Exploiting Transport Protocol Vulnerabilities in SAE J1939 Networks

VehicleSec 2023

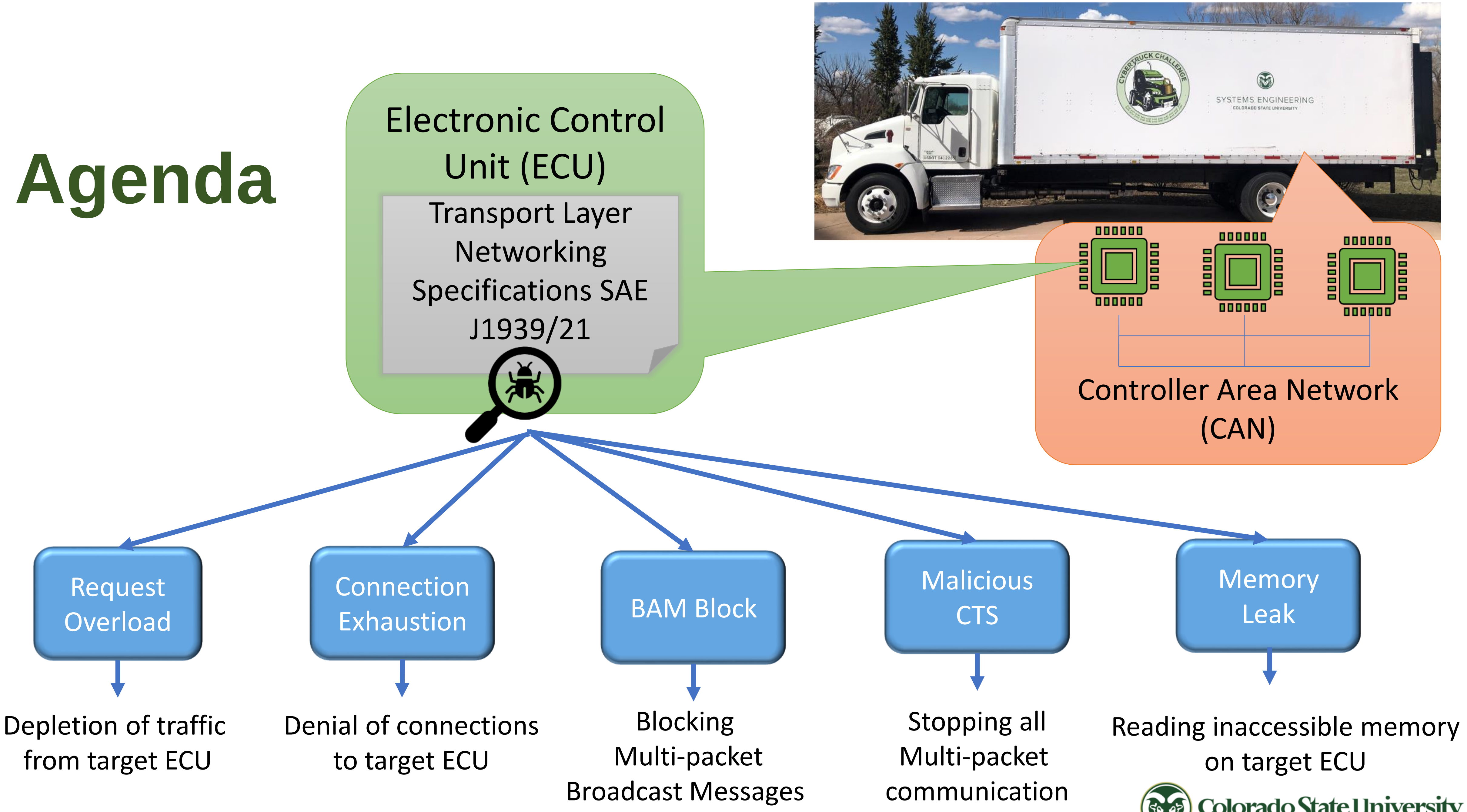
Rik Chatterjee

Subhojeet Mukherjee

Jeremy Daily

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

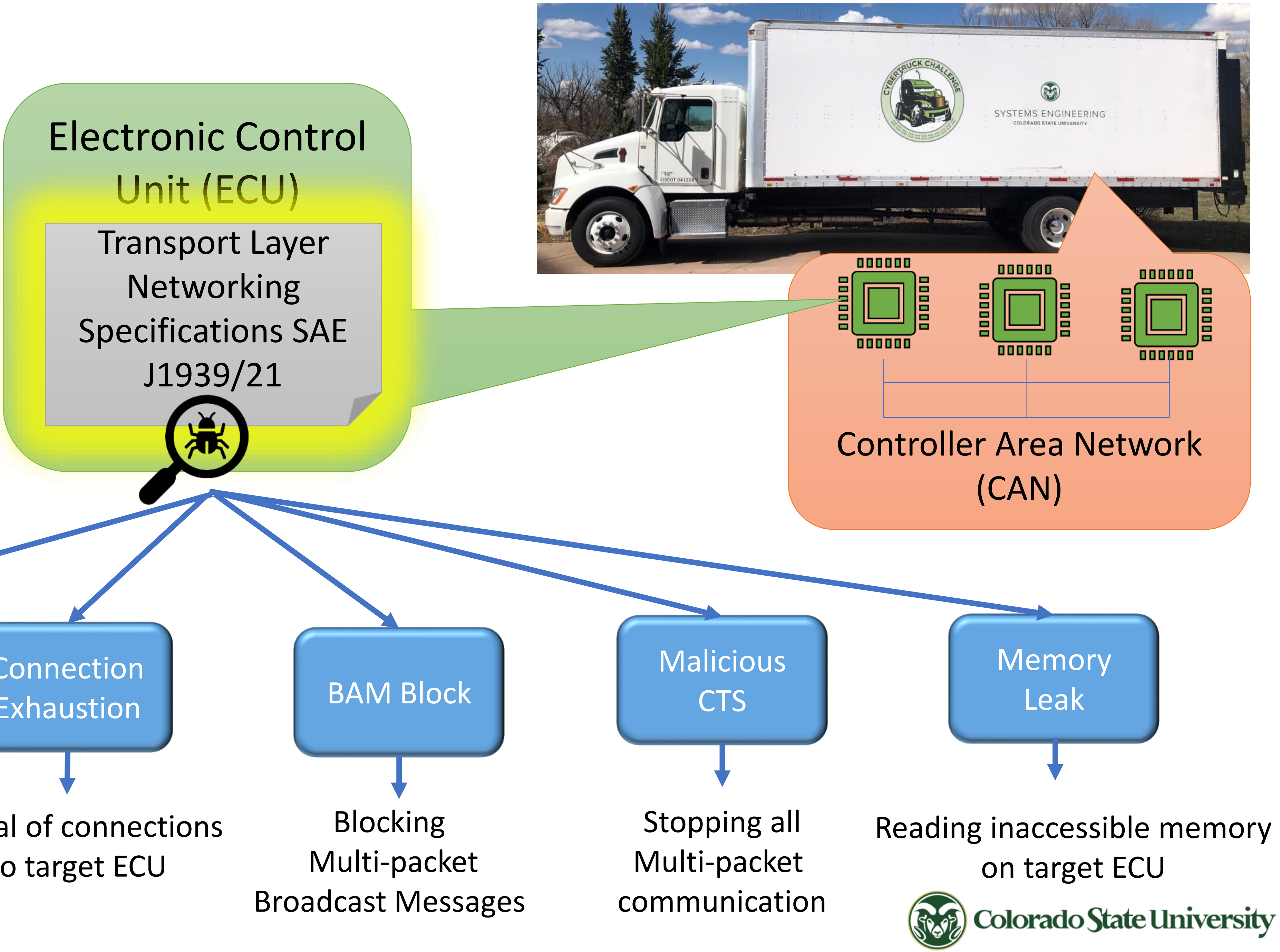
BAM Block → Blocking Multi-packet Broadcast Messages

