Counter Attacks for Bus-off Attacks

Daisuke Souma[1], Akira Mori[1], Hideki Yamamoto[2] and Yoichi Hata[2]

[1]National Institute of Advanced Industrial Science and Technology
[2]Sumitomo Electric Industries, Ltd.

STRIVE 2018

18 September 2018

Agenda

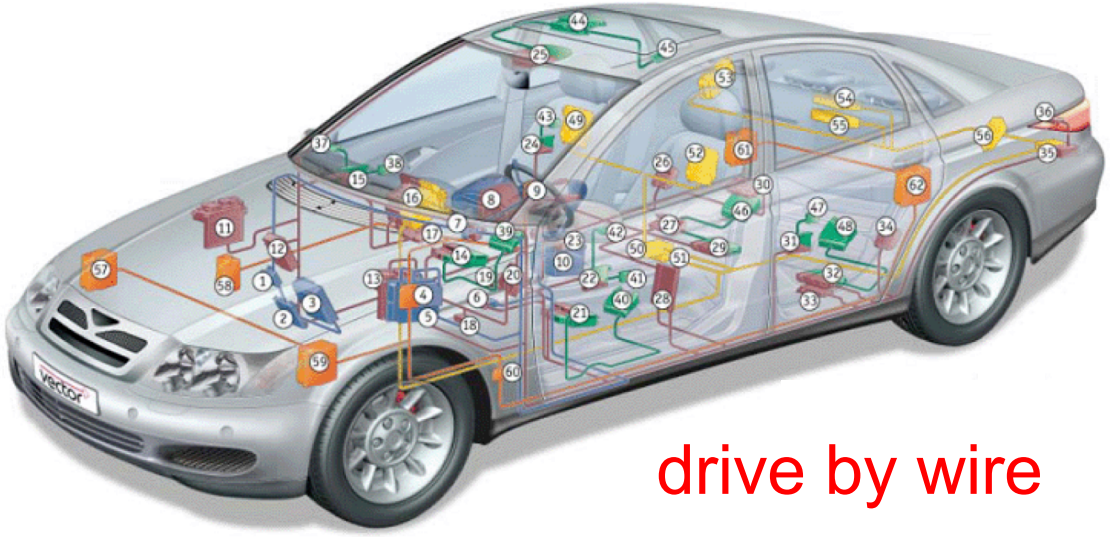
- Preliminaries
  - Controller Area Network (CAN)
  - Bus-off Attacks and Attack Model
- Countermeasure
  - Overview
  - Counterattack
  - Experiments
- Conclusion and Future Works

Preliminaries

CAN

- Designed by Bosch in 1980s.

- Multi-master serial bus standard.
- Maximum communication speed is 1Mbps.
- Messages are broadcasted.
  - No sender information
  - Message ID is used for acceptance filtering and arbitration



Physical signal transmission

- Use voltage differential between two wires as physical signal transmission.
  - 2V：dominant（0）
  - 0V：recessive（1）
  - Increase noise immunity, but exist asymmetry of state of bus.
  - Dominant (0) overwrites Recessive (1).

Node A	0	1	0	0	0	1	1	1
Node B	0	0	0	1	1	0	1	1
Node C	0	0	1	0	1	1	0	1
CAN bus	0	0	0	0	0	0	0	1

The CAN bus level becomes 1 (recessive), if all nodes transmits 1.

CAN Error Handling

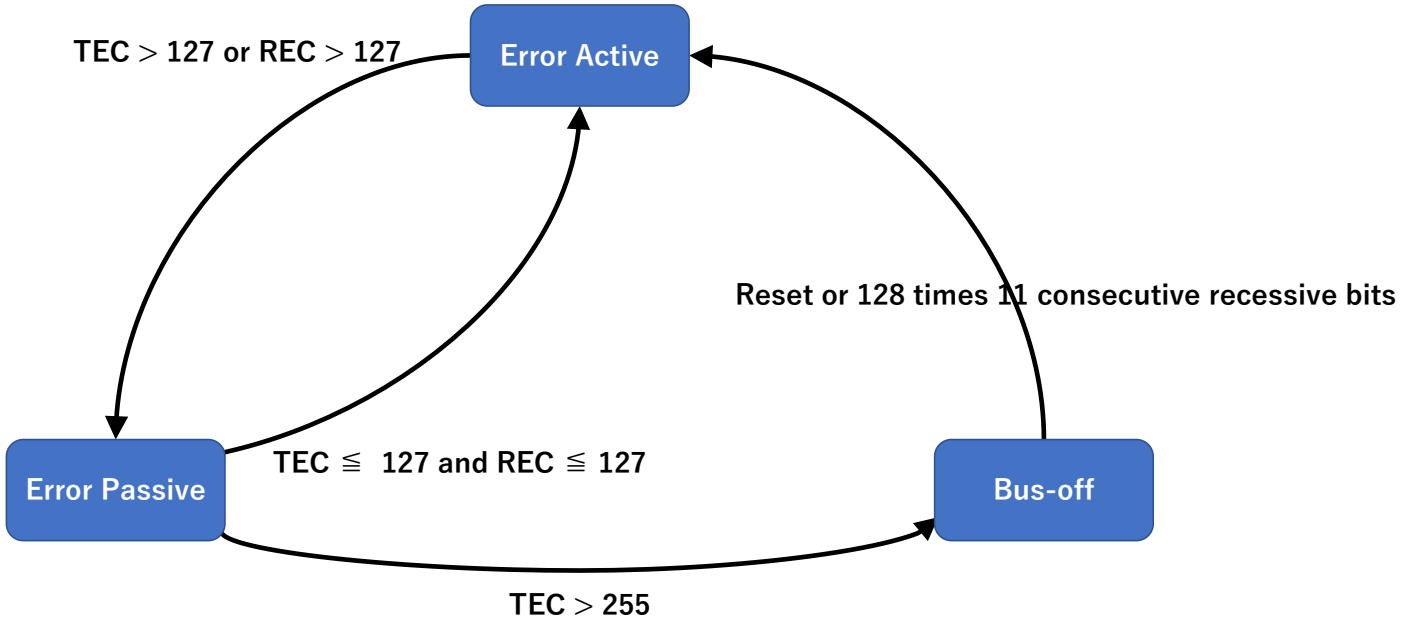
- Each node handles communication errors.
  - When an error is detected, the error frame is transmitted (to indicate occurrence of errors to all nodes).
  - After transmit the error frame, restart normal communication.

