In-ComVec Sec: In-vehicle Security for Medium and Heavy Duty Vehicles

Subhojeet Mukherjee

Advisor: Dr. Indrakshi Ray, Dr. Indrajit Ray

Computer Science Department

Colorado State University

Introduction

Why In-ComVec Sec

Transport goods worth about $53 billion were moved each day in 2015

- Financially motivated attacks.

Emergency vehicle response time is critical

- Personally motivated attacks.

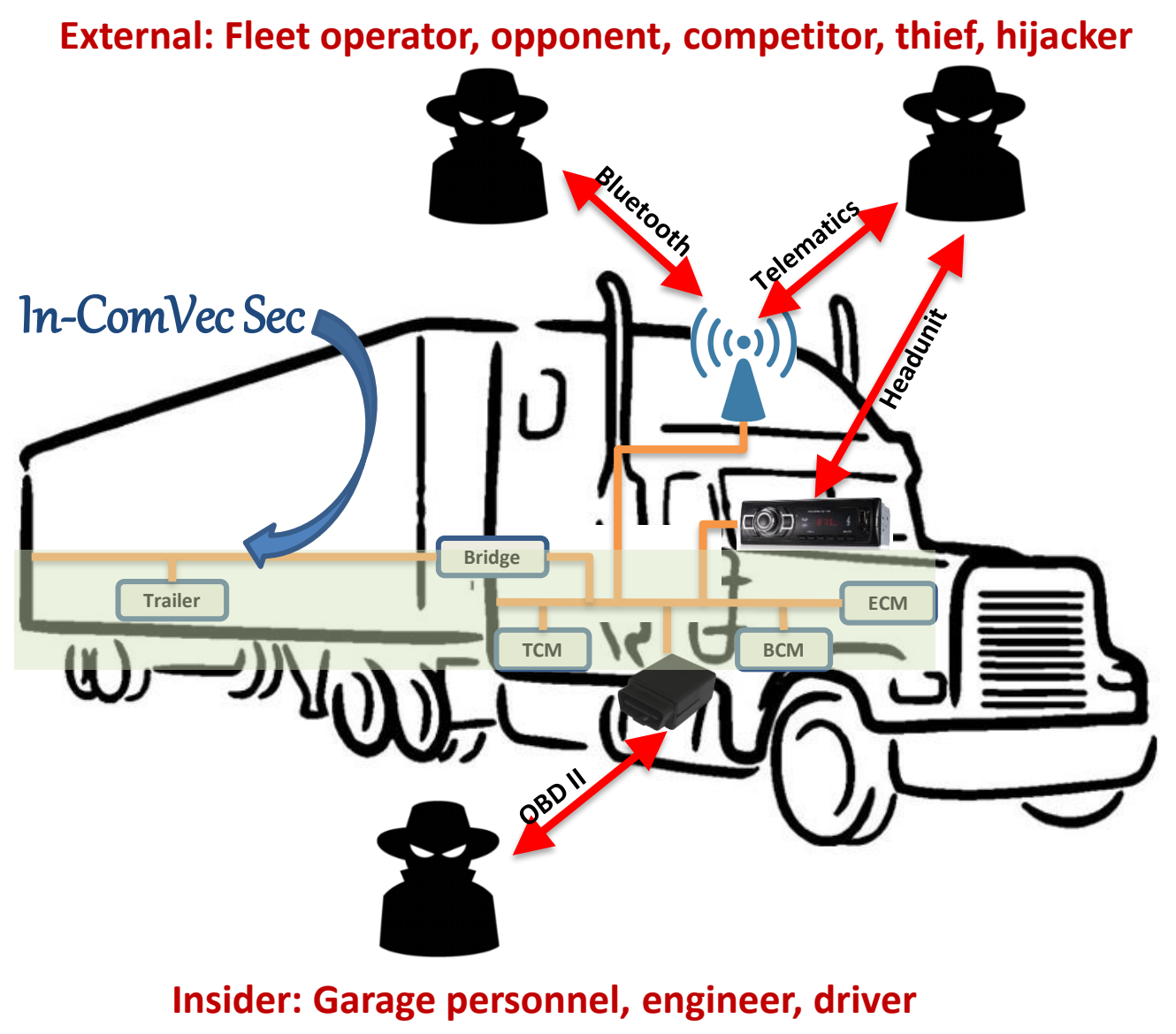
Capital equipment bear high asset value

- Commercially motivated attacks.

Military vehicles are mission critical

- Politically motivated attacks.

Mechatronic Threats: Our Scope



External: Fleet operator, opponent, competitor, thief, hijacker
In-ComVec Sec
Bluetooth
Telematics
Headunit
Bridge
Trailer
TCM
BCM
ECM
OBD II
Insider: Garage personnel, engineer, driver

Electronic control units (ECU) communicate over the 2-wire CAN bus

- Make informed decisions.
- Enhanced reliability, quality and safety.
- Messages composed and interpreted according to SAE J1939 standards.

Existing flaws in ECU and external connectivity can be exploited

- Direct access to critical ECUs via CAN bus can be threatening.