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

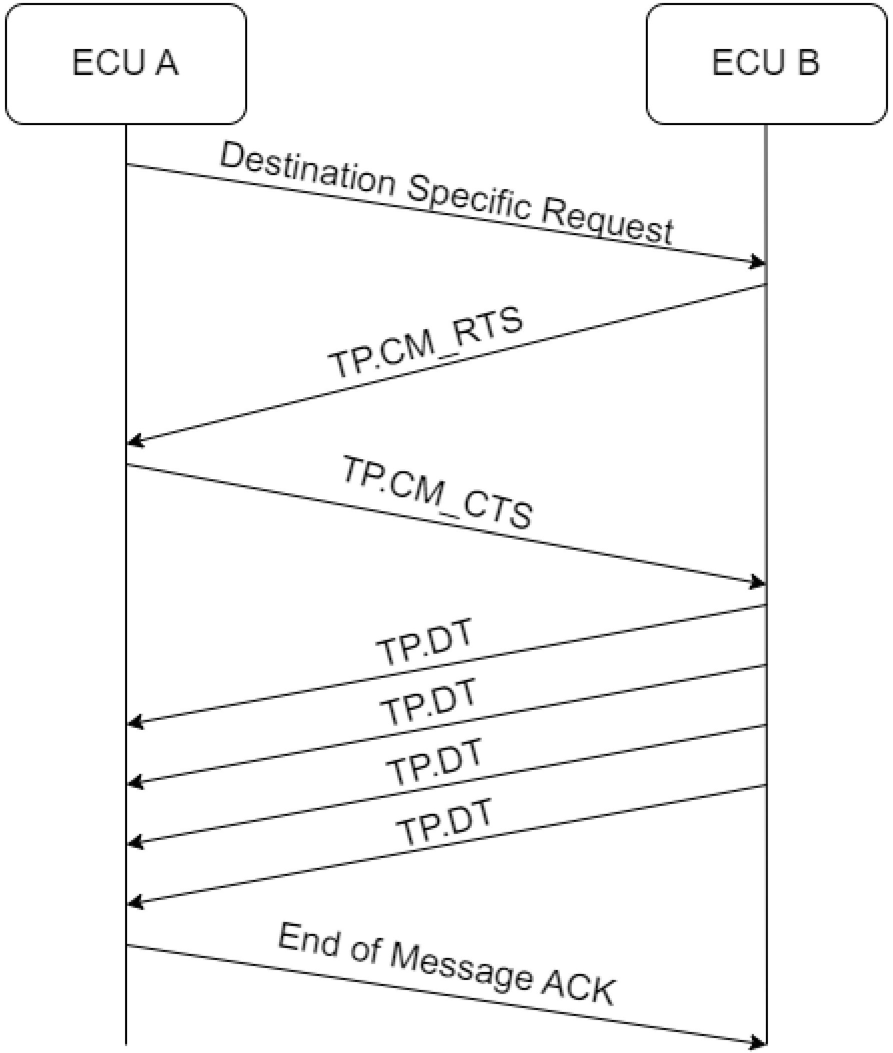
BAM Block → Blocking Multi-packet Broadcast Messages

Malicious CTS → Stopping all Multi-packet communication

Memory Leak → Reading inaccessible memory on target ECU

Colorado State University

SAE J1939 Transport Protocol

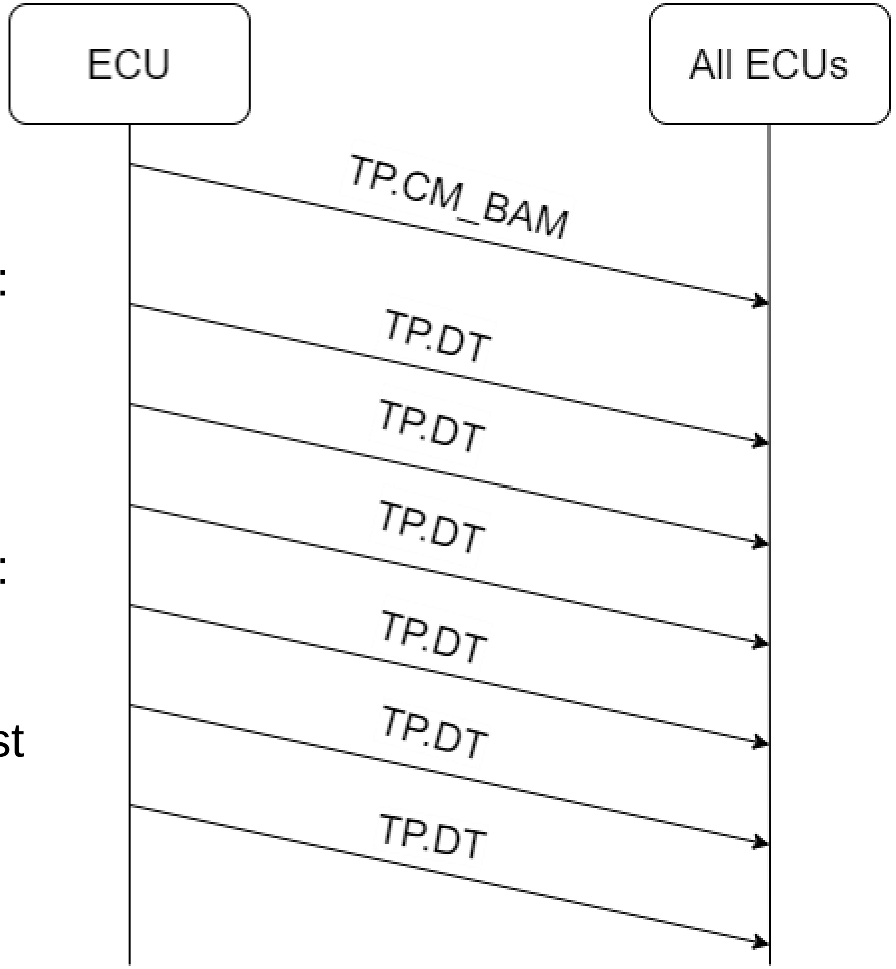


- TP.CM_RTS: Connection Management Message: Request-to-Send

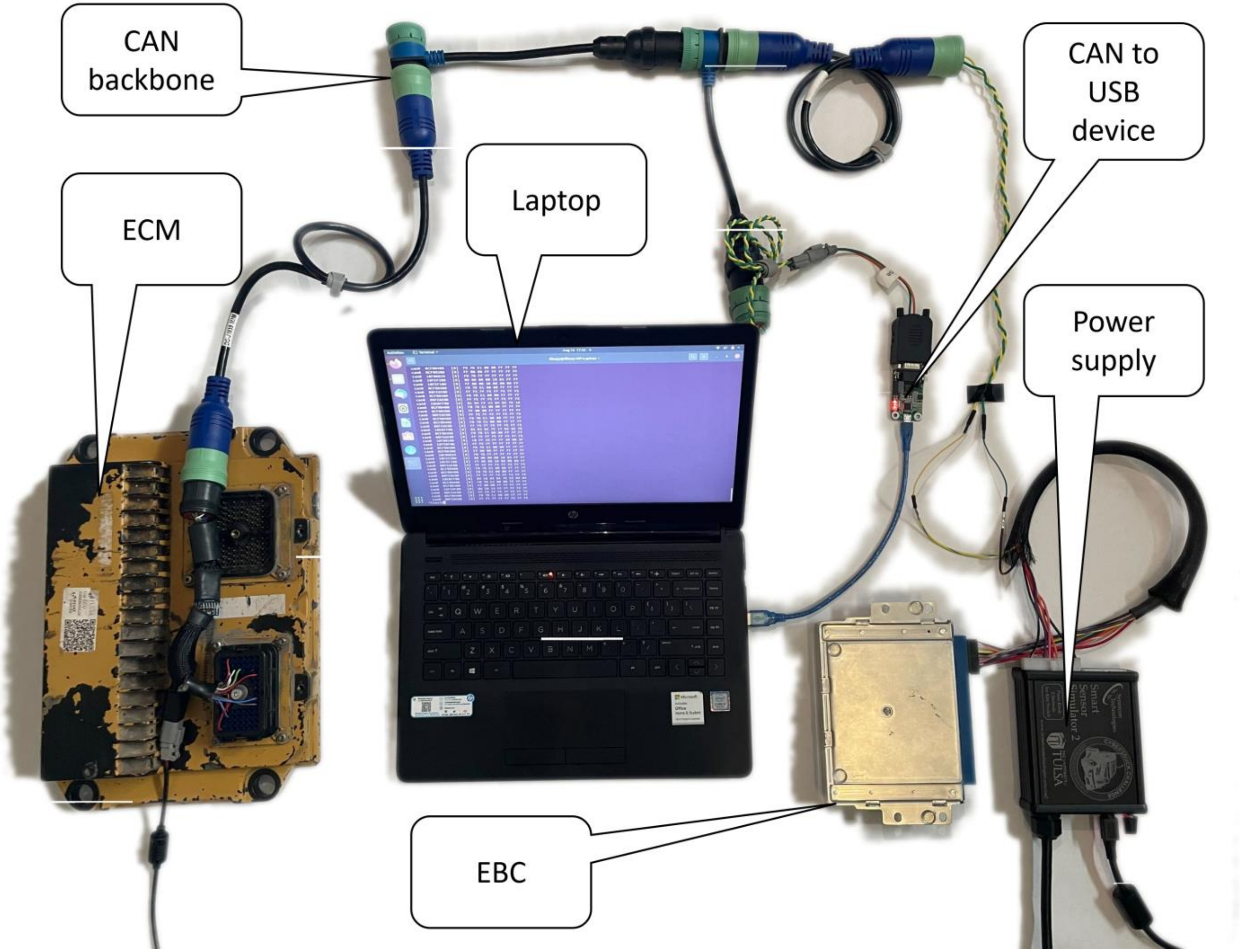
- TP.CM_CTS: Connection Management Message: Clear-to-send