- To track error, every node has 2 counters.
  - TEC (Transmit Error Counter)
  - REC (Receive Error Counter)
- TEC and REC increase/decrease according to predefined rules.
  - TEC
    - Increased by 8 when a transmitting node cause an error.
    - Decreased by 1 when a message is successfully transmitted.
  - REC
    - Increased by 1 when transmits a secondary error flag.
    - Increased by 8 when detects a receive error.
    - Decreased by 1 when receives a message successfully.

In normal node, error flag is consisted of 6 dominant bits.

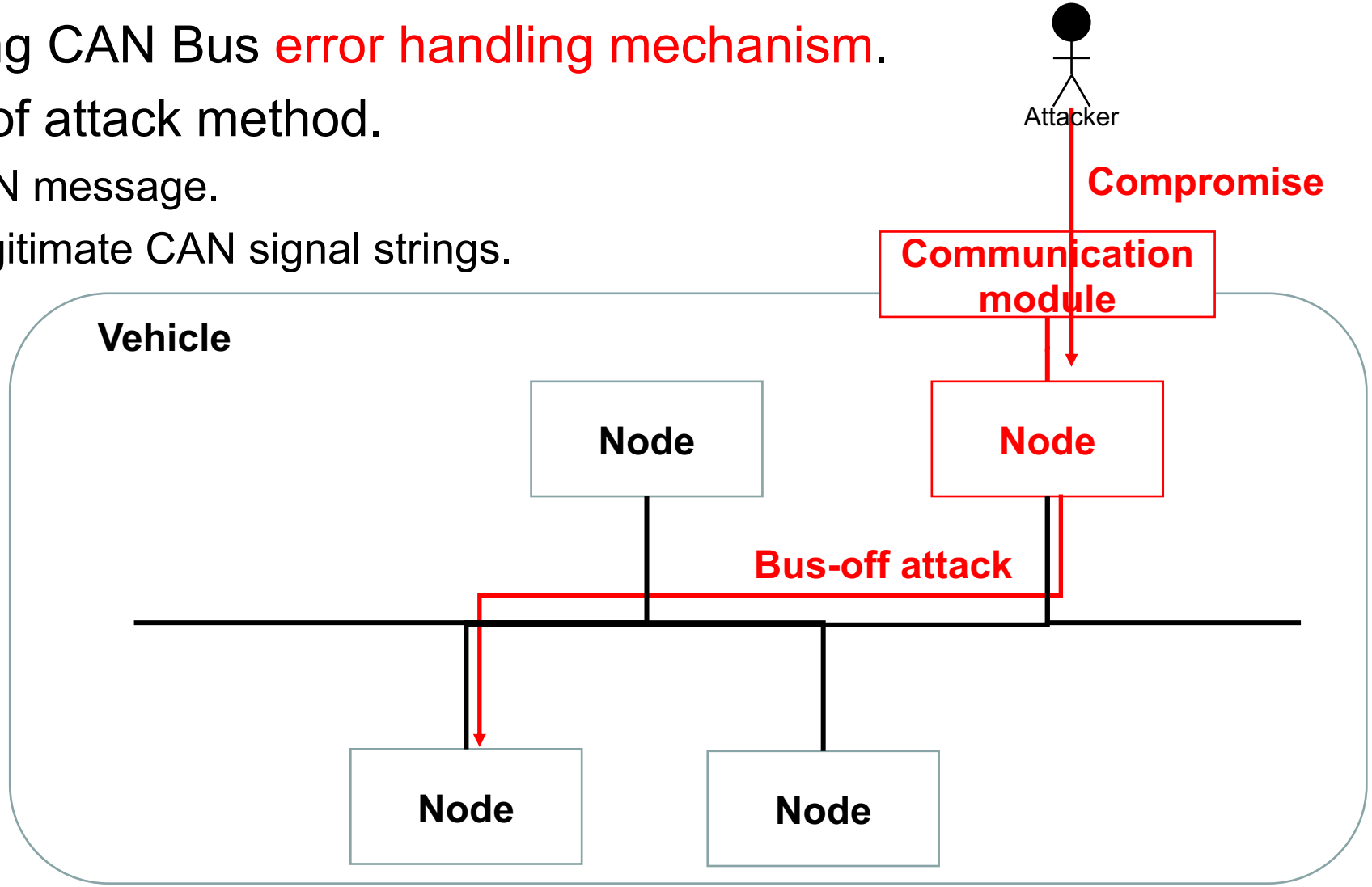
CAN Error Handling

- Error active state.
