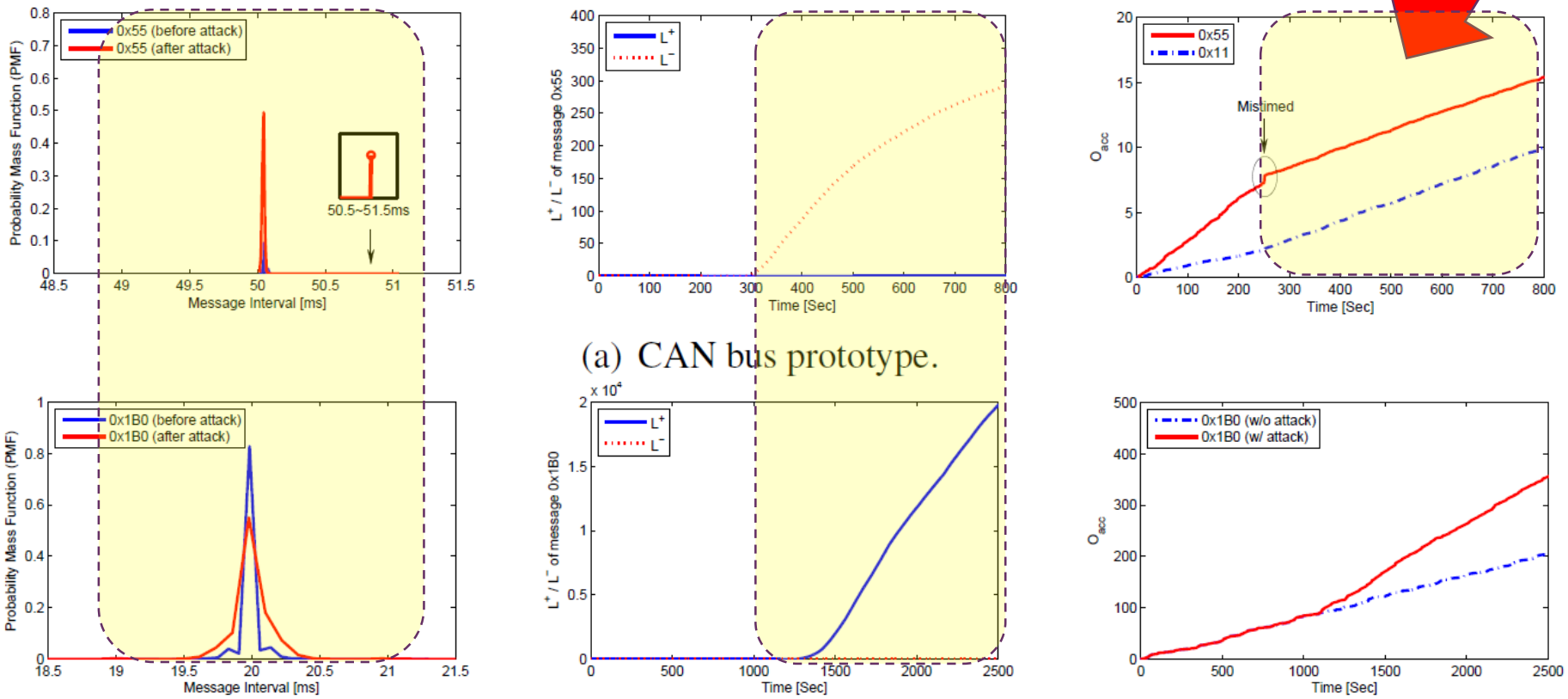
Attacker



Evaluation

- Defending Masquerade Attack

"Root-cause Analysis"



