Exploiting Transport Protocol Vulnerabilities in SAE J1939 Networks

Rik Chatterjee
Subhojeet Mukherjee
Jeremy Daily
Colorado State University

Colorado State University

Agenda

Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

Controller Area Network (CAN)

- Request Overload → Depletion of traffic from target ECU
- Connection Exhaustion → Denial of connections to target ECU
- BAM Block → Blocking Multi-packet Broadcast Messages
- Malicious CTS → Stopping all Multi-packet communication
- Memory Leak → Reading inaccessible memory on target ECU

Colorado State University

Transport Protocol

Electronic Control Unit (ECU)

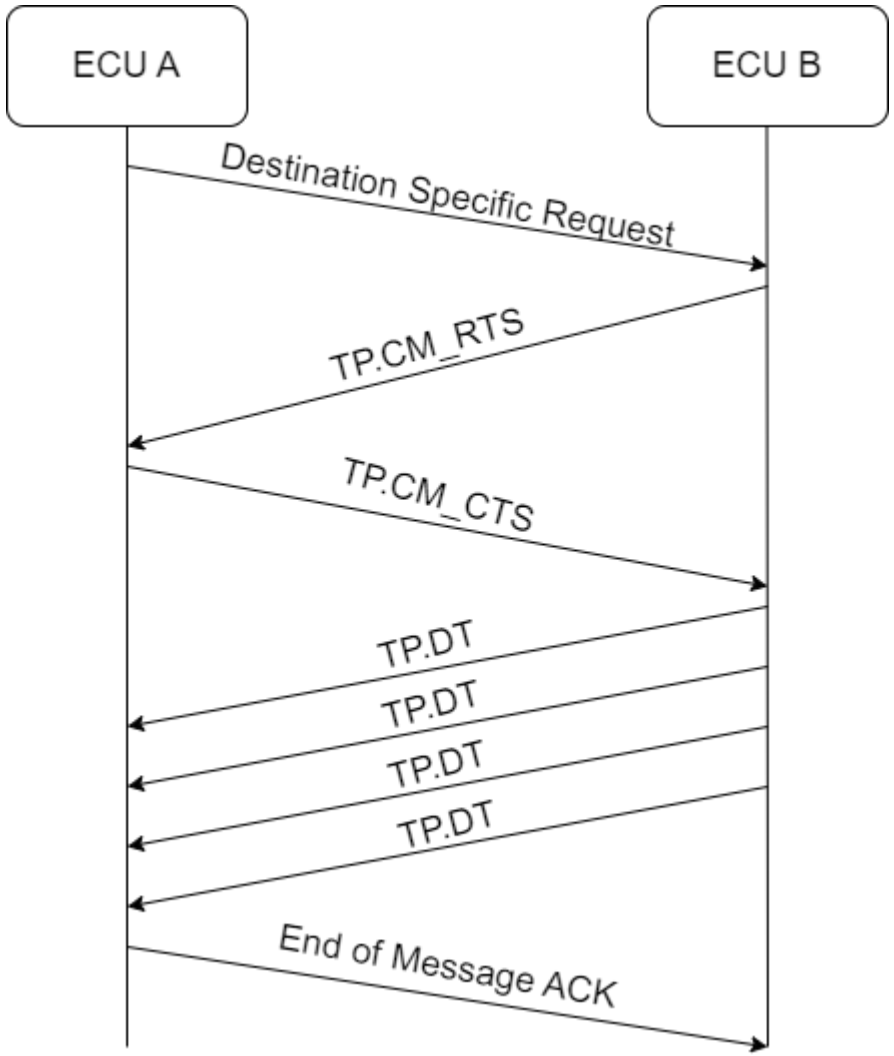
Transport Layer Networking Specifications SAE J1939/21

Controller Area Network (CAN)

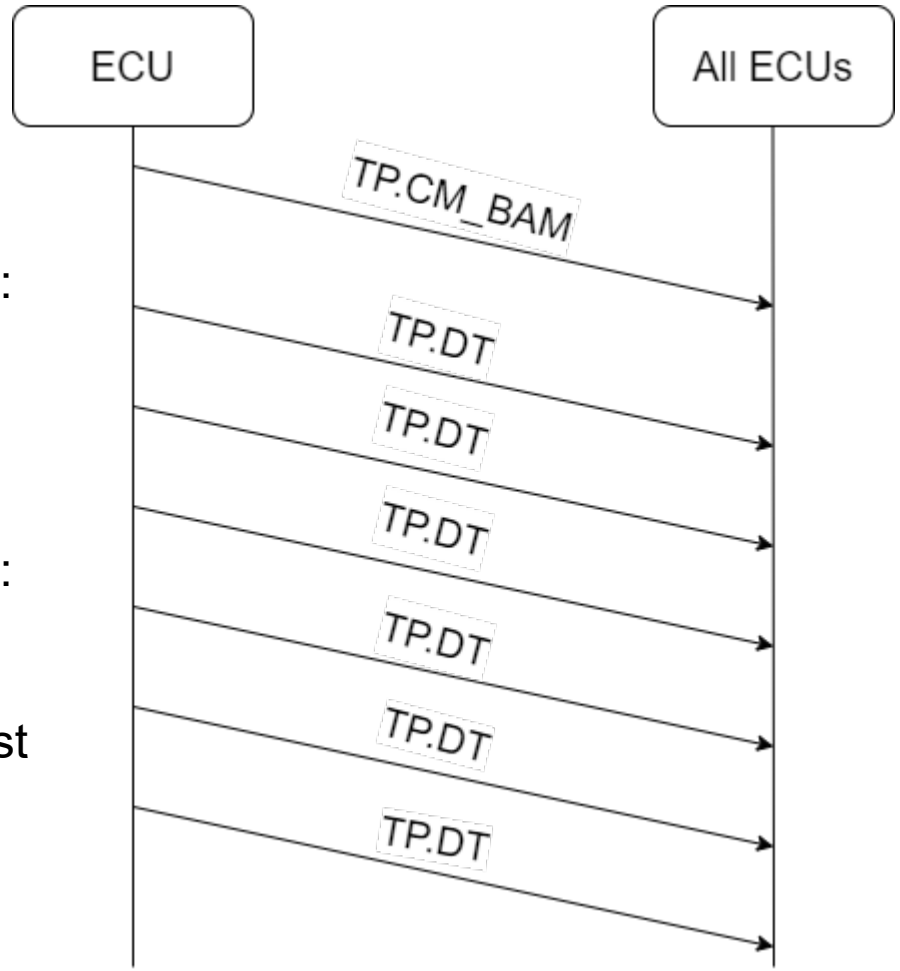
- Request Overload → Depletion of traffic from target ECU
- Connection Exhaustion → Denial of connections to target ECU
- BAM Block → Blocking Multi-packet Broadcast Messages
- Malicious CTS → Stopping all Multi-packet communication
- Memory Leak → Reading inaccessible memory on target ECU