A Novel Research Topic

Passenger car security was perceived towards the middle of last decade

- 1.4 million Jeep cars recalled in 2015.
- Significant amount of security research on CAN since 2004.

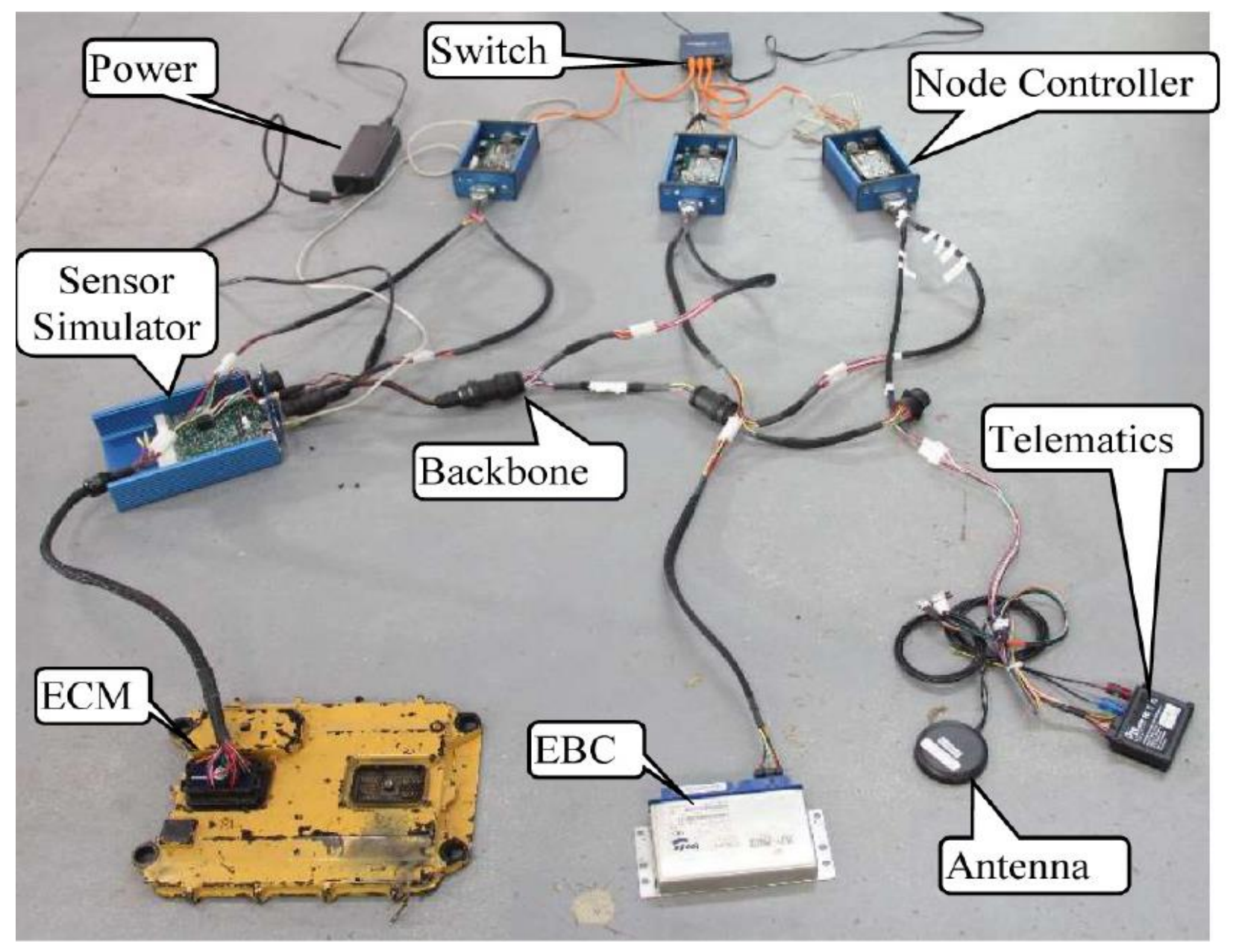
Heavy vehicles are different…

- Attacking SAE J1939, a common standard, can have large-scale impact.
- Non-proprietary standards on actively changing networks.
- Greater automation and external access.

New, possibly unknown threats are likely.

Highly adaptive, and possibly novel security solutions are required.