  - Normal state.
- Error passive state.
  - Waits for 8 bits (called a passive IFS) before transmitting another message when transmitting two consecutive messages.
  - The error flag changes to 6 consecutive recessive bits (called passive error flag).
- Bus off state.
  - Virtually detached from the bus.
  - Can not transmit a message.



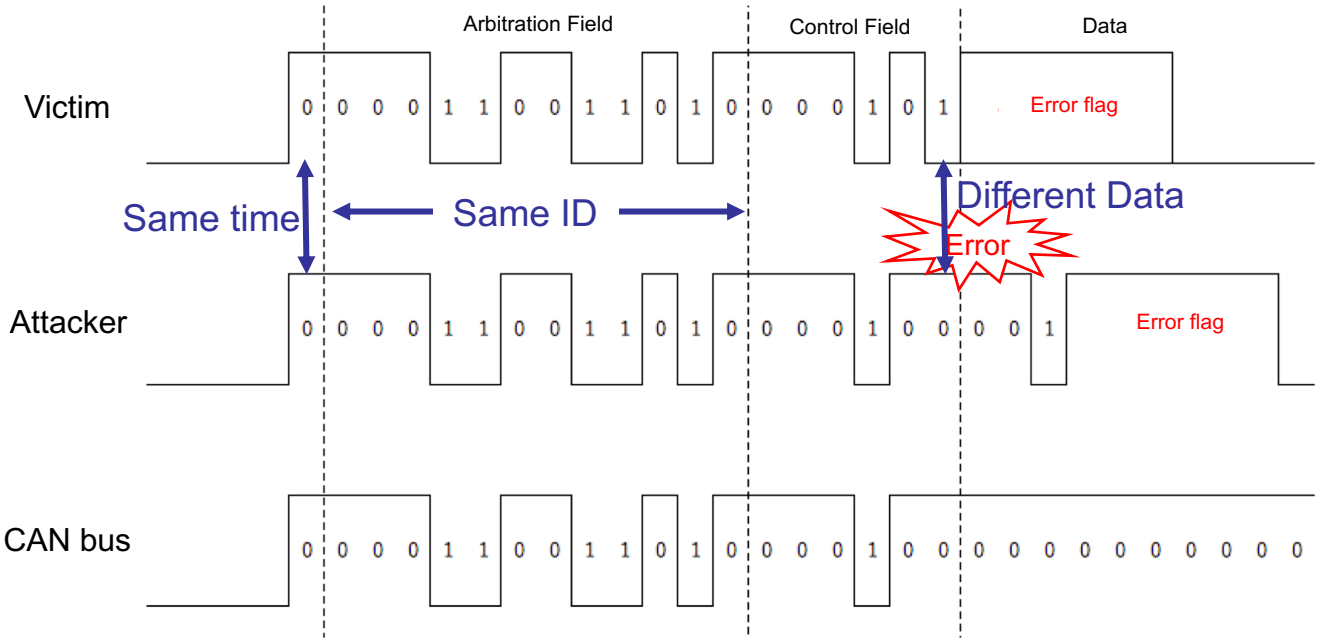
Bus-off Attacks and Attack Model

- Impeding availability of target (victim) node (DoS attack).
- By exploiting CAN Bus error handling mechanism.
- Two types of attack method.
  - Using CAN message.
  - Using illegitimate CAN signal strings.