Colorado State University

SAE J1939 Transport Protocol

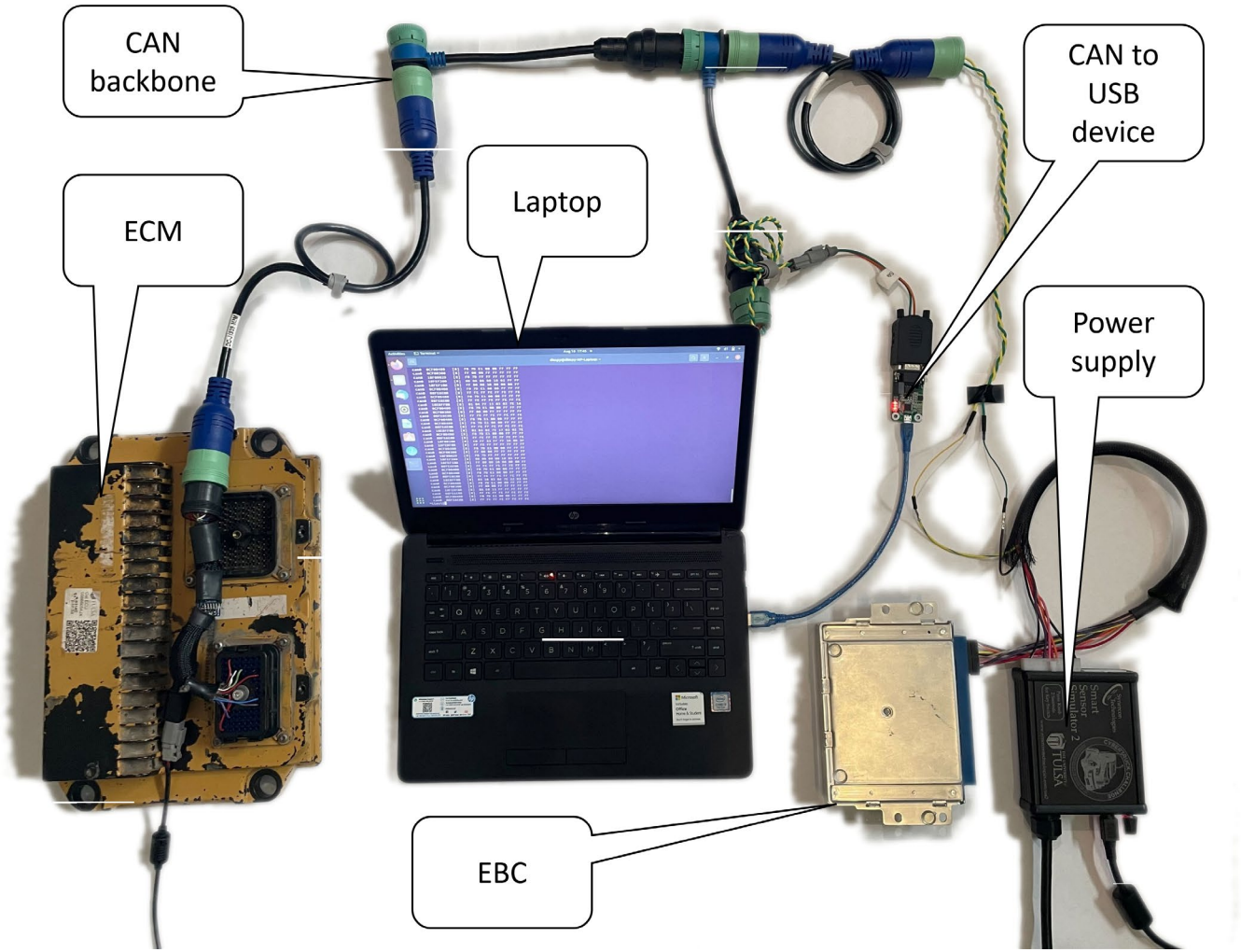


- TP.CM_RTS: Connection Management Message: Request-to-Send
- TP.CM_CTS: Connection Management Message: Clear-to-send
- TP.CM_BAM: Broadcast Announcement Message
- TP.DT: Data Packets



Colorado State University

Testbed Setup



- ➢ Testbed 1:
  - Cummins 870 ECM
  - Bendix EC-80 EBC
- ➢ Testbed 2:
  - Cummins 2350 ECM
  - Bendix EC-80 EBC
- ➢ Testbed 3:
  - Caterpillar ADEM 3 ECM
  - Bendix EC-80 EBC
- ➢ Testbed 4:
  - Caterpillar ADEM 4 ECM
  - Bendix EC-80 EBC