- TP.CM_BAM: Broadcast Announcement Message

- TP.DT: Data Packets



Testbed Setup



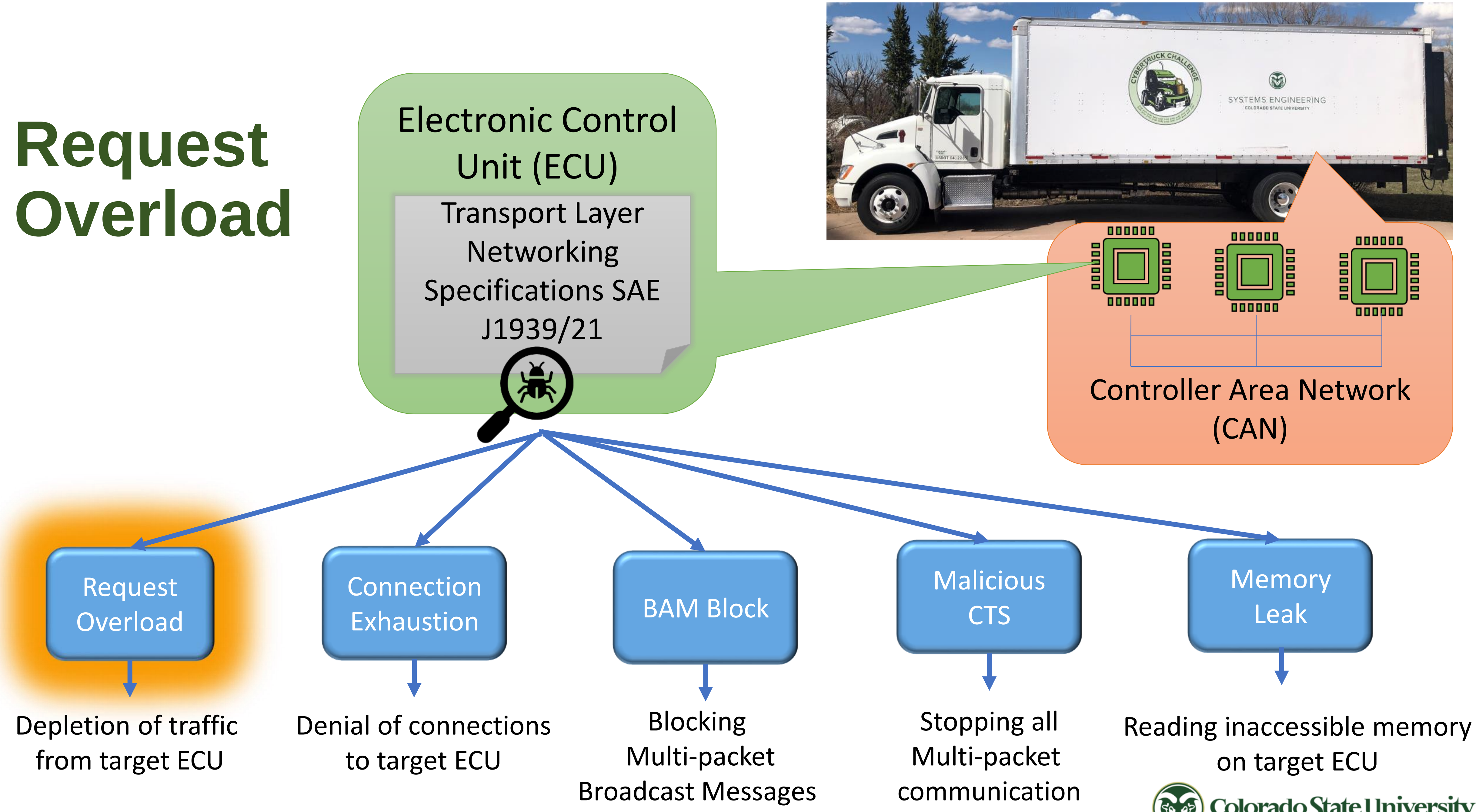
- ➢ Testbed 1:
  - Cummins 870 ECM
  - Bendix EC-80 EBC
- ➢ Testbed 2:
  - Cummins 2350 ECM
  - Bendix EC-80 EBC
- ➢ Testbed 3:
  - Caterpillar ADEM 3 ECM
  - Bendix EC-80 EBC
- ➢ Testbed 4:
  - Caterpillar ADEM 4 ECM
  - Bendix EC-80 EBC

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

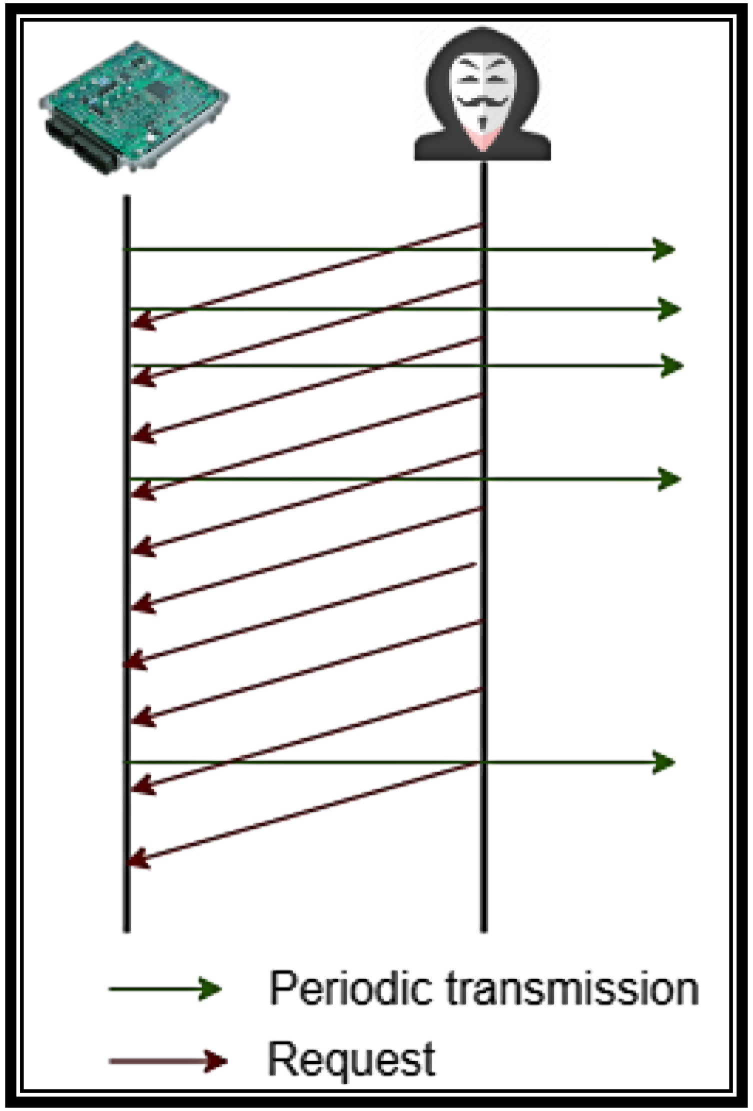
Malicious CTS → Stopping all Multi-packet communication