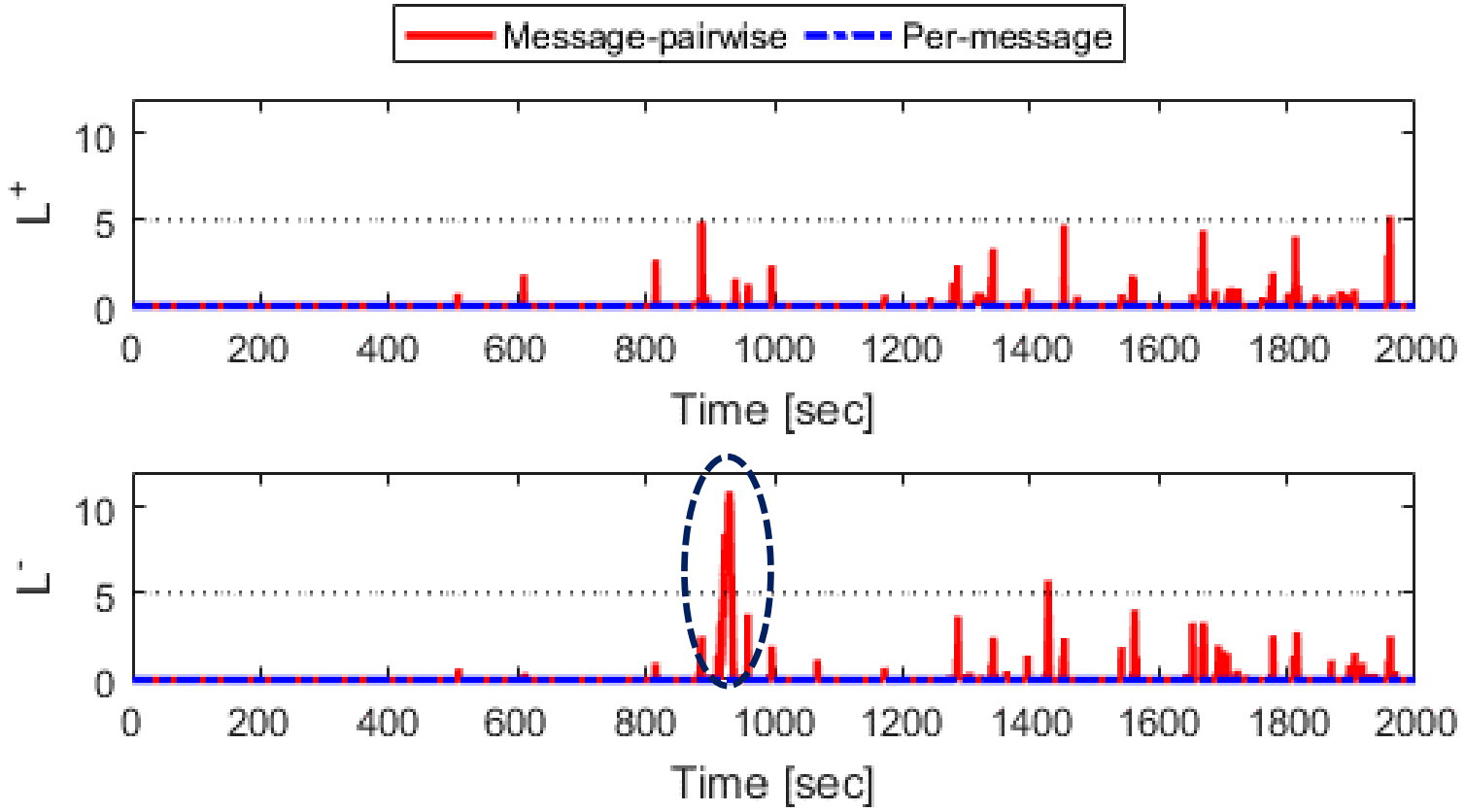
(a) CAN bus prototype.

(b) Real vehicle.