Prepare @SAE Comvec'16

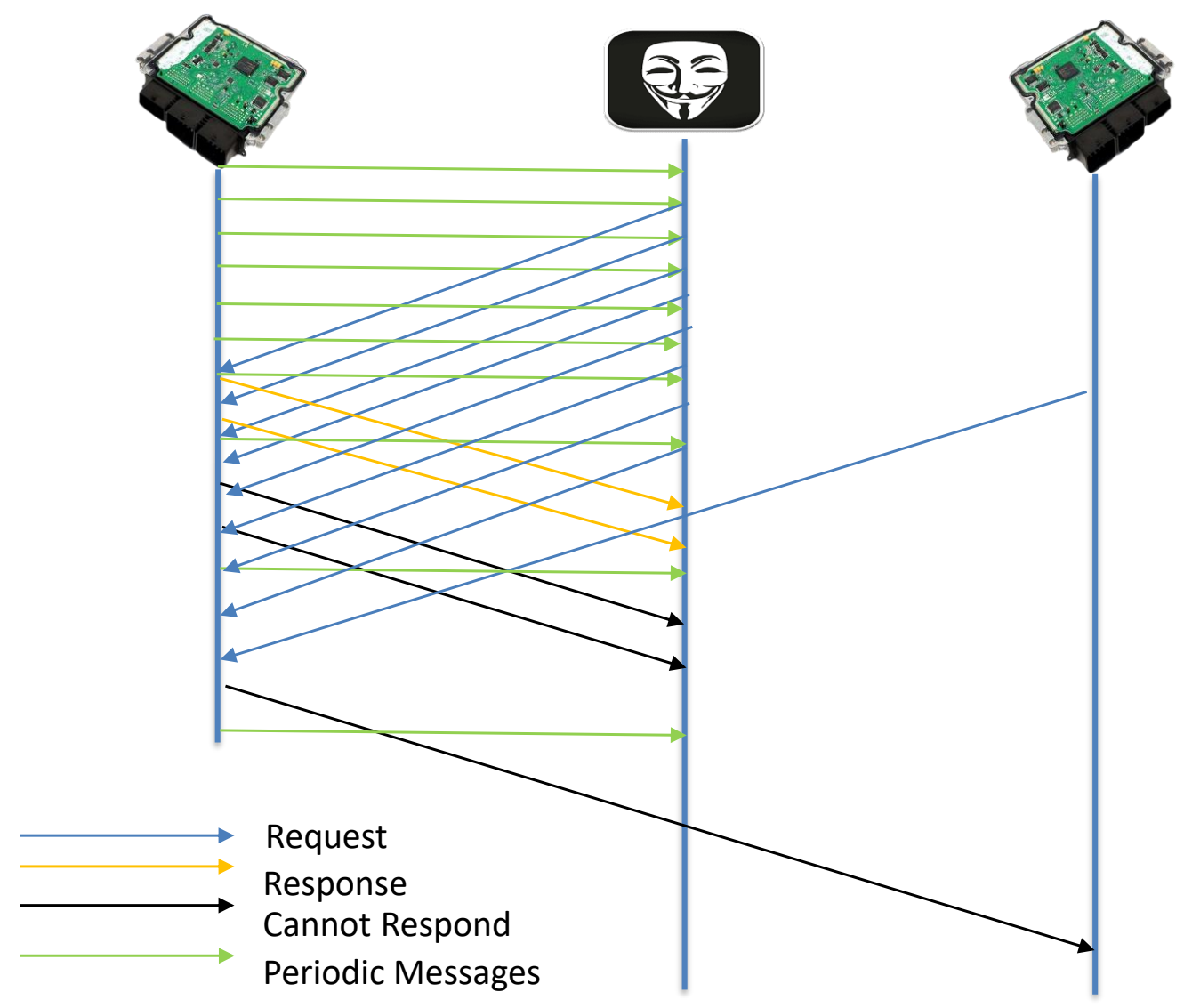


A testbed for conducting sandboxed heavy vehicle security research

- Nodes connected to the network
  - Engine and retarder controller.
  - Brake controller
  - Telematics unit
  - Beaglebone node controllers.
- **Remote access.**
  - Allows access to a CAN backbone.

Invade @ICISS '16

Request Overload



Issue

- Network nodes will process all requests directed to them [SAE J1939-21].