Memory Leak → Reading inaccessible memory on target ECU

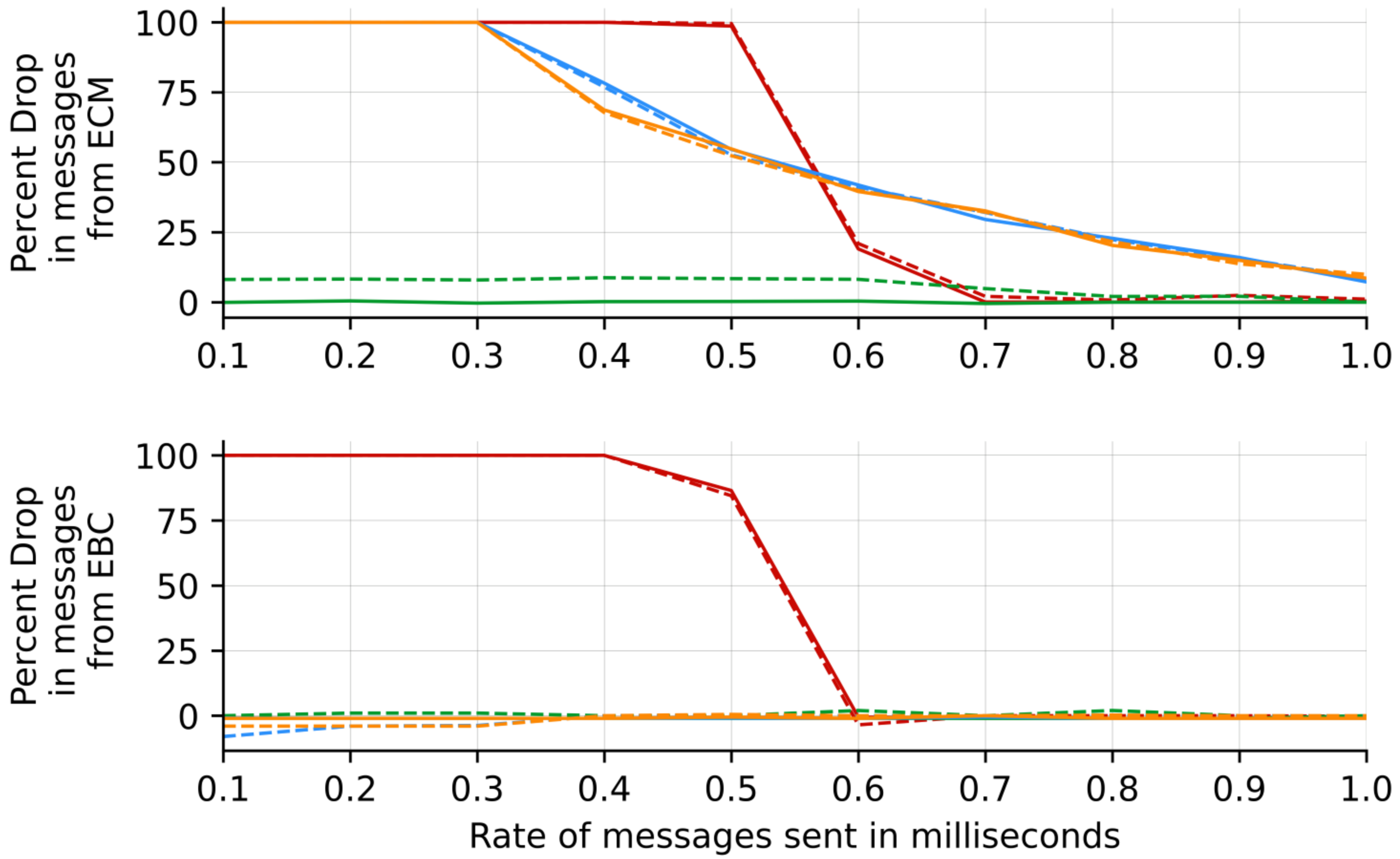
Colorado State University

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

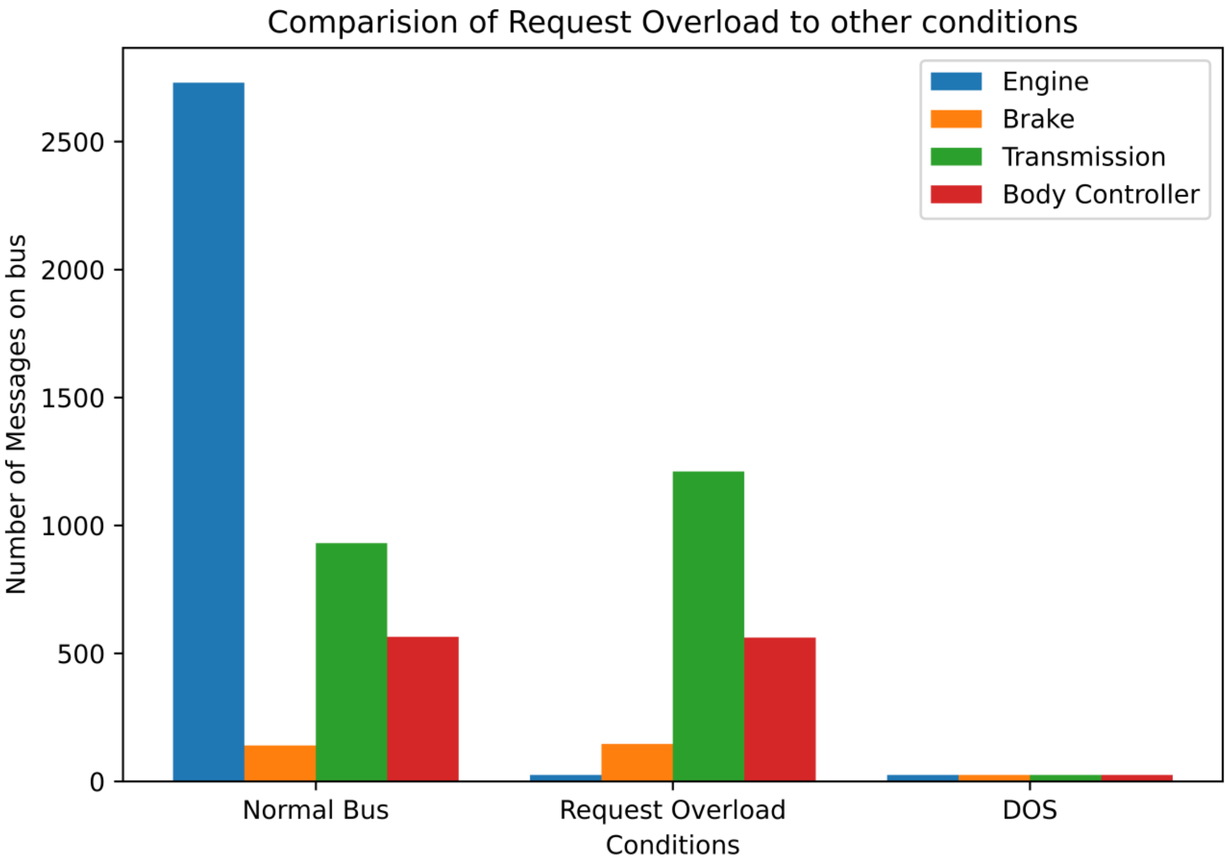
Green: On flooding with messages of ID $1C000000_{16}$

Line shape significance:

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

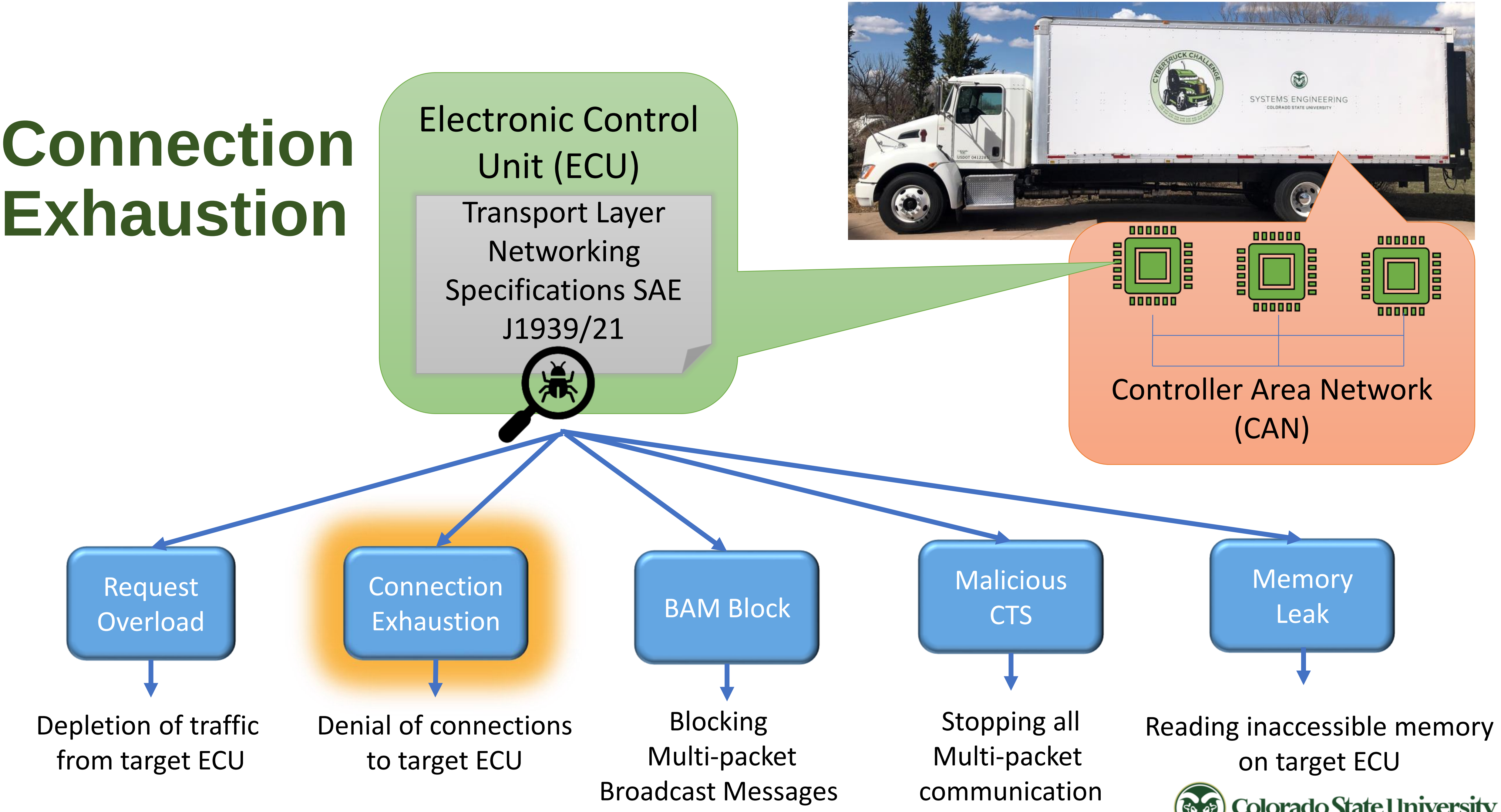
Dashed: Low priority ([4,7]) messages

Observation on a Kenworth T270 Truck



Live Attack Demonstration on Kenworth T270 Truck

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

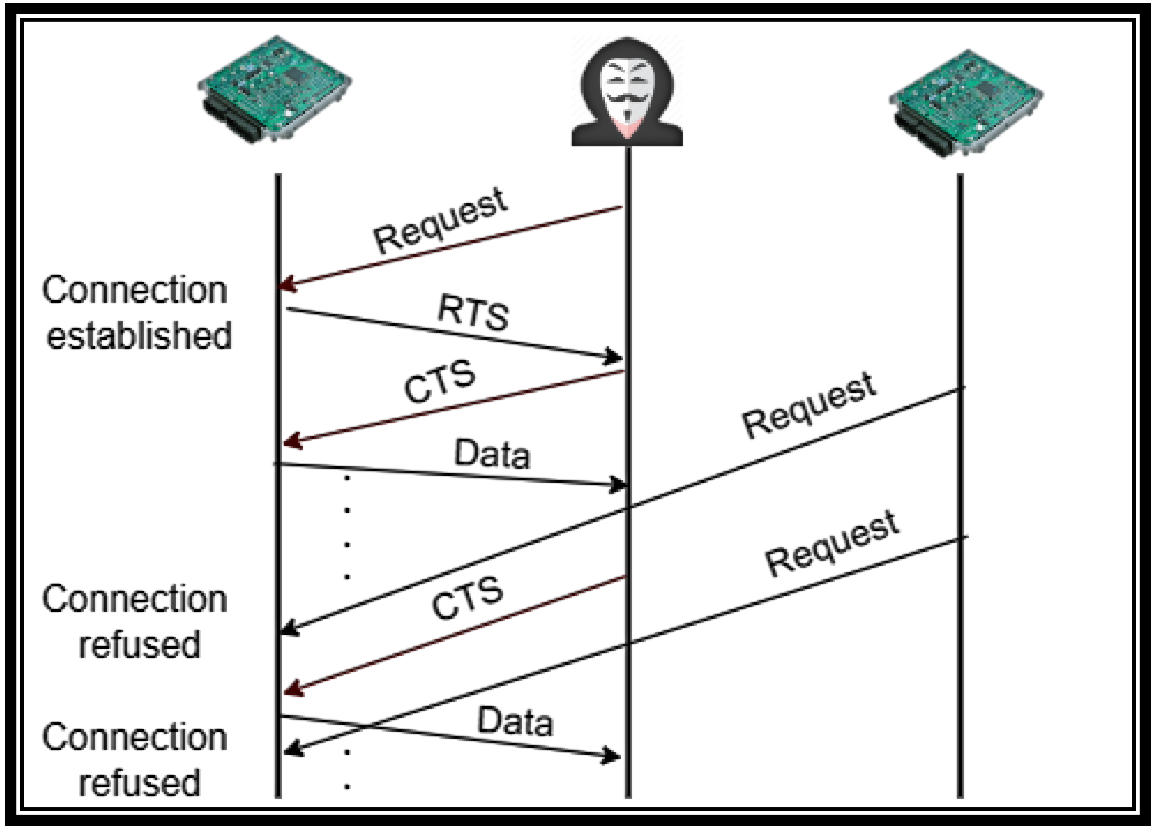
BAM Block → Blocking Multi-packet Broadcast Messages

Malicious CTS → Stopping all Multi-packet communication

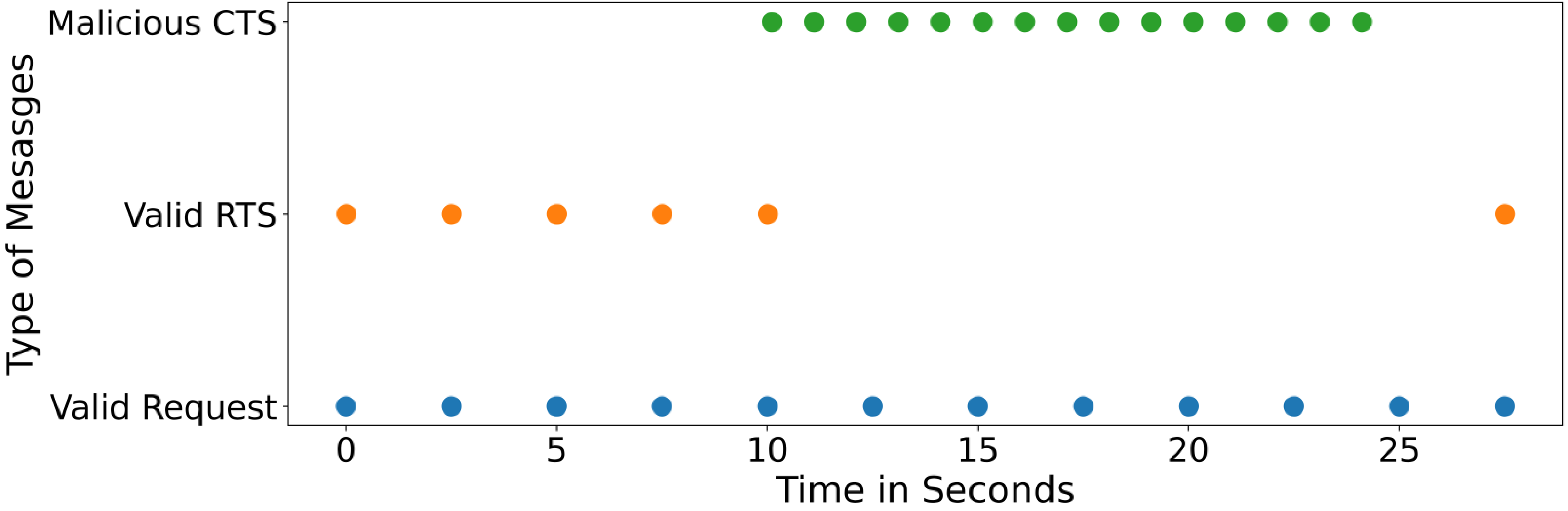
Memory Leak → Reading inaccessible memory on target ECU