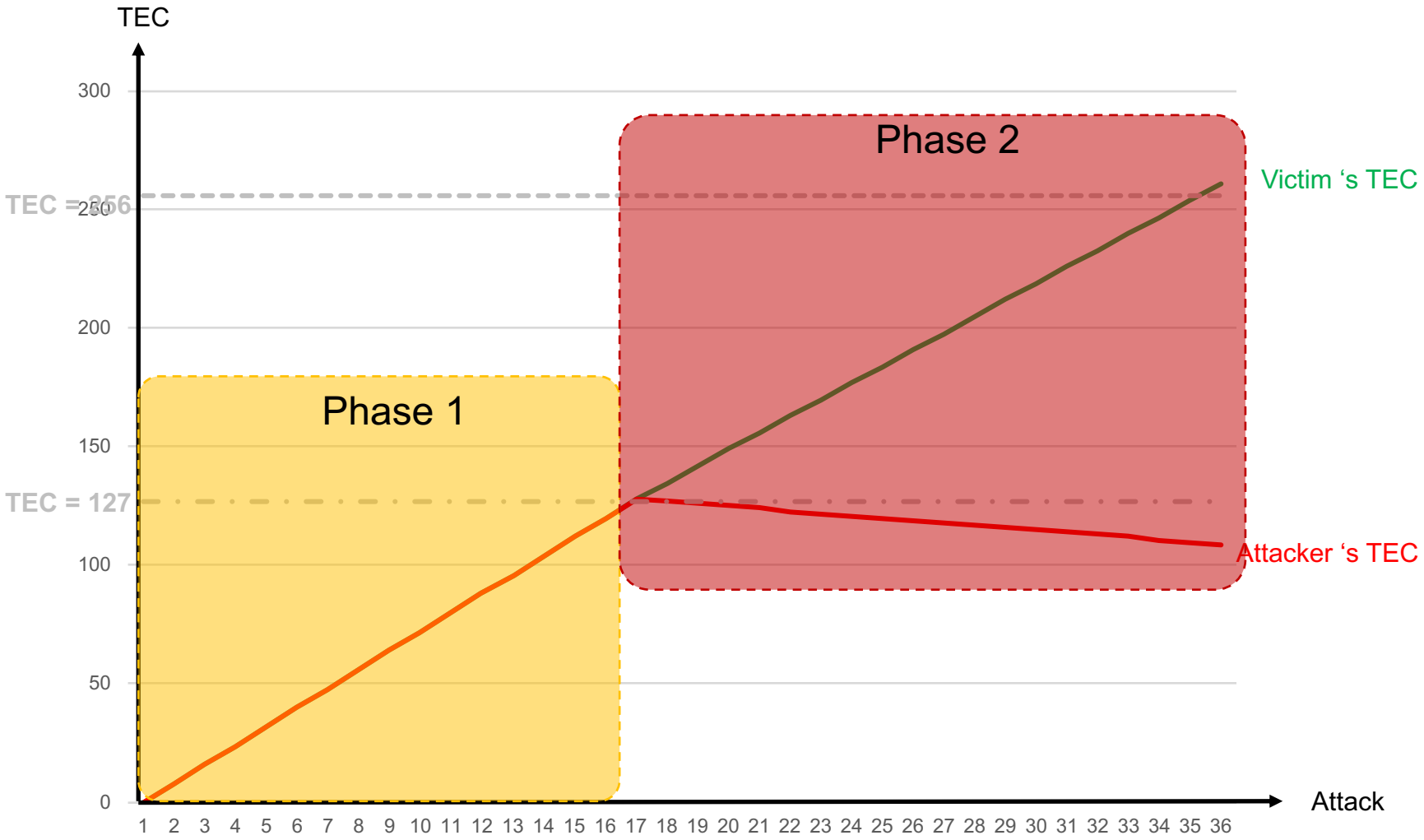
Bus-off Attacks (using CAN message)

- Causes an error by overwriting a victim's message repeatedly.
  - Adequate attack message
    - Same message ID
    - Data
  - Transmit timing
    - Same time as a victim's message strictly
- TECs of both nodes are increased.



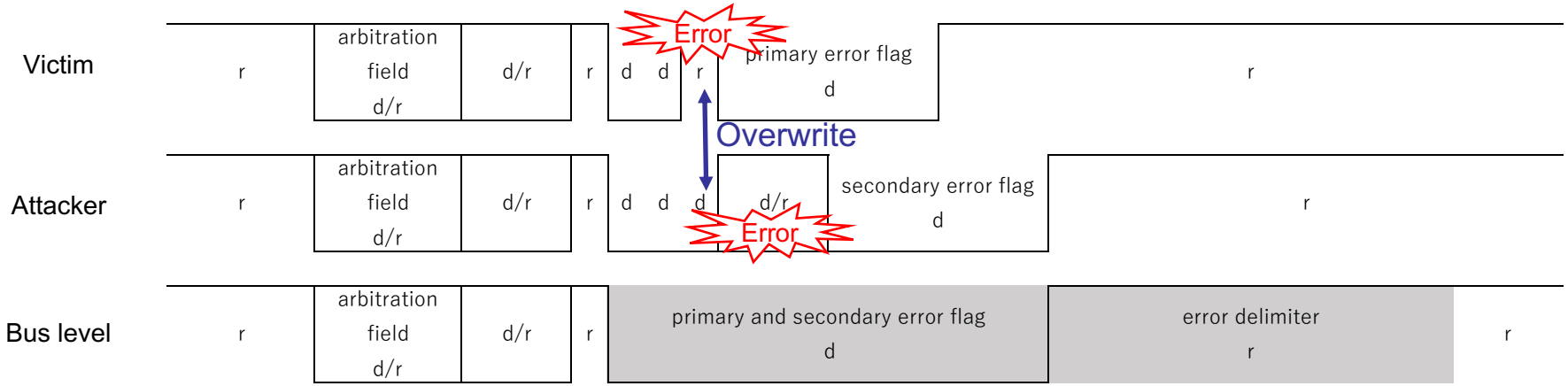
Bus-off Attacks (using CAN message)

- Increasing victim's TEC until it reaches the bus-off state.