Colorado State University

Research Truck - PACCAR PX-7-Powered 2014 Kenworth T270

- Details:
  - Cummins 2350 ECM
  - Bendix EC-60 EBC
  - Allison RDS-200 Transmission Control Unit
  - Paccar CECU Body Controller Unit

Colorado State University

Request Overload

Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

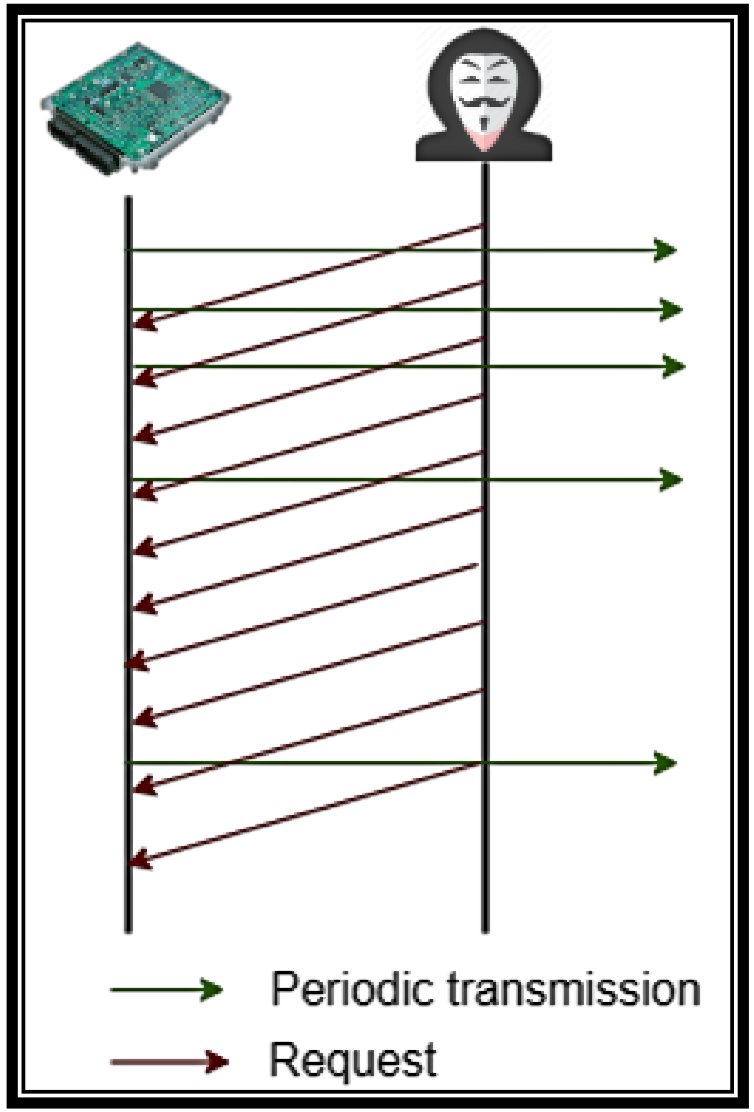
Controller Area Network (CAN)

- **Request Overload** — Depletion of traffic from target ECU
- **Connection Exhaustion** — Denial of connections to target ECU
- **BAM Block** — Blocking Multi-packet Broadcast Messages
- **Malicious CTS** — Stopping all Multi-packet communication
- **Memory Leak** — Reading inaccessible memory on target ECU