Evaluation

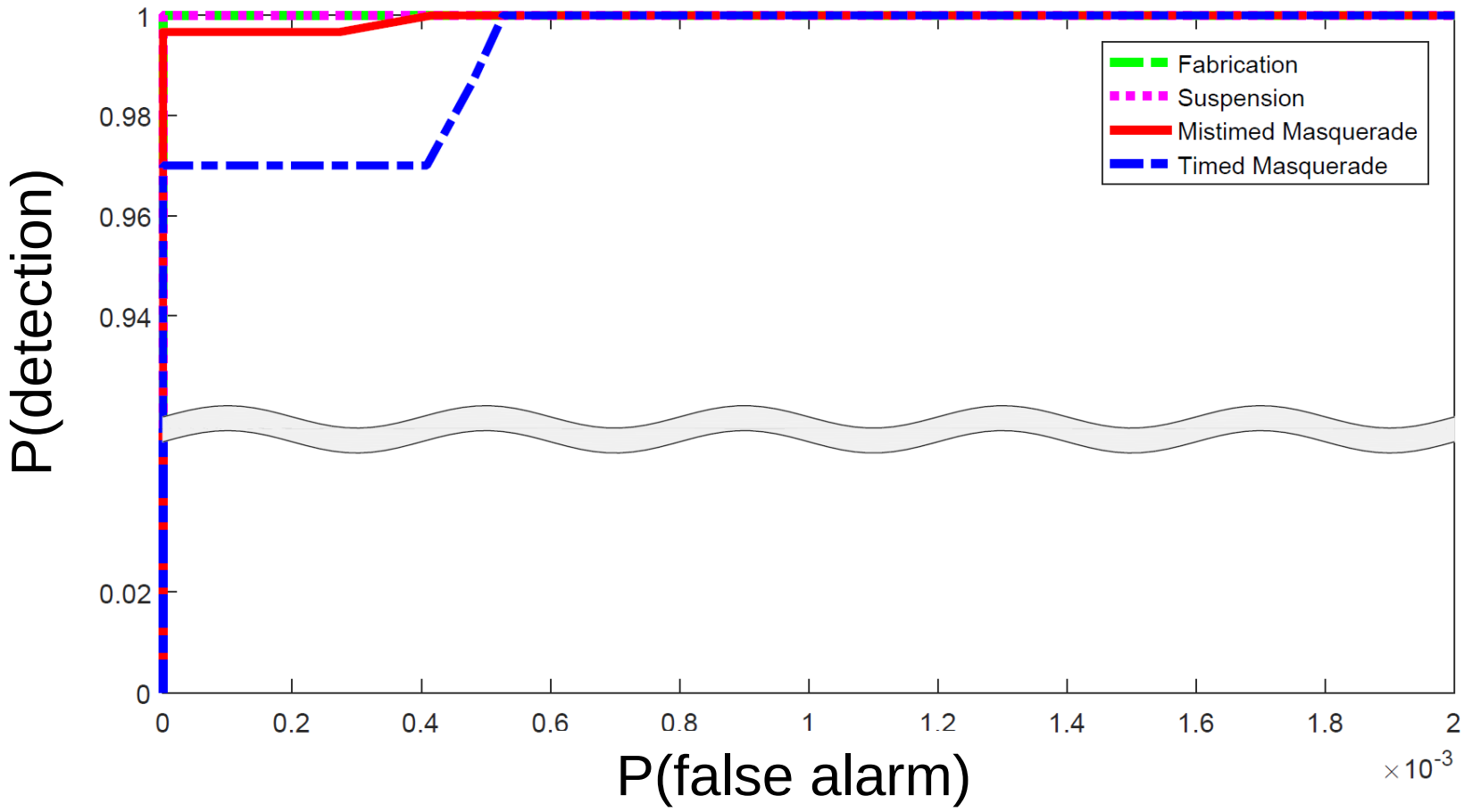
- Message-pairwise Detection

What if impersonating node has near-equivalent “clock skew”?