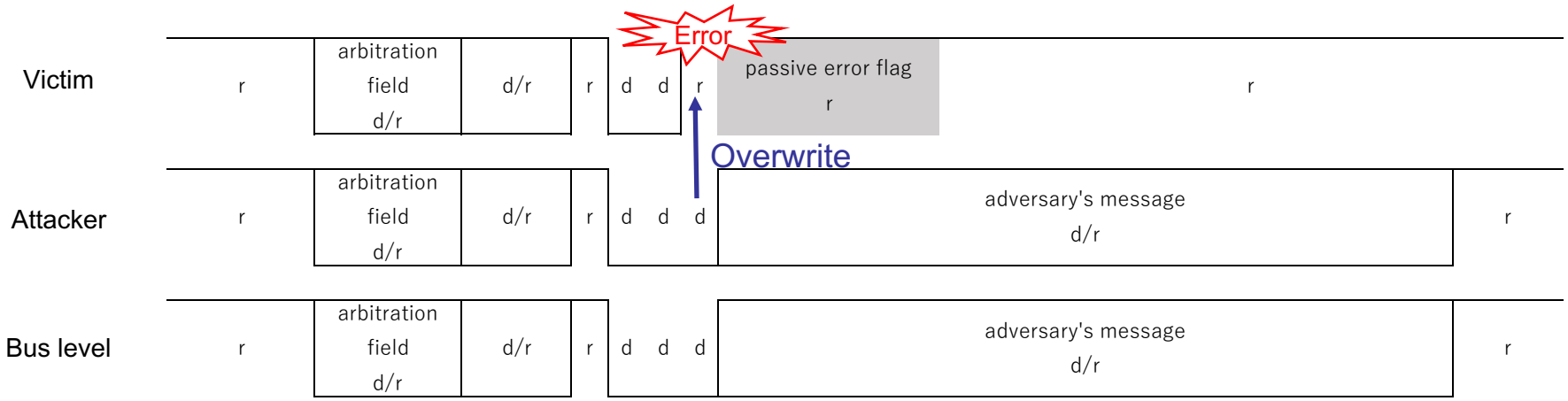


Bus-off Attacks (using CAN message)

- Phase 1 (both nodes are in the error active state): TECs of both nodes are increased.



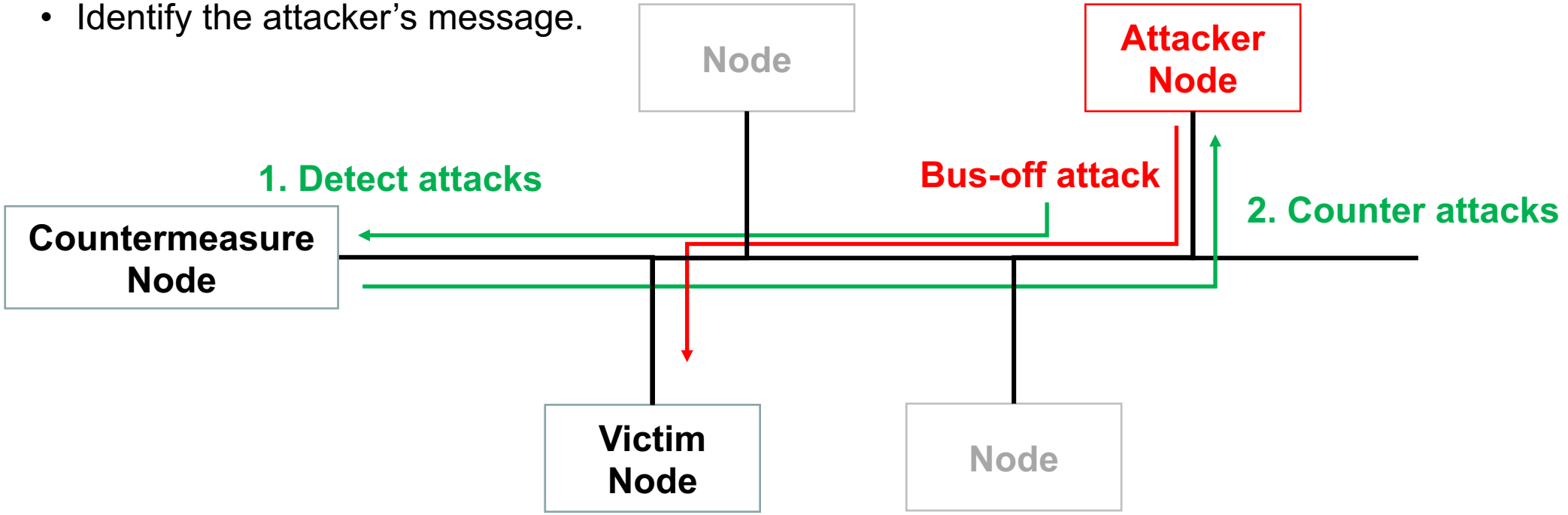
- Phase 2 (at least one node is in the error passive state): Only the victim's TEC is increased.