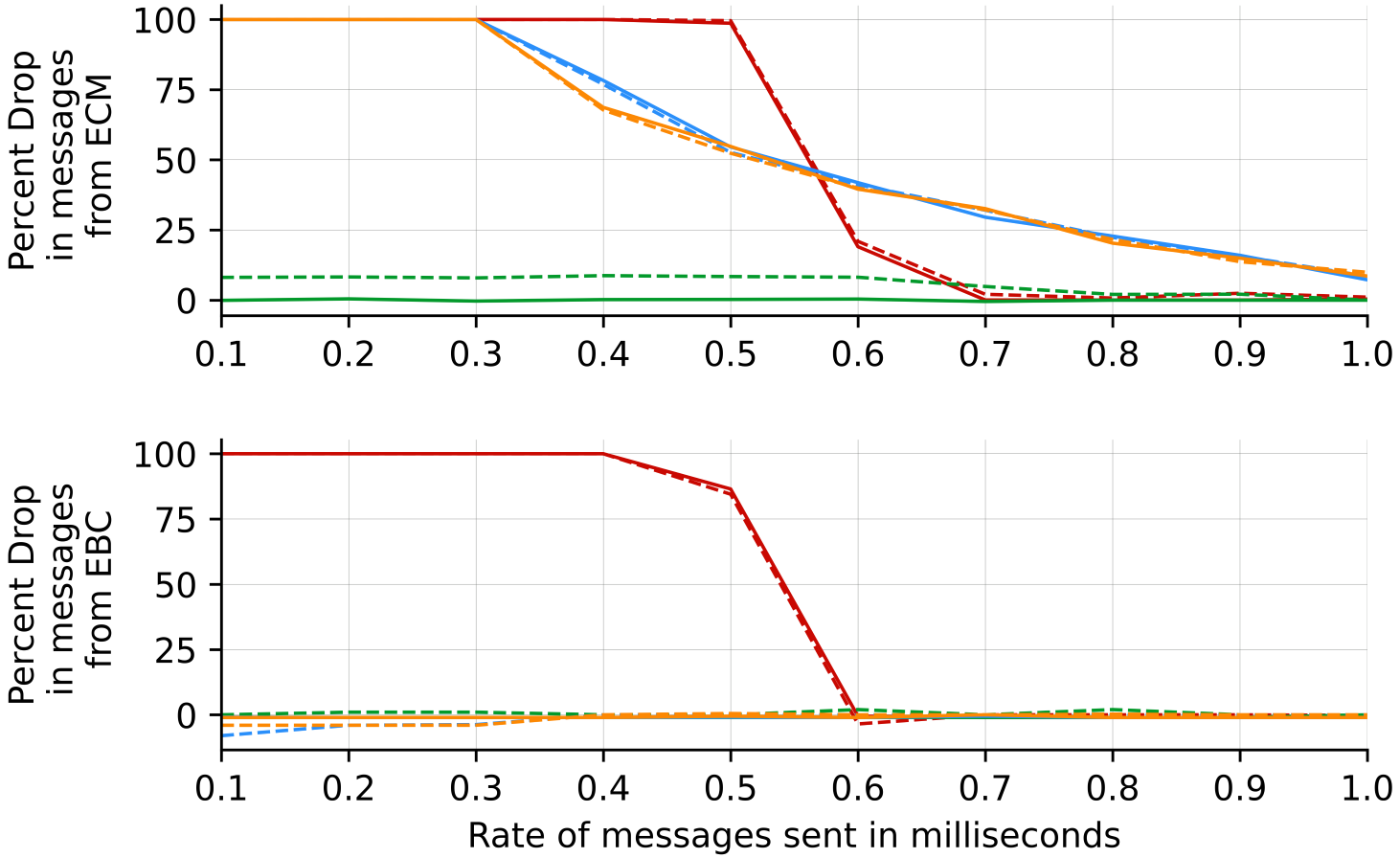
Colorado State University

Hypothesis

- **Specification**
  - All directed requests to an ECU must be processed.
- **Attack**
  - Send a high volume of SAE J1939 requests to the target ECU
- **Expected result**
  - In an attempt to serve the sent requests, the ECU fails to perform regular, more critical tasks like transmission of periodic messages



Observation on Testbed 2



Line color significance:

Red: On flooding with messages of ID 00000000_{16}

Blue: On overloading with valid request messages

Orange: On overload with invalid request messages

Green: On flooding with messages of ID $1C000000_{16}$

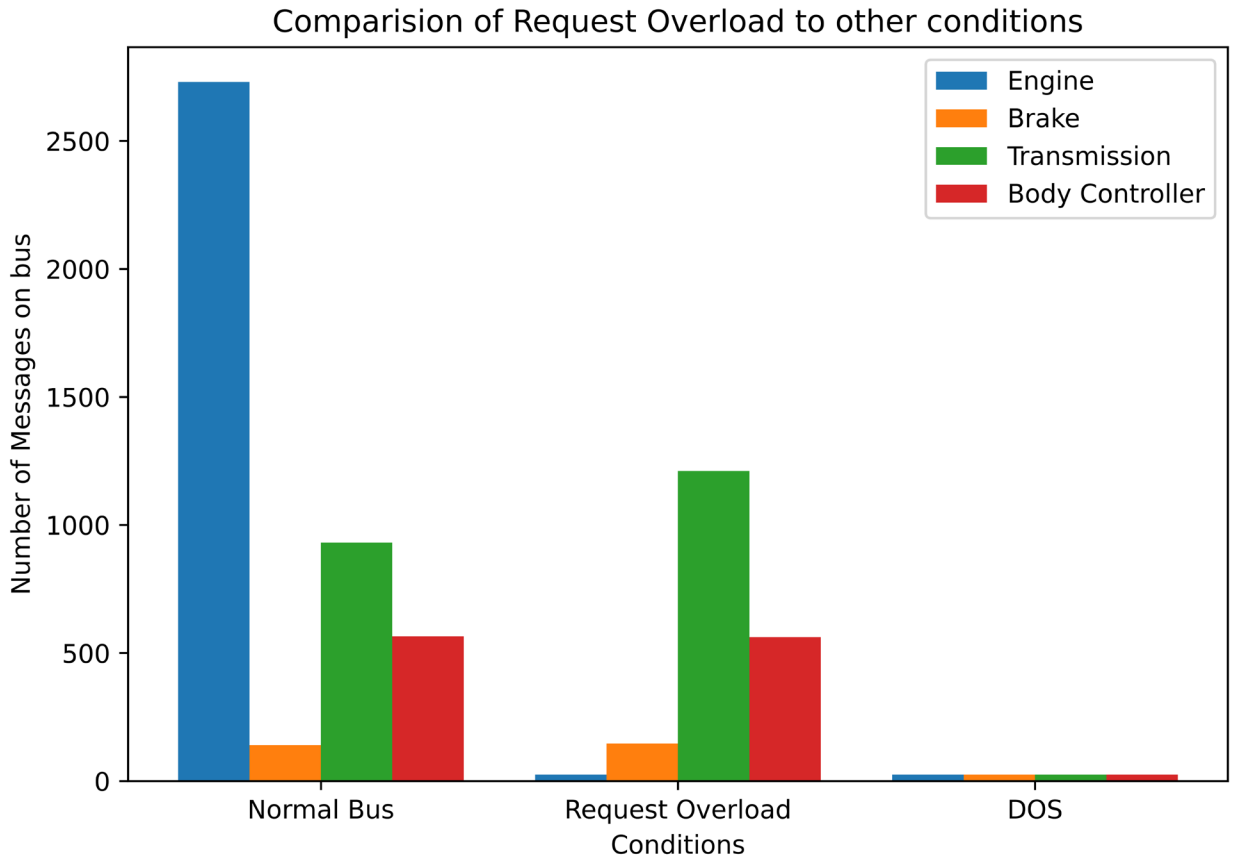
Line shape significance:

Solid: High priority ([0,3]) messages

Dashed: Low priority ([4,7]) messages

Colorado State University

Observation on a Kenworth T270 Truck



Colorado State University

Connection Exhaustion

Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

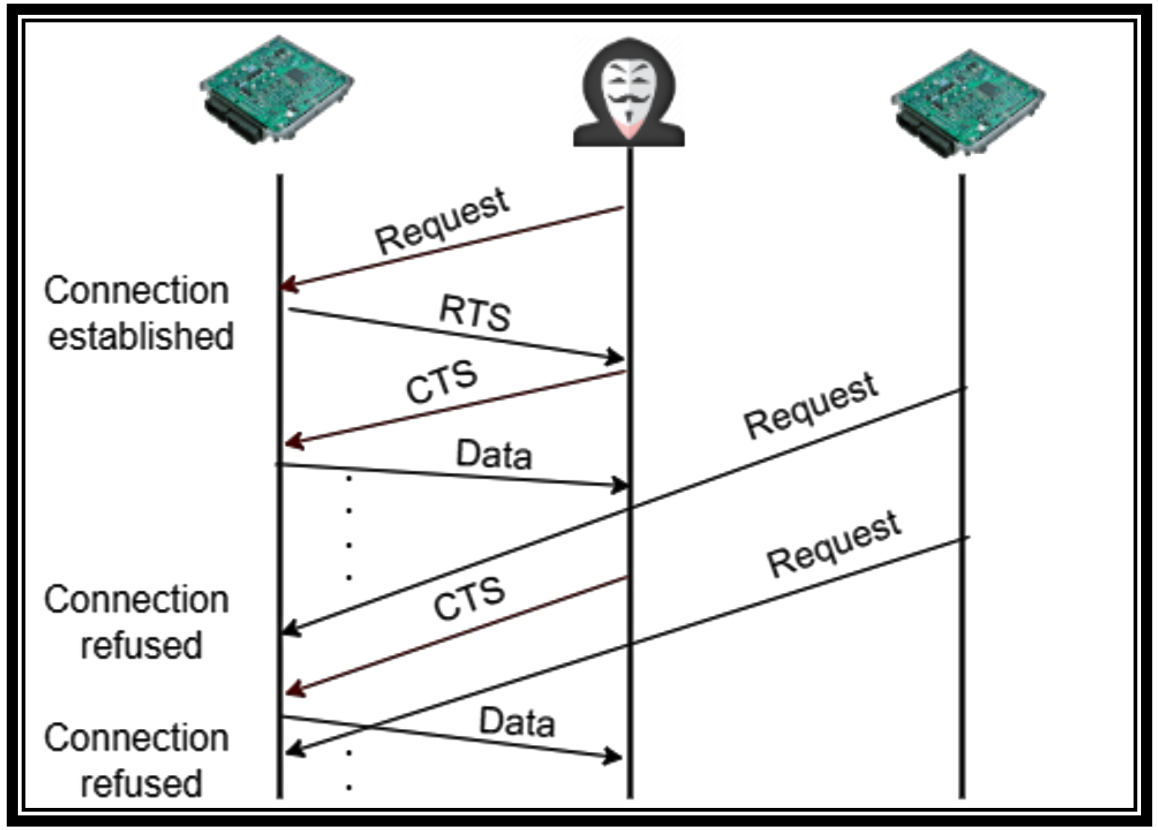
Controller Area Network (CAN)

- Request Overload → Depletion of traffic from target ECU
- Connection Exhaustion → Denial of connections to target ECU
- BAM Block → Blocking Multi-packet Broadcast Messages
- Malicious CTS → Stopping all Multi-packet communication
- Memory Leak → Reading inaccessible memory on target ECU