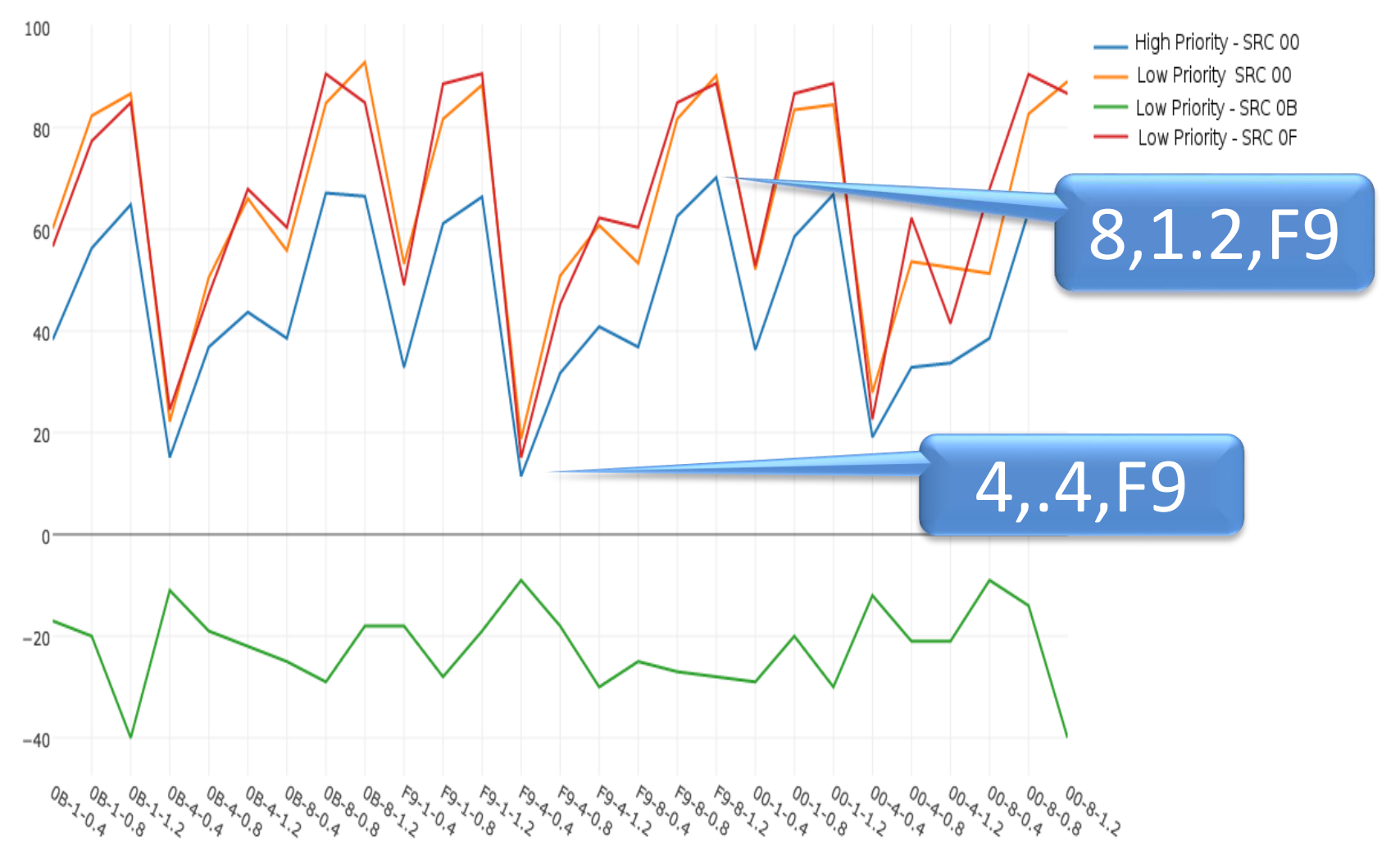
Attack

- Bombard a node with multiple requests.

Impact

- Node stops functioning.
- Replies back with *cannot respond*.
- Periodic messages decrease drastically.

Succesfully executed on a real truck at the 1st Cyber-Truck challenge, Warren, Michigan.