Countermeasure

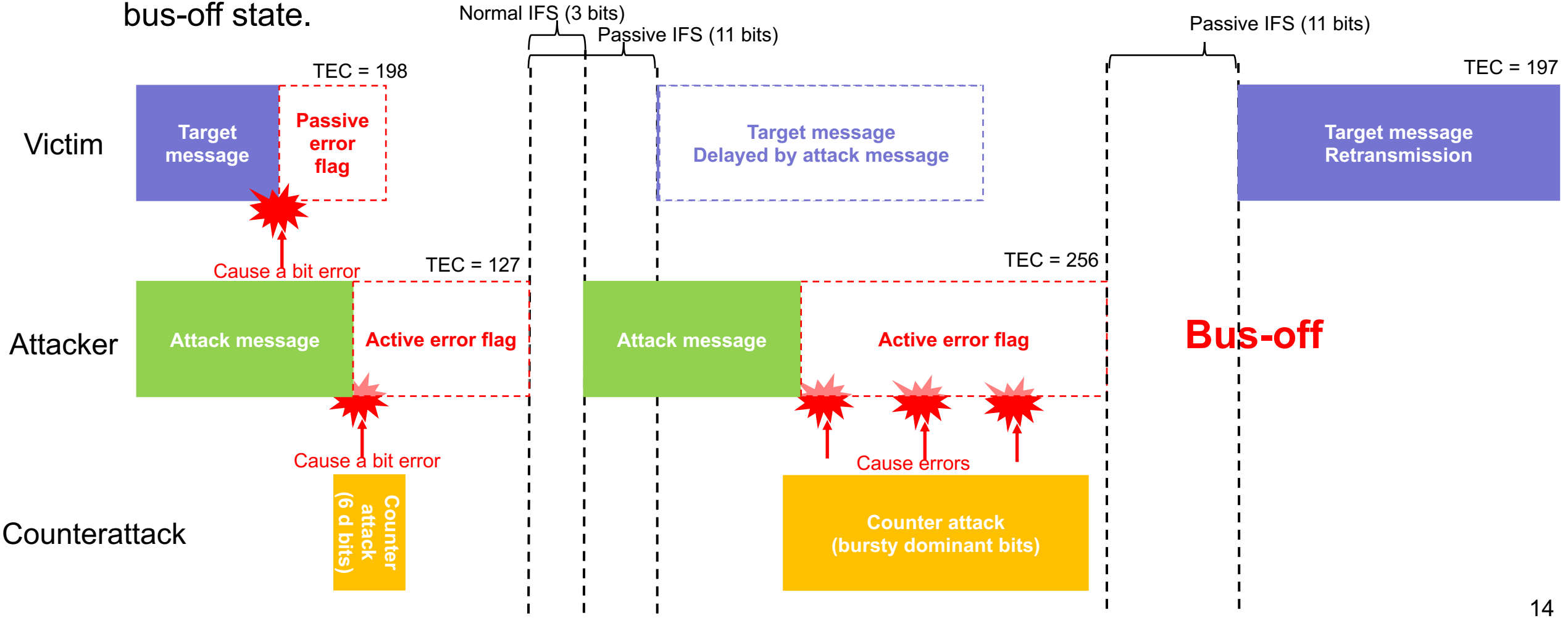
Overview

- The countermeasure force the attacker node into the bus-off state before the victim node.
- The countermeasure consists of 2 parts:
  - Detects the bus-off attack ⇒ The same method as proposed by Cho and Shin
  - Counterattacks to the attacker node.
    - Create counterattack timing.
    - Identify the attacker's message.