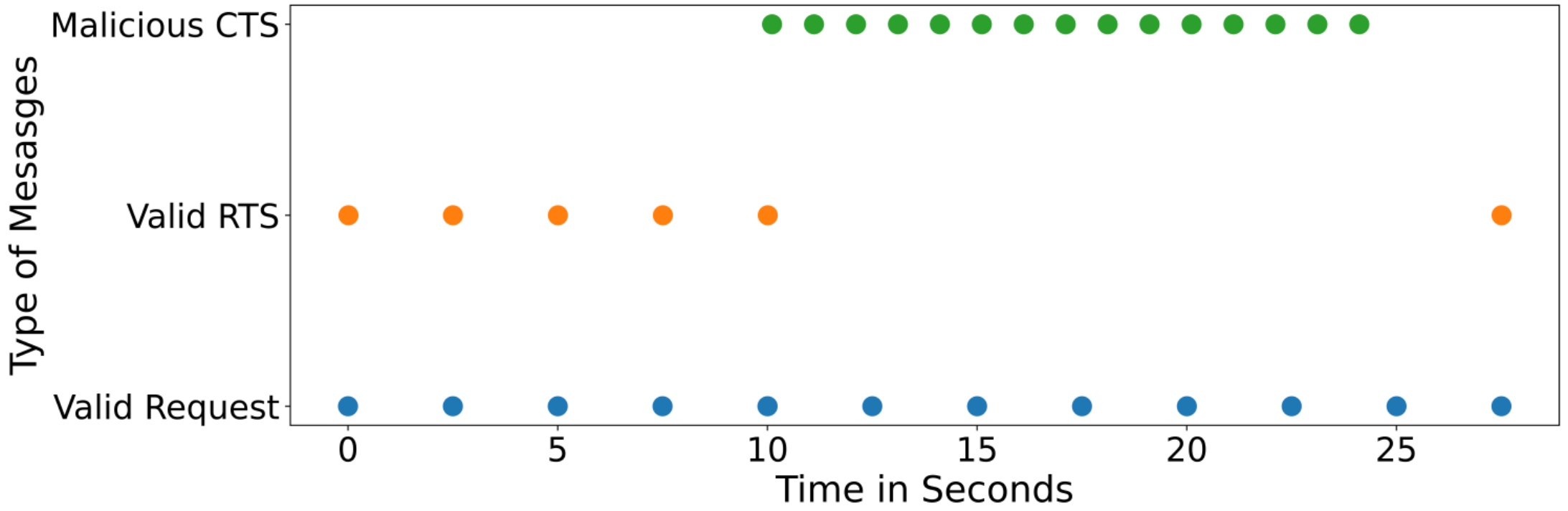
Colorado State University

Hypothesis

- **Specification**
  - Exactly one established connection for unidirectional transfer
  - Connection can be kept open for 1250 milliseconds by not sending the end of message acknowledgment
  - CTS message can be sent to request message retransmission
- **Attack**
  - Create multiple spoofed connections
  - Keep connections open by
    - Sending CTS at intervals less than 1250 ms
    - Not sending of end of message acknowledgement
- **Expected result**
  - Denial of legitimate connection attempts to the target

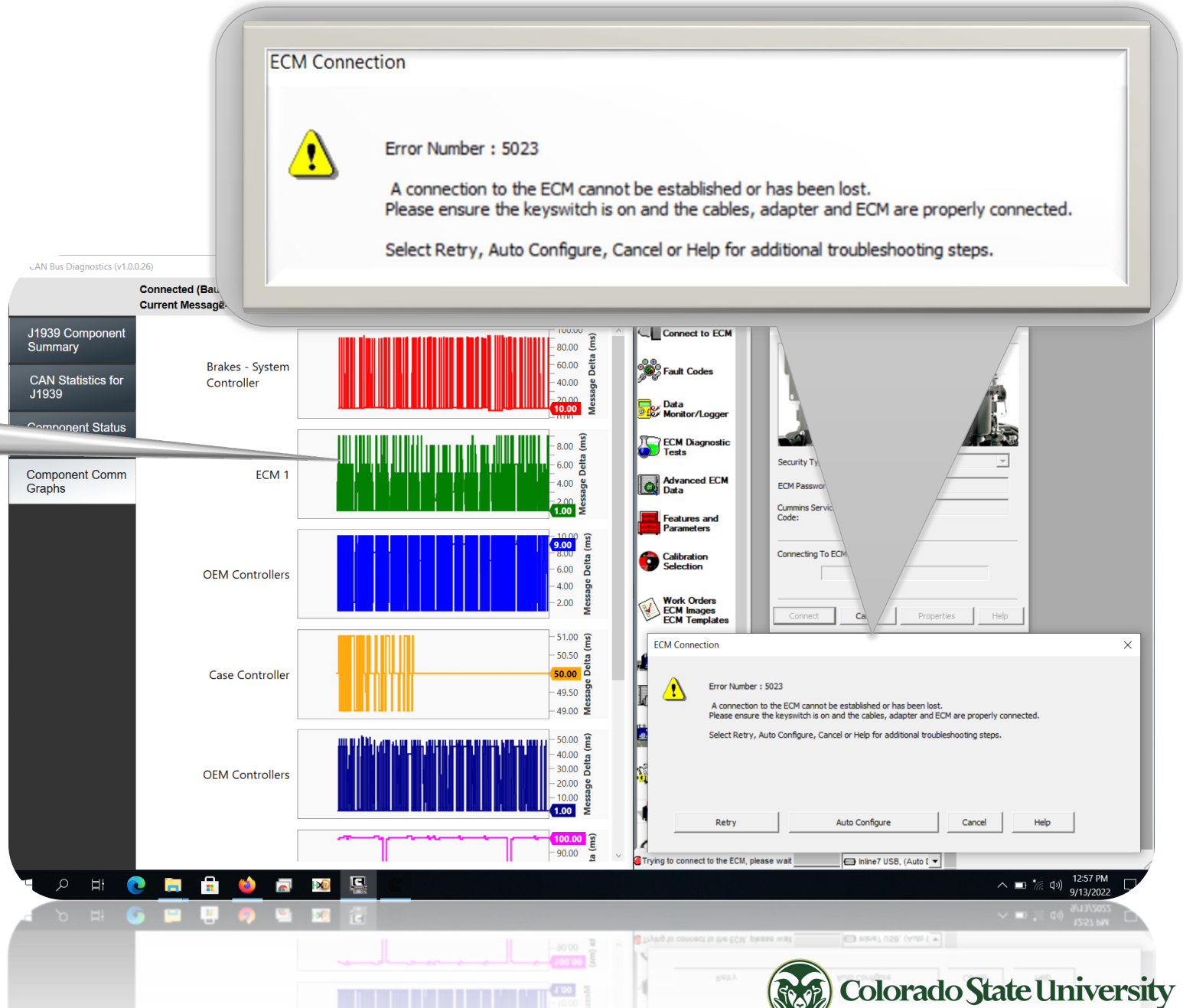


Observation on Testbed 1



Observation on Cummins Diagnostic Tool

ECM activity normal



Colorado State University

BAM Block

Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

Controller Area Network (CAN)