Experiment independent Factors

- number of concurrent thread
- injection time interval in ms
- source address

High Priority messages

- Average drop: 46%

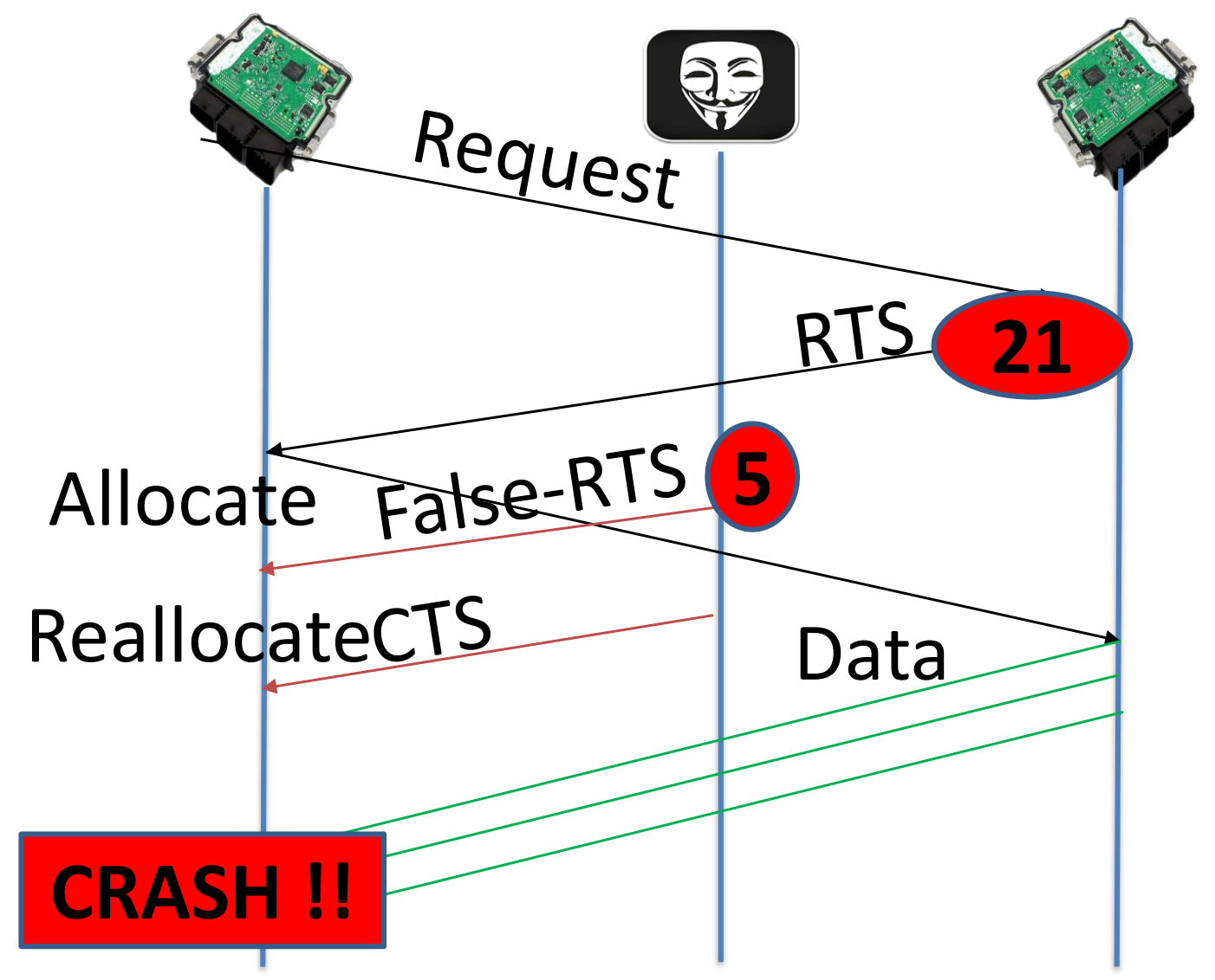
Low Priority Messages

- Average drop: 65 %

Two-tailed Mann-Whitney U test

- p-value of 0.01468 (<= .5)
- 5% confidence interval

False RTS



Issue

- During connection set-up a RTS can be sent to the recipient with piggybacked message size [SAE J1939-21].
- If a new RTS is sent, it shall be acted upon.
- No notification is sent back to the original sender.

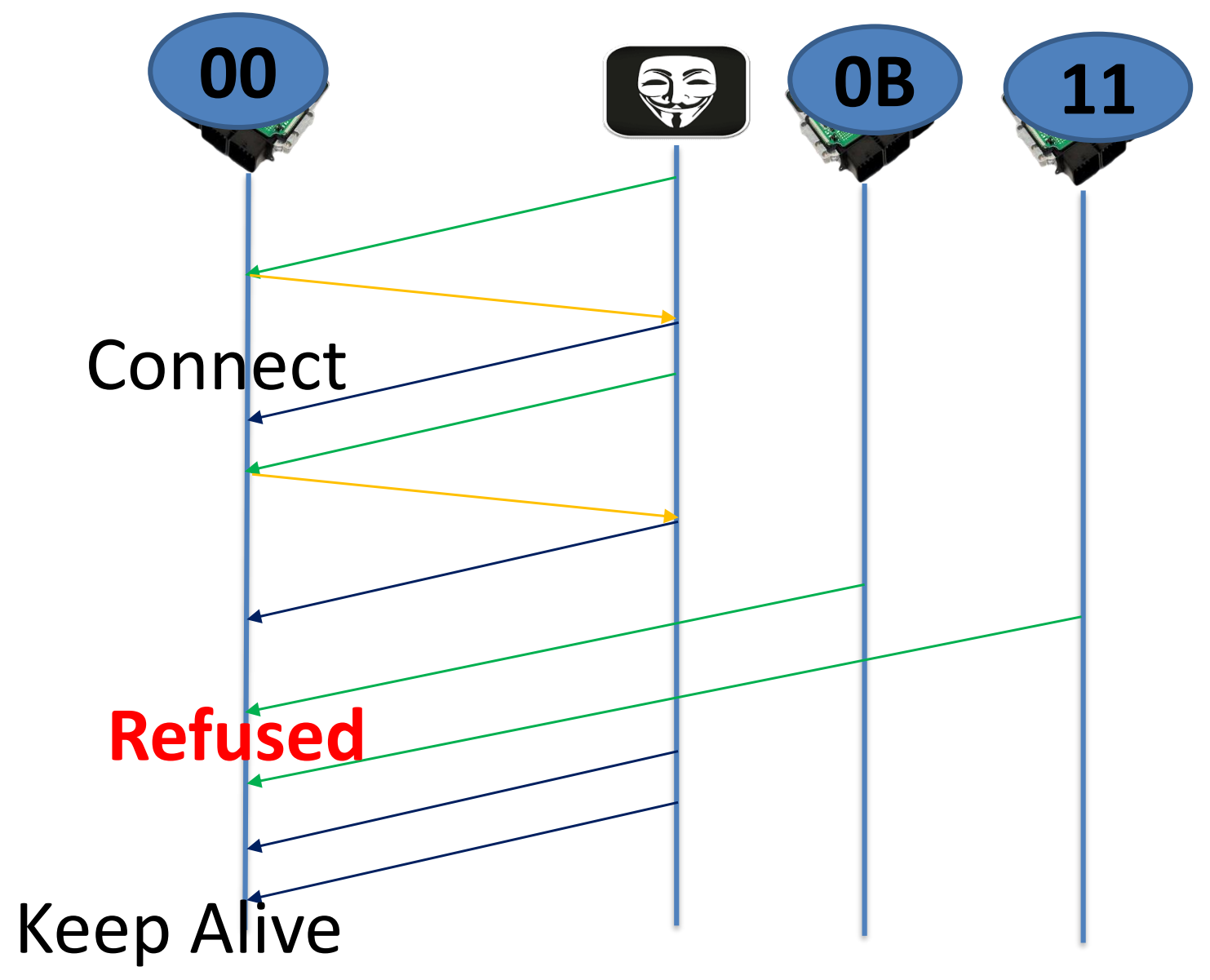
Attack

- Send false RTS with reduced message size.