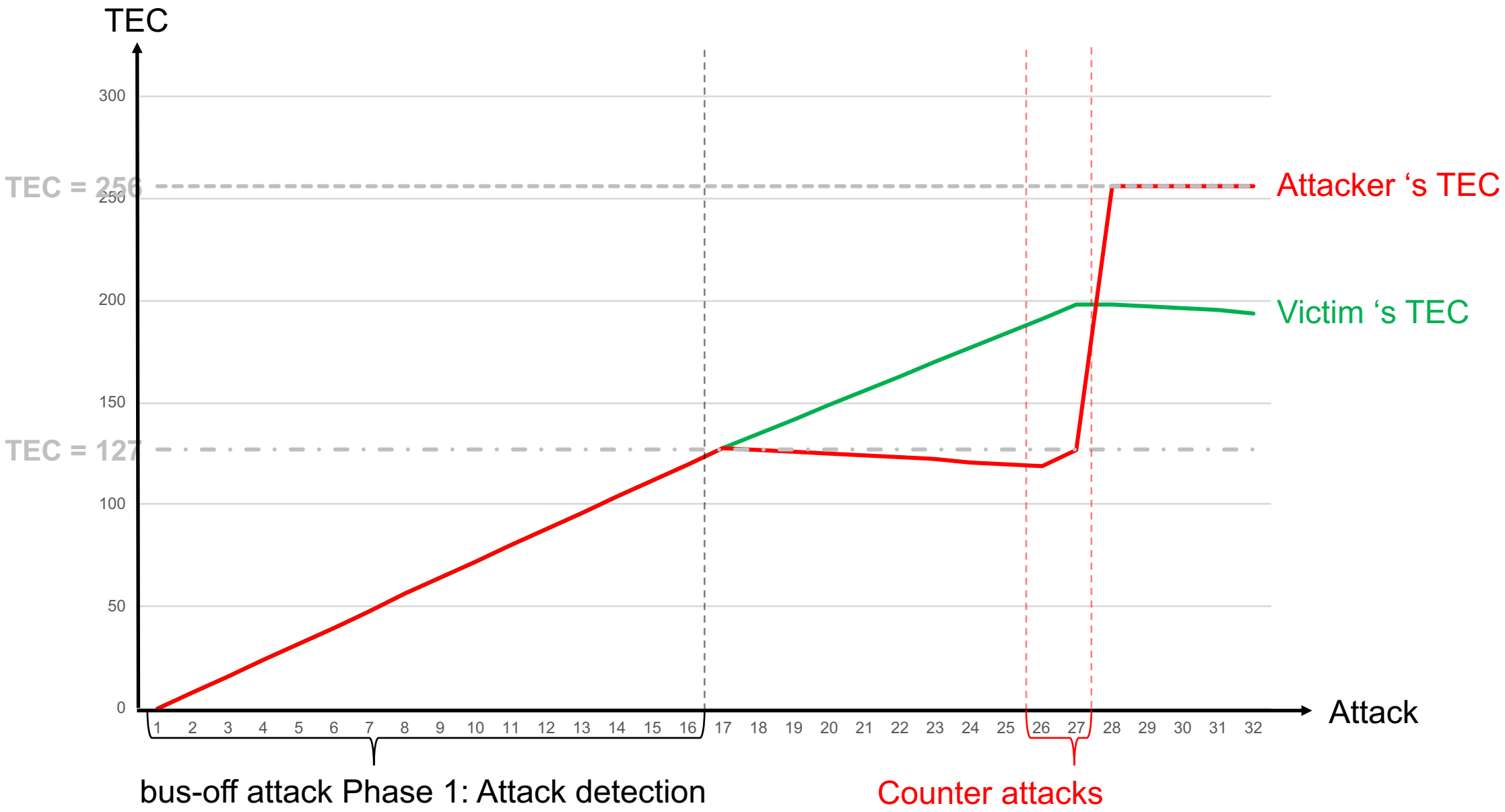


Counterattack – create timing

- We can create the opportunity that only the attacker transmits a message.
  - Difference of IFSs of the attacker (error active state) and the victim (error passive state)
- By transmitting bursty dominant bits as a counter attack, we can force the attacker into the bus-off state.