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

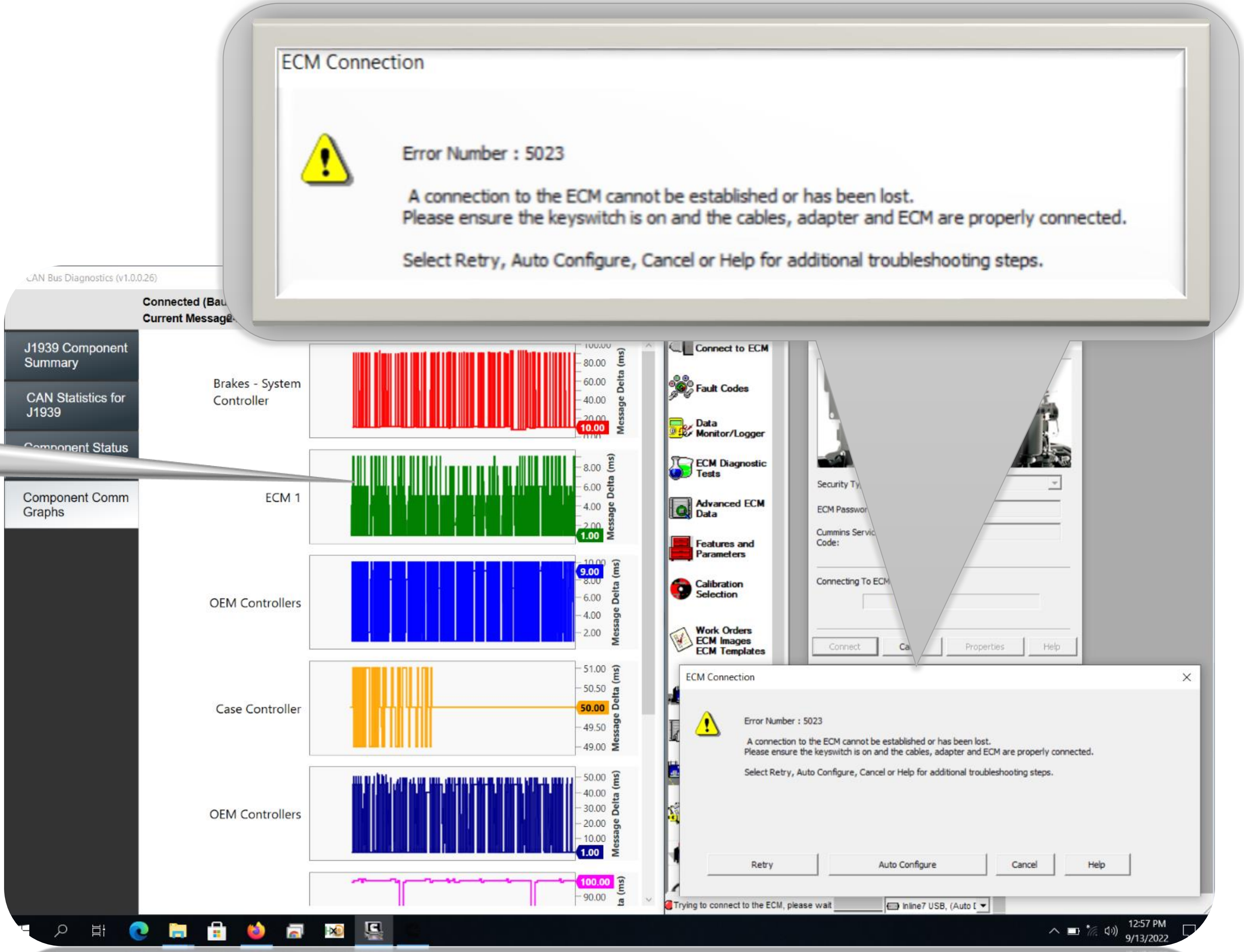


Observation on Testbed 1



Observation on Cummins Diagnostic Tool

ECM activity normal



ECM Connection

Error Number : 5023

A connection to the ECM cannot be established or has been lost.
Please ensure the keyswitch is on and the cables, adapter and ECM are properly connected.

Select Retry, Auto Configure, Cancel or Help for additional troubleshooting steps.

ECM Connection

Error Number : 5023

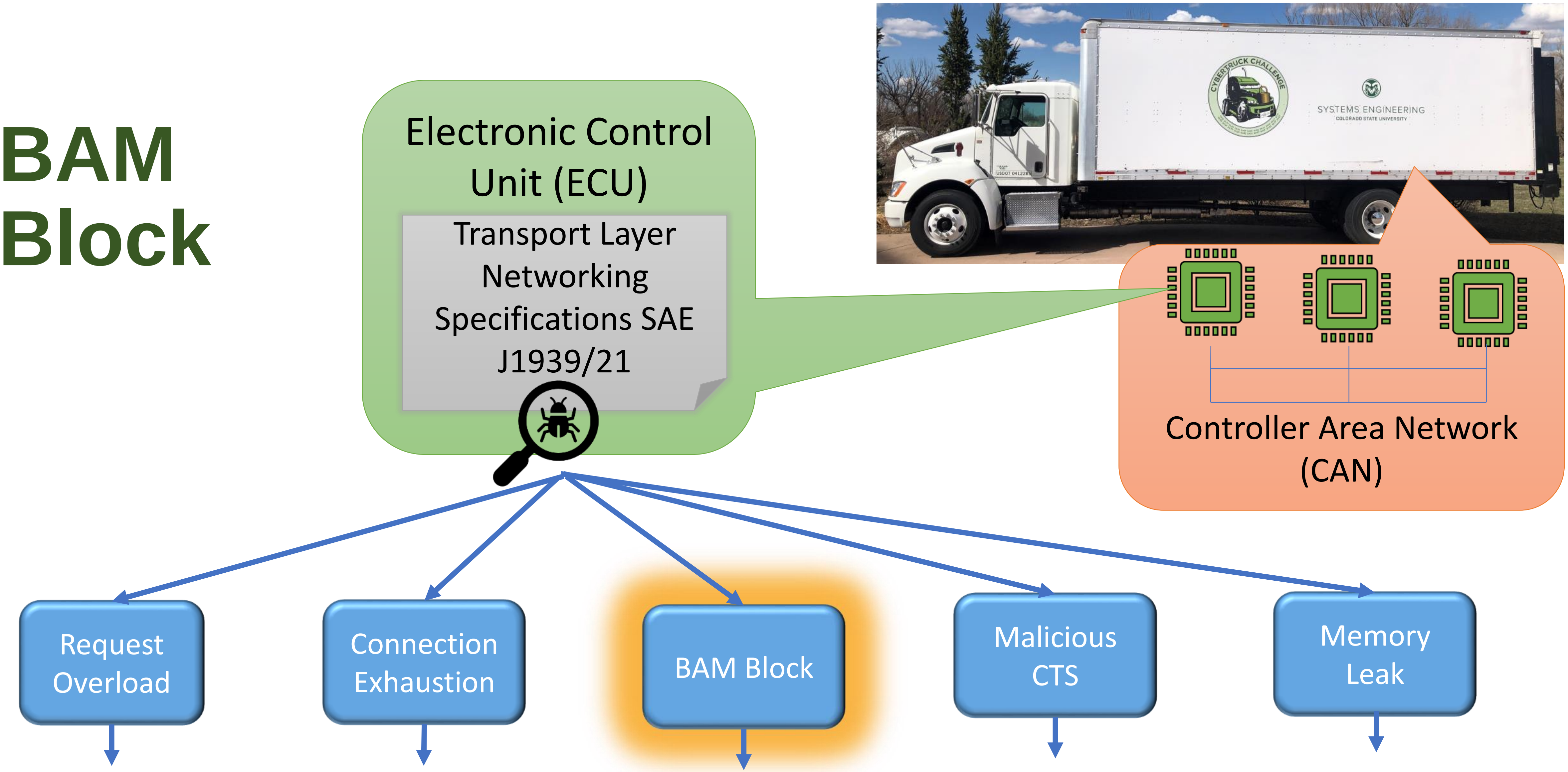
A connection to the ECM cannot be established or has been lost.
Please ensure the keyswitch is on and the cables, adapter and ECM are properly connected.

Select Retry, Auto Configure, Cancel or Help for additional troubleshooting steps.

Trying to connect to the ECM, please wait

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

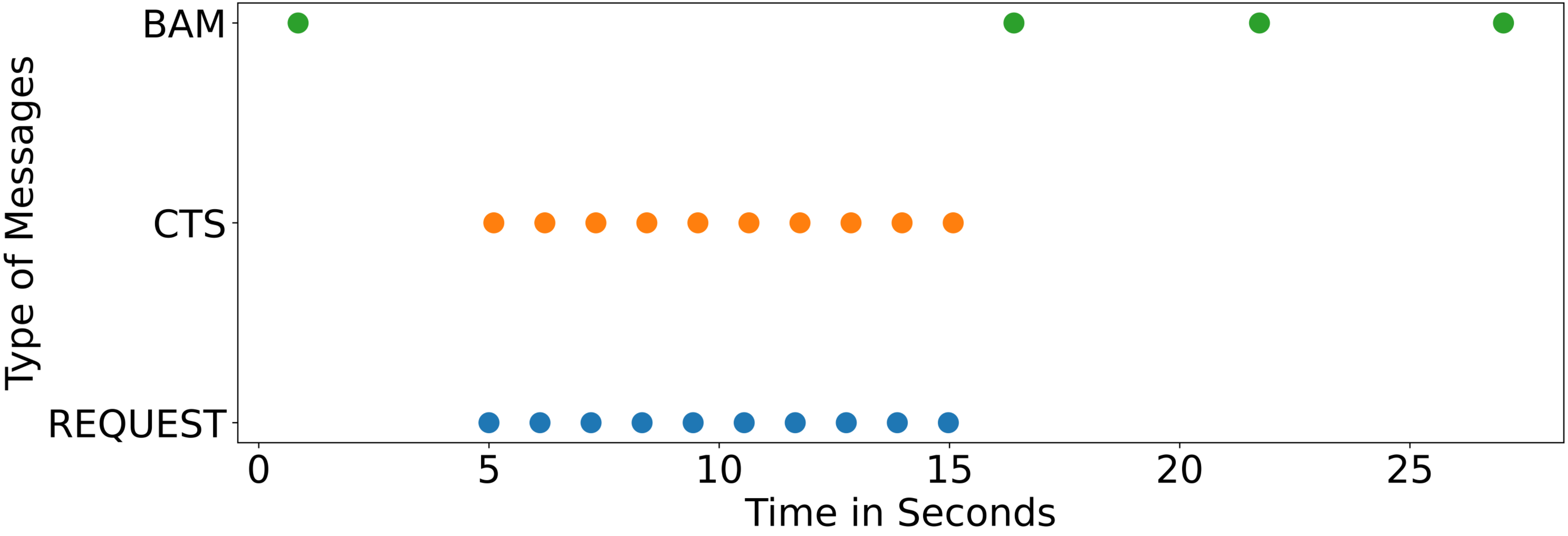
Memory Leak: Reading inaccessible memory on target ECU