Impact

- Possible buffer overflow.

Connection Exhaustion



Issue

- Only 255 possible addresses.
- Only 1 active connection from a node [SAE J1939-21].
- Connections can be kept alive by sending periodic clear-to-send (CTS).

Attack

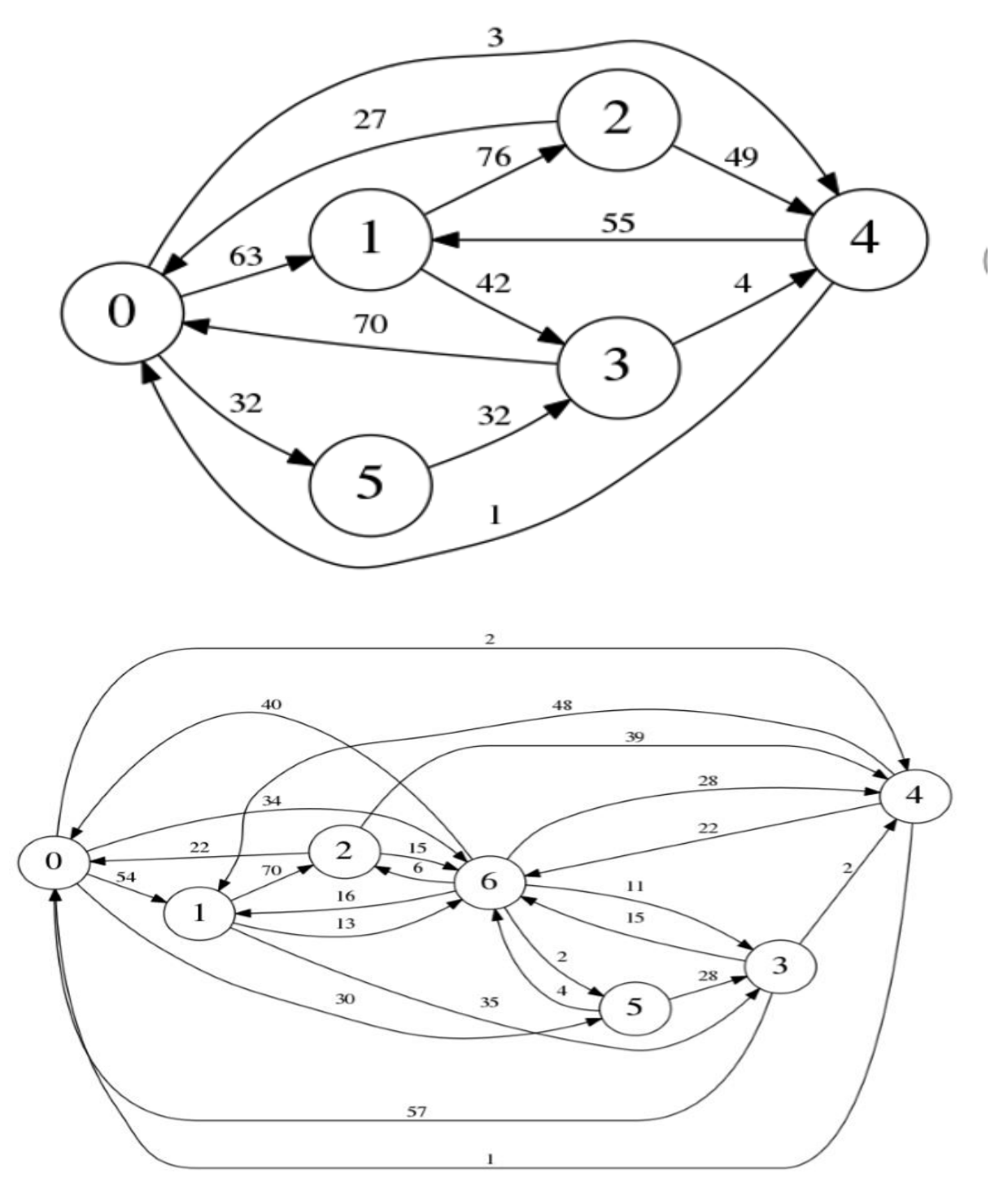
- Masquerade as nodes on the network.
- Make connections.