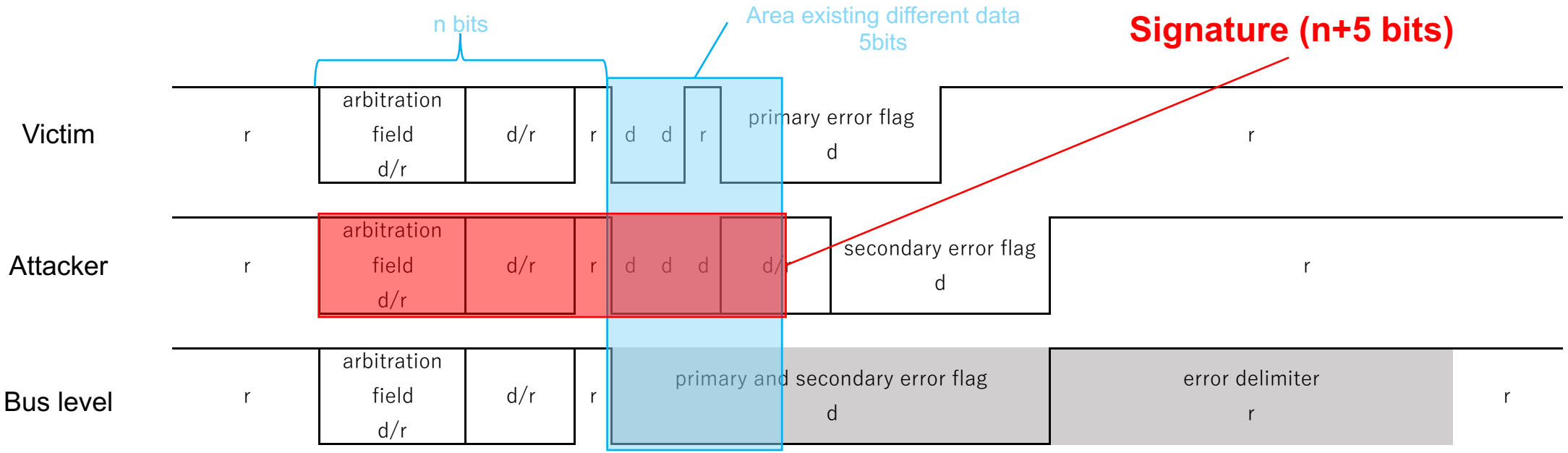


Counterattack



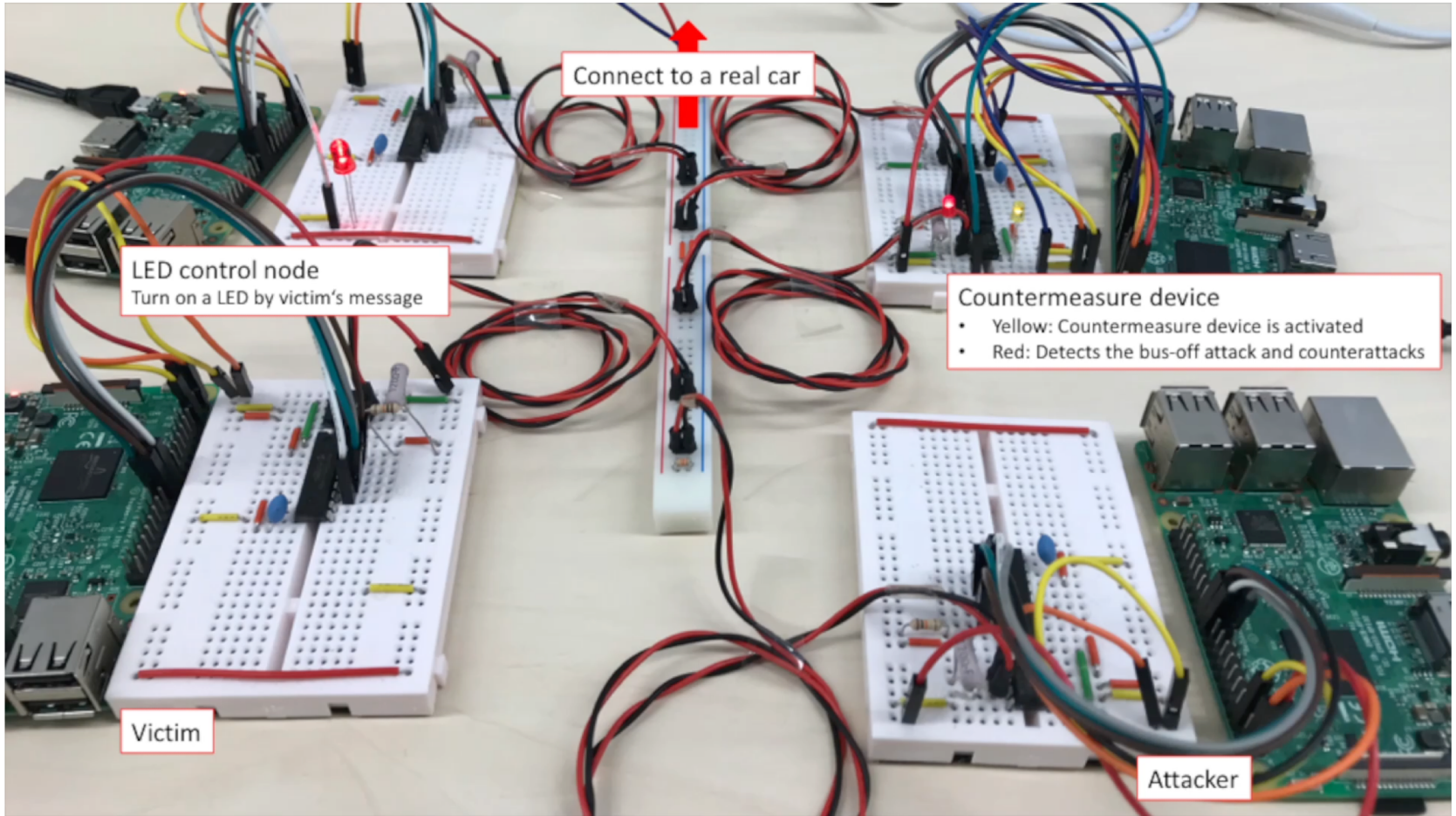
Counterattack – identify a message

- There is a possibility of counterattacking to the victim mistakenly in actual situation.
- To prevent counterattacking to the victim, identify the attacker's message.
  - Using sequence of bits from the SOF up to the 5th bit of the error frame as a signature.



Experiments

- Evaluate the feasibility on 2 environments.
  - Prototype CAN network
  - Real car with the prototype CAN network
- Always succeed the counterattack.



Conclusion and future works

Conclusion

- We proposed a novel countermeasure for the bus-off attacks.
  - Counterattacks the attacker to force it into disable state.
  - Valid for the original bus-off attack (attacked by CAN messages).
- Weakness
  - Need several intervals from detection to counterattacks.
  - Easy to avoid the countermeasure, if its mechanism is known.