Colorado State University

Hypothesis

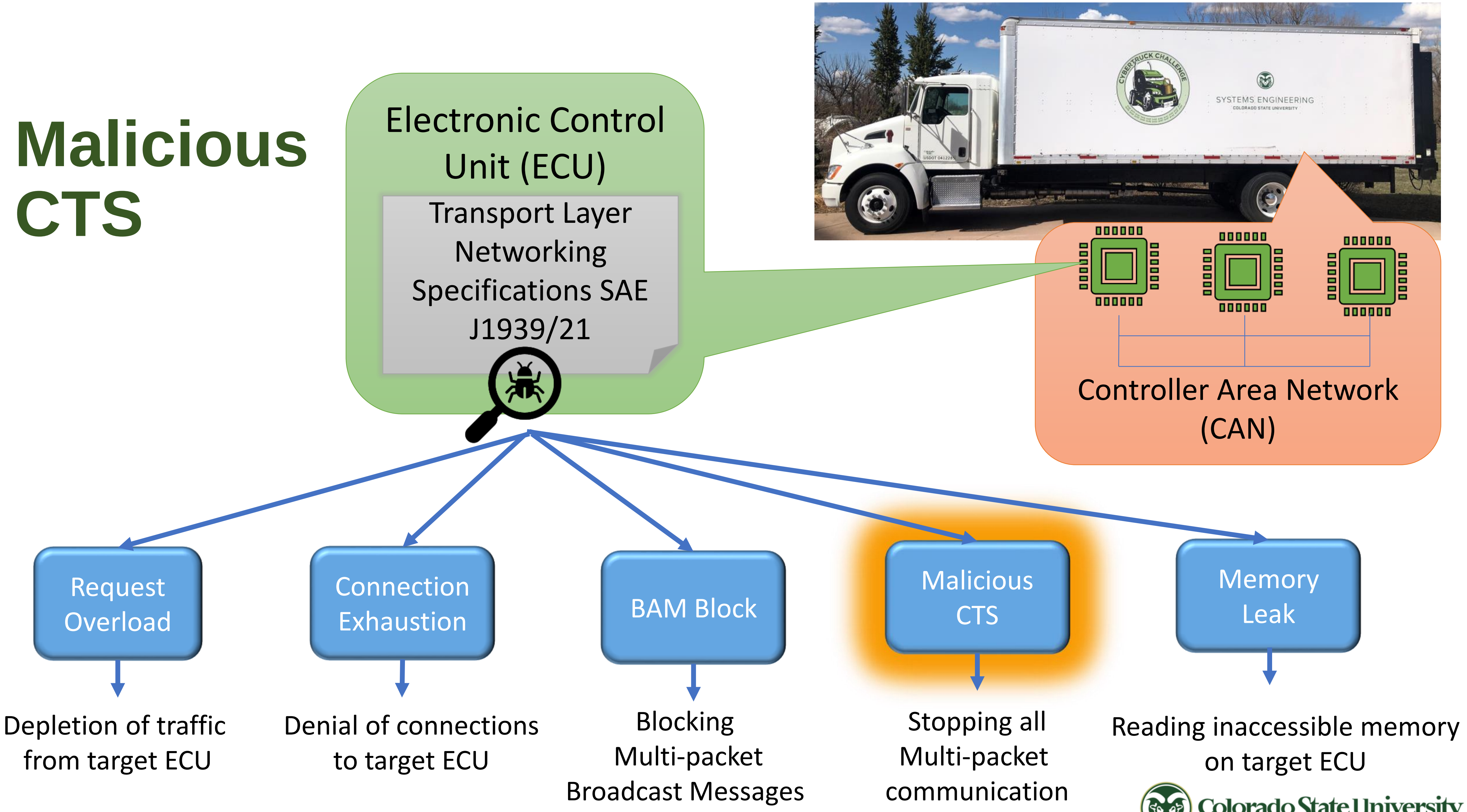
- **Specification**
  - The SAE J1939-21 standard suggests that an ECU must respond to destination-specific requests.
- **Attack**
  - An attack can be constructed whereby an attacker sends destination-specific requests for messages that an ECU broadcasts globally as BAMs with the expectation that this 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



Colorado State University

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

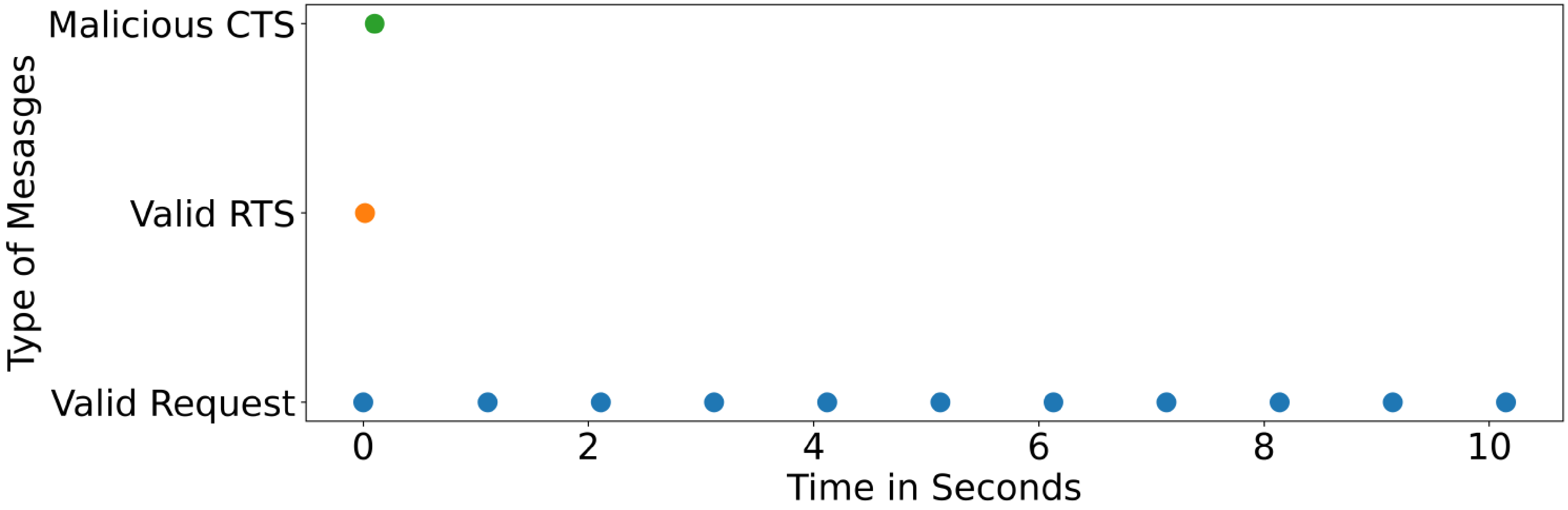
Reading inaccessible memory on target ECU