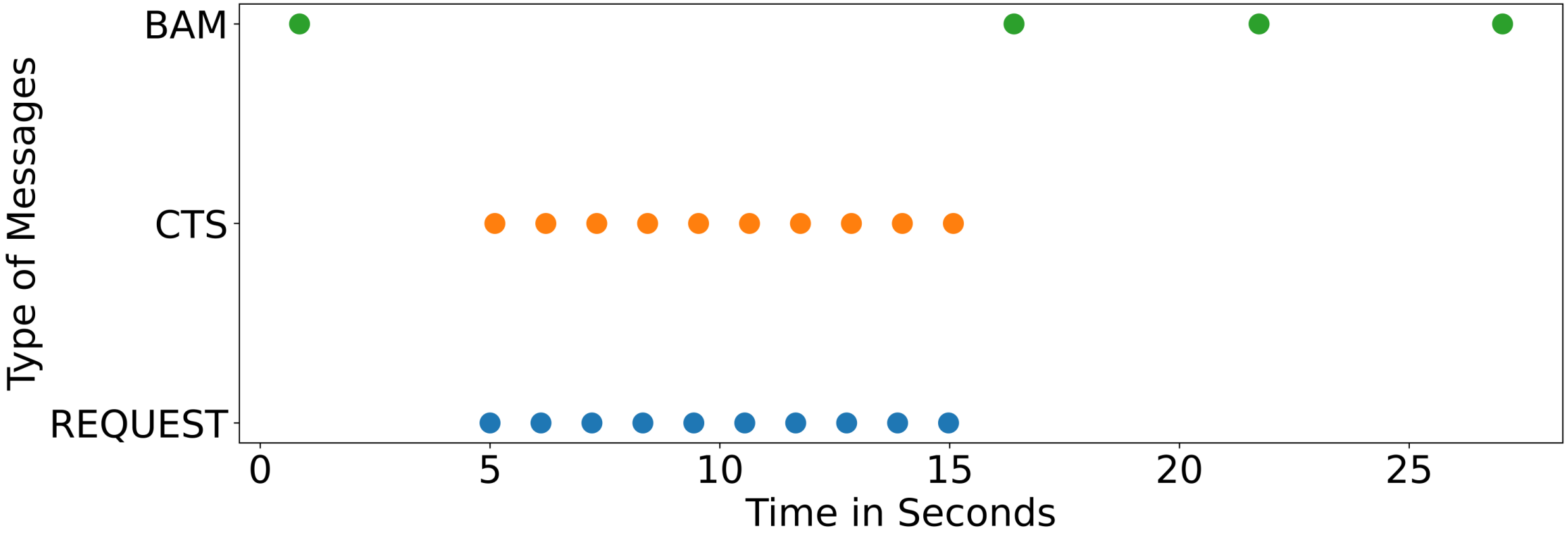
- Request Overload → Depletion of traffic from target ECU
- Connection Exhaustion → Denial of connections to target ECU
- BAM Block → Blocking Multi-packet Broadcast Messages
- Malicious CTS → Stopping all Multi-packet communication
- Memory Leak → Reading inaccessible memory on target ECU

Colorado State University

Hypothesis

- **Specification**
  - The SAE J1939-21 standard suggests that an ECU must respond to destination-specific requests.
- **Attack**
  - An attack can be constructed whereby an attacker sends destination-specific requests for messages that an ECU broadcasts globally as BAMs with the expectation that this might force the ECU to respond to such a request
- **Expected Result**
  - The global broadcast communication halts denying information to all ECUs on the network

Observation on Testbed 3



Malicious CTS

Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

Controller Area Network (CAN)

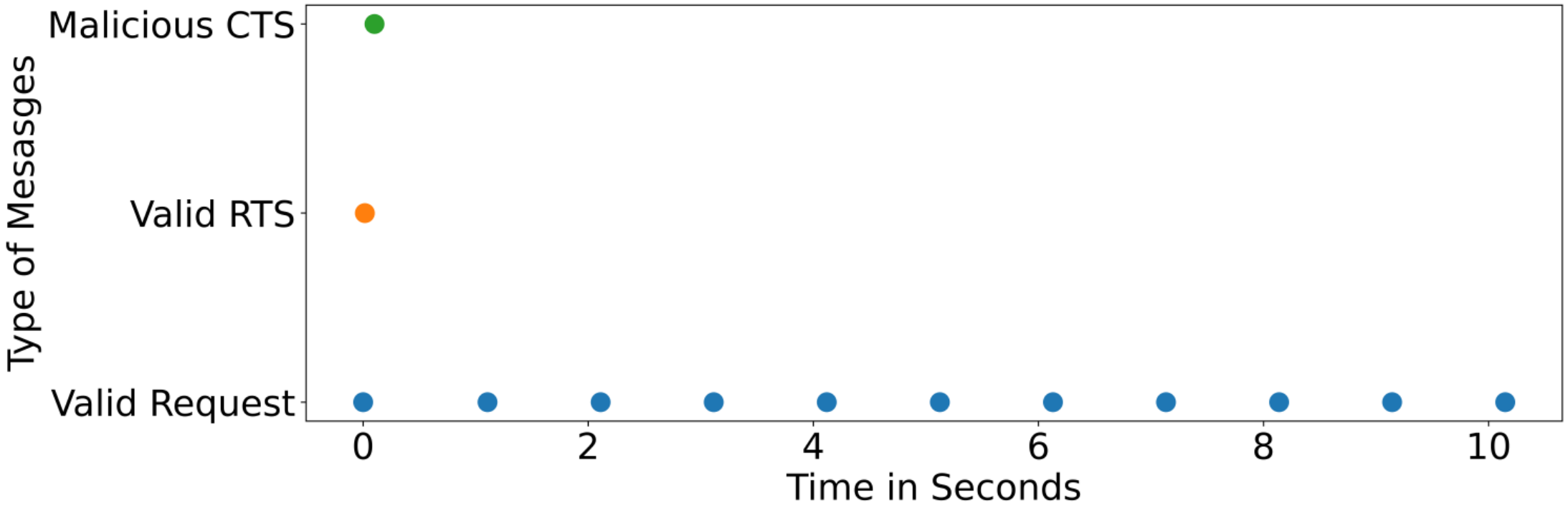
- Request Overload → Depletion of traffic from target ECU
- Connection Exhaustion → Denial of connections to target ECU
- BAM Block → Blocking Multi-packet Broadcast Messages
- Malicious CTS → Stopping all Multi-packet communication
- Memory Leak → Reading inaccessible memory on target ECU