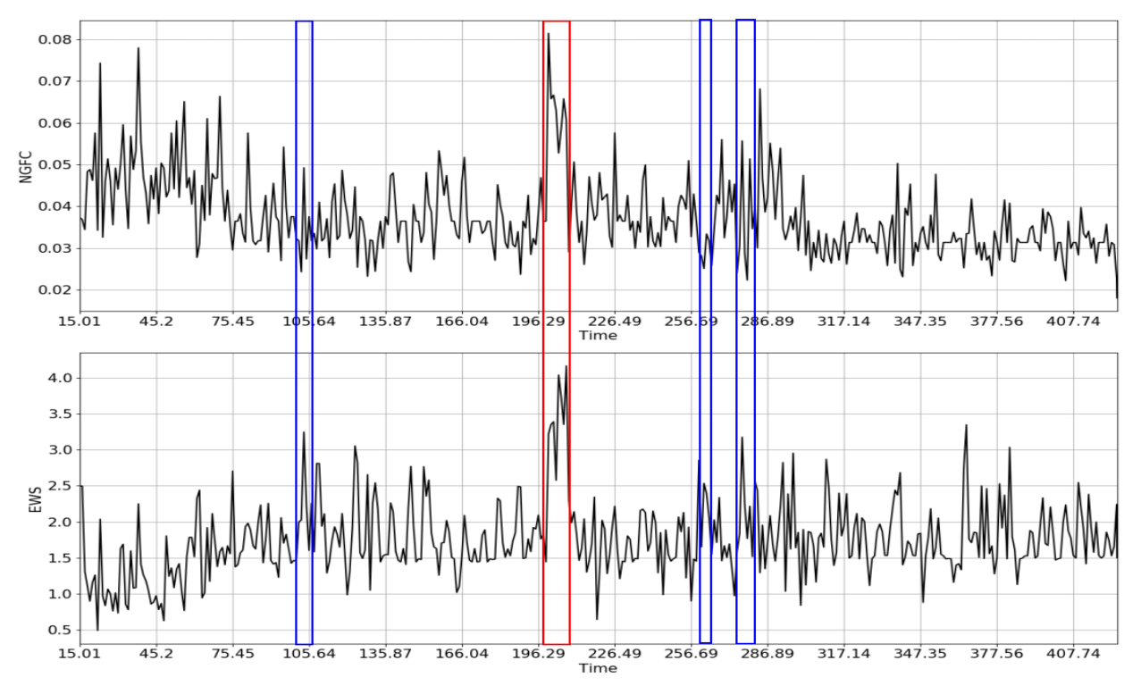
Impact

- Legitimate connections are rejected.

Defend @PST'17, CCS'17

Anomaly-Based Message Injection Detection





Report Precedence Graphs (RPG).

- Reports are basic units of state information derived from one J1939 message.

Erratic, unplanned transitions characterize malicious behavior.

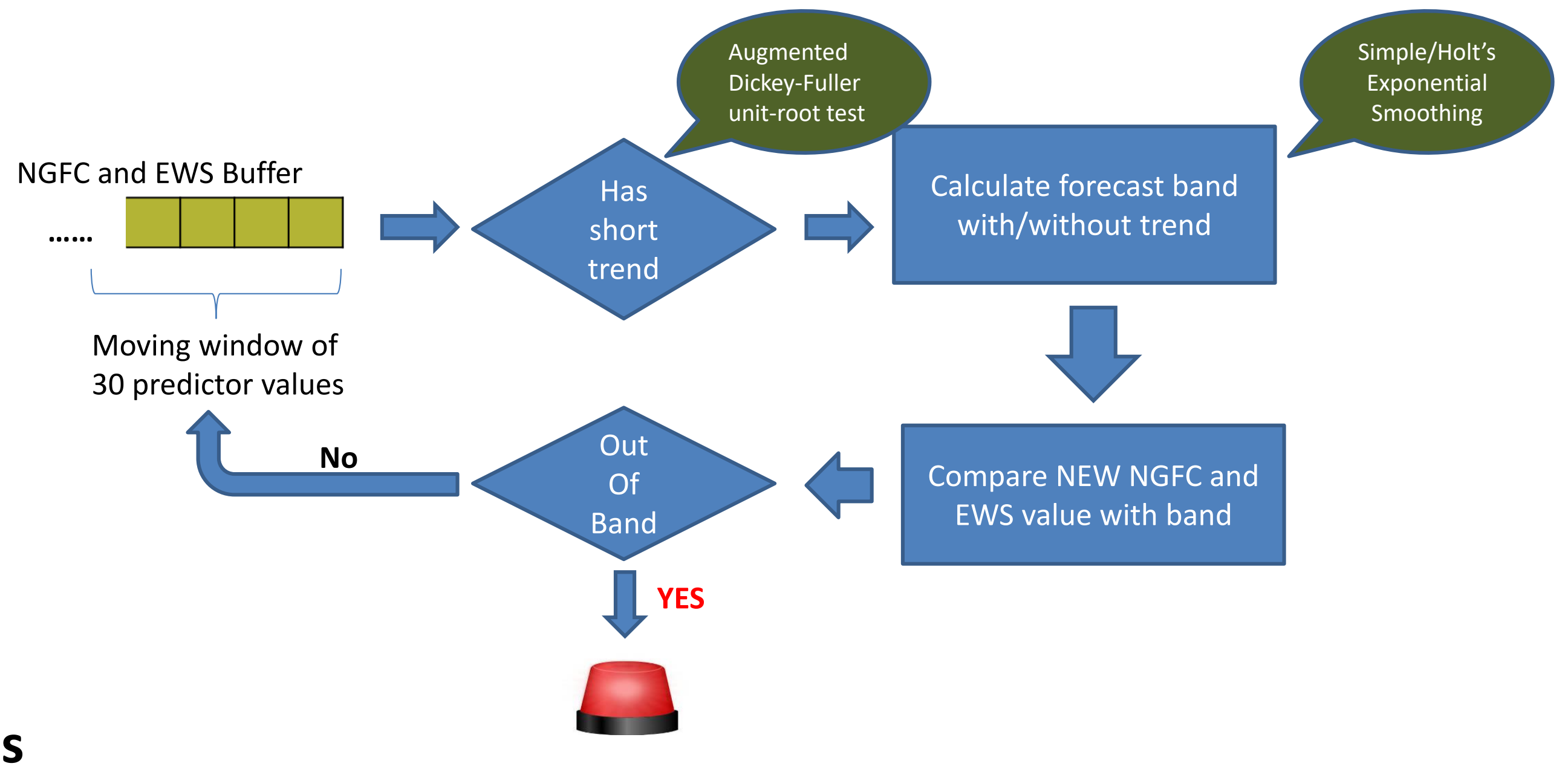
- Hard-barking, tire-slip are anomalous but not malicious.
- Can distinguish such behavior from attacks.