Colorado State University

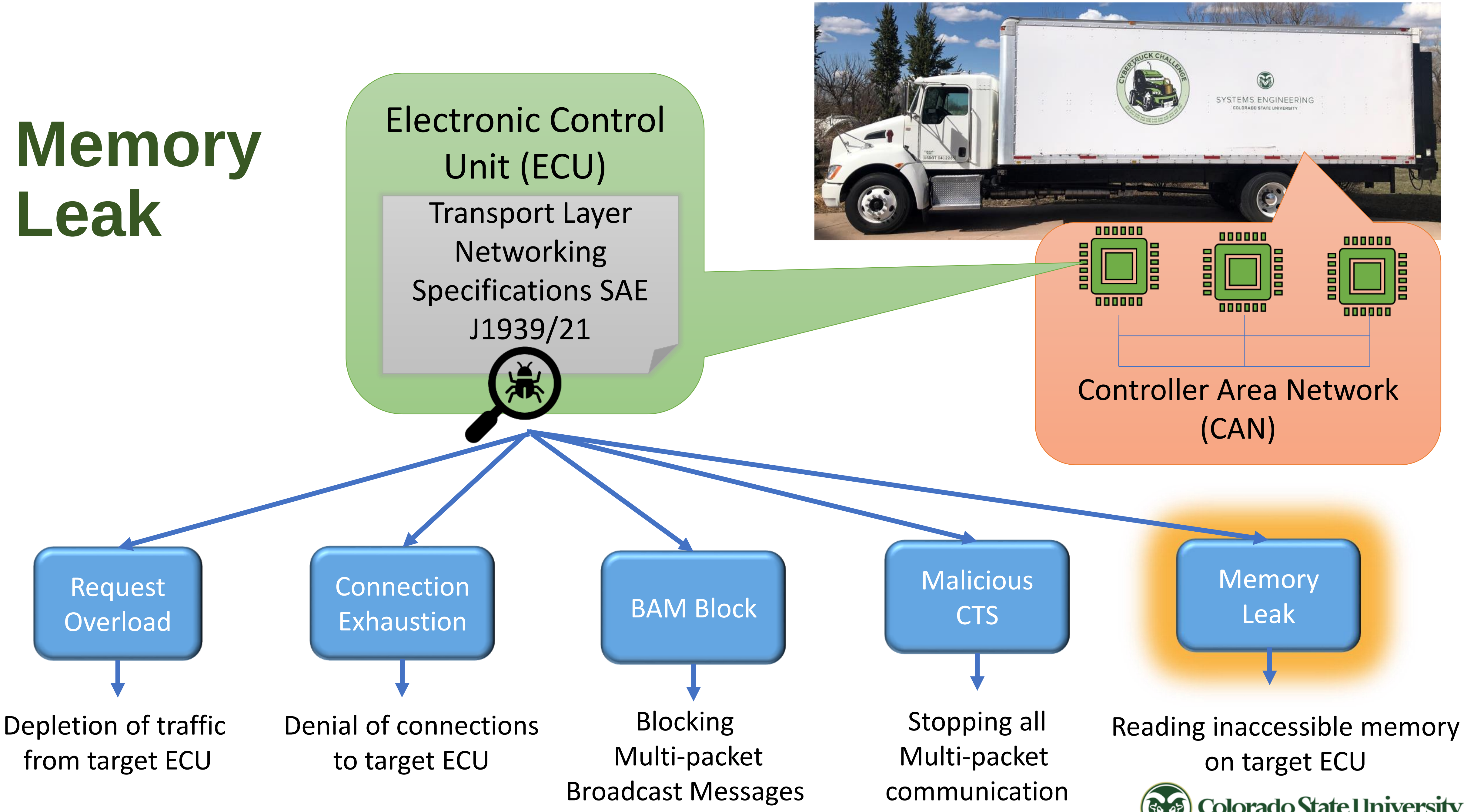
Hypothesis

- **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



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

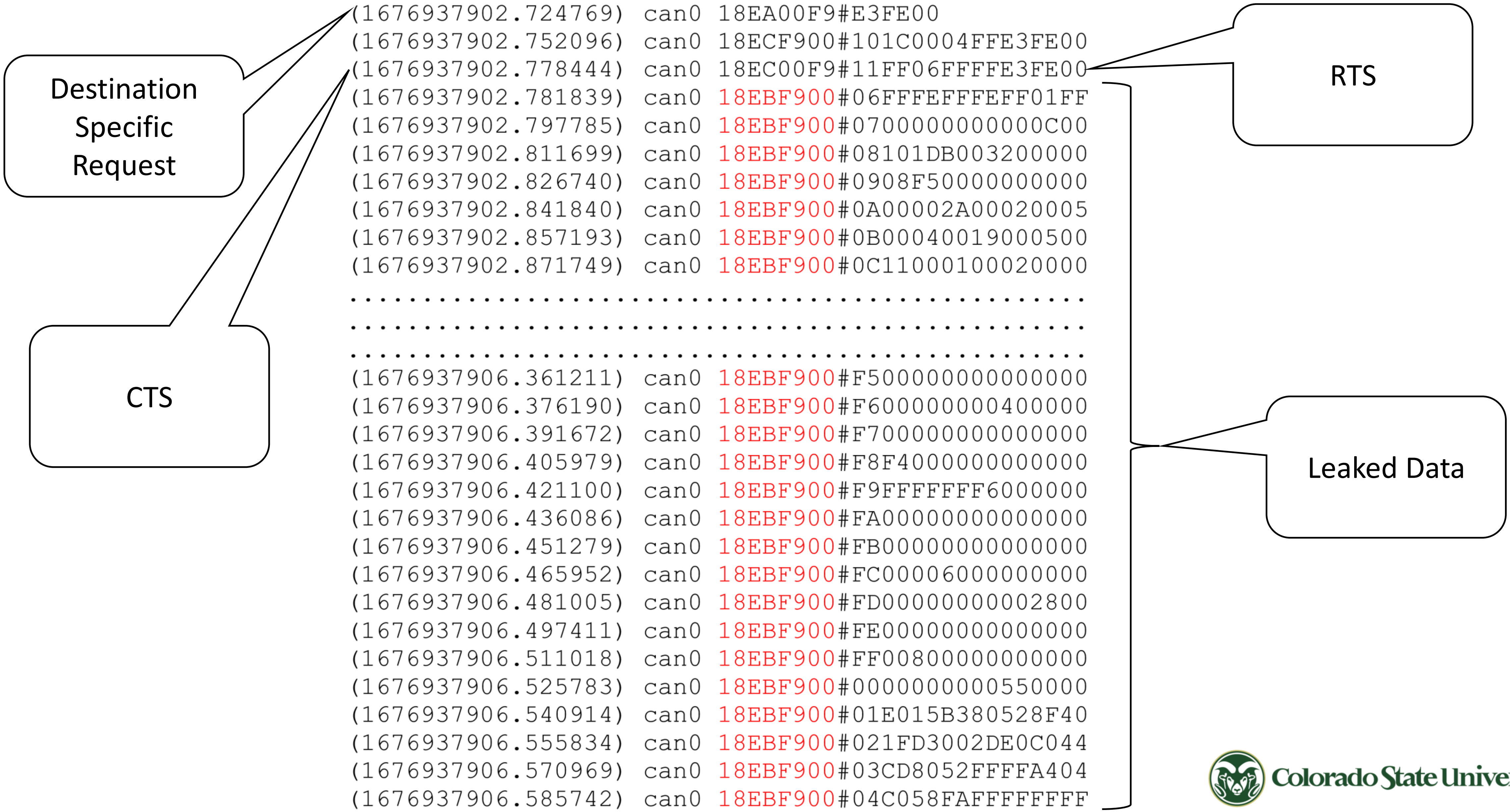
Reading inaccessible memory on target ECU

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



```
(1676937902.724769) can0 18EA00F9#E3FE00
(1676937902.752096) can0 18ECF900#101C0004FFE3FE00
(1676937902.778444) can0 18EC00F9#11FF06FFFFE3FE00
(1676937902.781839) can0 18EBF900#06FFFEFFFEFF01FF
(1676937902.797785) can0 18EBF900#0700000000000C00
(1676937902.811699) can0 18EBF900#08101DB003200000
(1676937902.826740) can0 18EBF900#0908F50000000000
(1676937902.841840) can0 18EBF900#0A00002A00020005
(1676937902.857193) can0 18EBF900#0B00040019000500
(1676937902.871749) can0 18EBF900#0C11000100020000
.................................................
.................................................
.................................................
(1676937906.361211) can0 18EBF900#F500000000000000
(1676937906.376190) can0 18EBF900#F600000000400000
(1676937906.391672) can0 18EBF900#F700000000000000
(1676937906.405979) can0 18EBF900#F8F4000000000000
(1676937906.421100) can0 18EBF900#F9FFFFFFF6000000
(1676937906.436086) can0 18EBF900#FA00000000000000
(1676937906.451279) can0 18EBF900#FB00000000000000
(1676937906.465952) can0 18EBF900#FC00006000000000
(1676937906.481005) can0 18EBF900#FD00000000002800
(1676937906.497411) can0 18EBF900#FE00000000000000
(1676937906.511018) can0 18EBF900#FF00800000000000
(1676937906.525783) can0 18EBF900#0000000000550000
(1676937906.540914) can0 18EBF900#01E015B380528F40
(1676937906.555834) can0 18EBF900#021FD3002DE0C044
(1676937906.570969) can0 18EBF900#03CD8052FFFFA404
(1676937906.585742) can0 18EBF900#04C058FAFFFFFFFF
```

Conclusion

- This paper presents five different scenarios where ECUs on SAE J1939 networks are subjected to different types of attacks
- First, two of the five scenarios demonstrate validations of attacks discovered in prior literature. The validation incorporates a more comprehensive testing setup. The latter three scenarios demonstrate new attack cases.
- Each of these attacks exploits specifications from the SAE J1939 protocol standards.
- At its core, this paper helps in enhancing the existing threatscape of vehicle security for medium and heavy-duty vehicles.

Thank you

Colorado State University

Questions ?