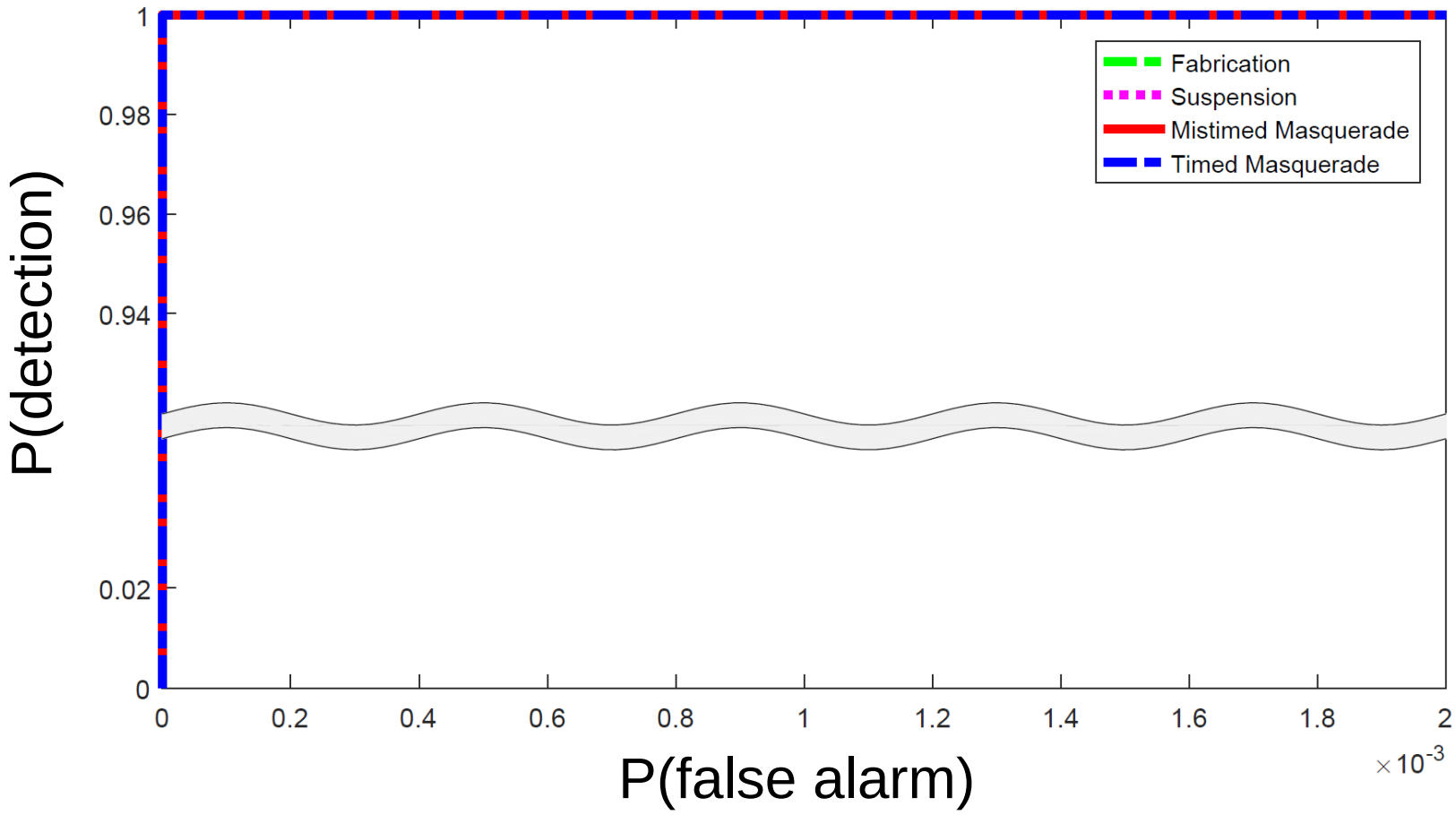
Evaluation

- False Alarm Rate : Per-message



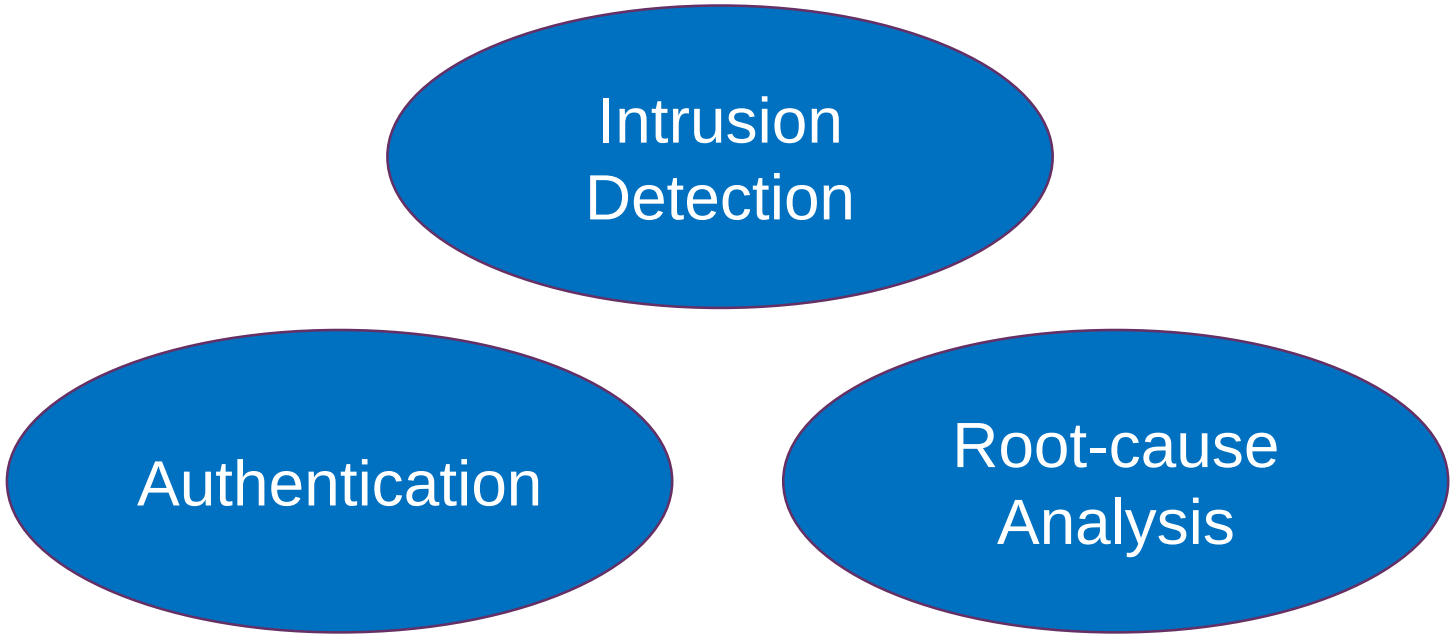
Evaluation

- False Alarm Rate : Per-message + Message-pairwise



Conclusion

- CIDS: Clock-based IDS
  - ✓ Fingerprints transmitters based on extracted clock skew
  - ✓ Overcomes the limitations of state-of-the-art defenses
  - ✓ No change in protocol/messages required!



Thank you!

ktcho@umich.edu