Features

- Normalized Graph Flux Capacity (NGFC)
  - Flux capacity: fc(n) = *in-deg(n)*out-deg(n)*
  - NGFC = $\sum fc(n)/|\{n\}|^3$
- Edge-Weight Distribution Skewness (EWS)

Visualizing anomalous behavior

- Blue box
  - Hard-brake
  - No significant deviation in both features
- Red box
  - Attack
  - Significant deviation in both features



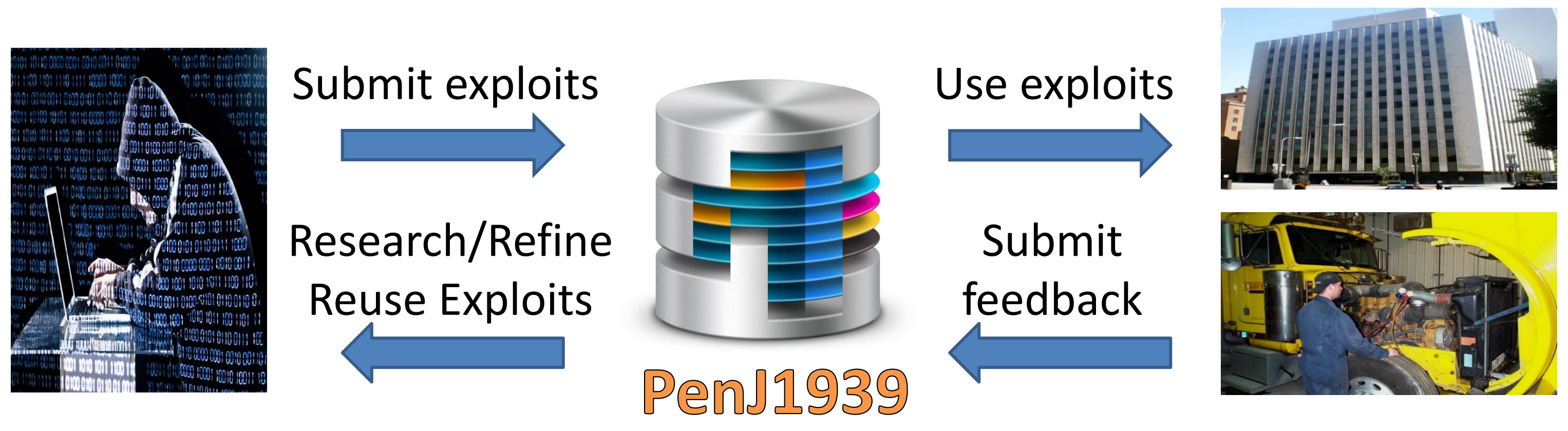
NGFC and EWS Buffer
……
Moving window of 30 predictor values
Has short trend
Augmented Dickey-Fuller unit-root test
Calculate forecast band with/without trend
Simple/Holt's Exponential Smoothing
Compare NEW NGFC and EWS value with band
Out Of Band
No
YES

Results

- Almost 80-90% of injections detected. 60-70% attack windows detected.
- 1-9 % false positive (hard-brake) detection rate.

Vehicle (Attack) State Visualization

Obtain Attack Traffic Patterns



Ongoing and Future Research

Visualize vehicle states

- Vehicle states are distinct combinations of parameter instances.
- Our application realizes states from network traffic.
- Eg. accelerating, hard-braking, malicious message injections etc.

Prevent malicious injections.

- Adapting low power cryptographic approaches.

This work was supported in part by NSF under award numbers CNS 1619641 and CNS 1715458.