Colorado State University

Hypothesis

- **Specification**
  - A CTS message should contain information indicating the packet number of the next data packet to be sent
- **Attack**
  - An attack can be constructed to send a malicious CTS message with value of the next packet to be sent that exceeds the total number of packets that can be sent indicated by the RTS message
- **Expected Result**
  - This may cause the targeted ECU to enter an unknown state and thus hinder normal operations

Observation on Testbed 3



Colorado State University

Memory Leak

Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

Controller Area Network (CAN)

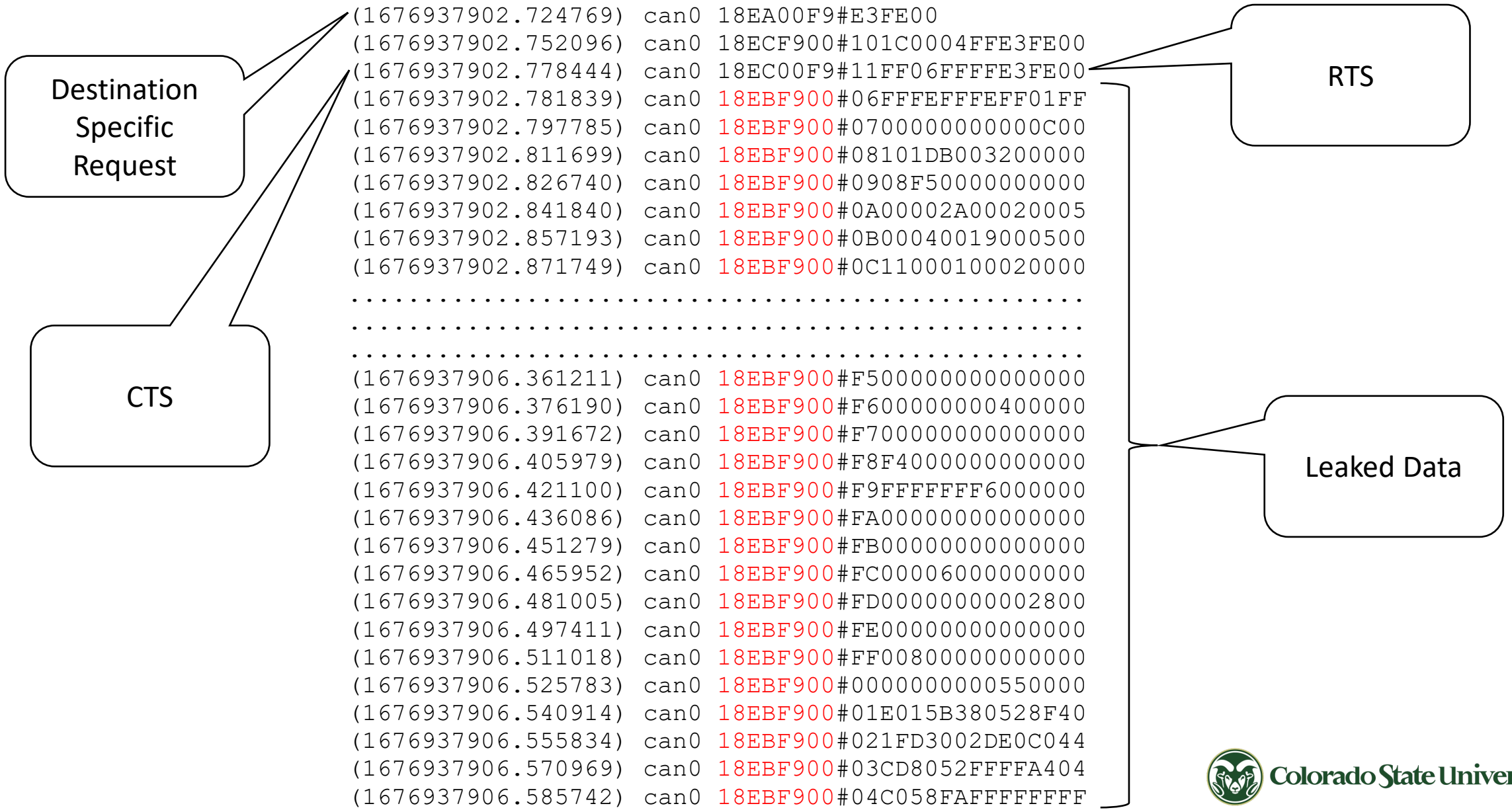
- **Request Overload** → Depletion of traffic from target ECU
- **Connection Exhaustion** → Denial of connections to target ECU
- **BAM Block** → Blocking Multi-packet Broadcast Messages
- **Malicious CTS** → Stopping all Multi-packet communication
- **Memory Leak** → Reading inaccessible memory on target ECU

Colorado State University

Hypothesis

- **Specification**
  - A CTS message should contain information indicating the number of data packets that can be sent over the transport protocol
- **Attack**
  - An attack can be constructed by sending a crafted CTS message with the value of the number of packets that can be sent larger value indicated by the RTS
- **Expected Result**
  - Get back data that is not supposed to be returned in multipacket transfer

Observation on Testbed 3



Colorado State University

Thank you

Questions ?