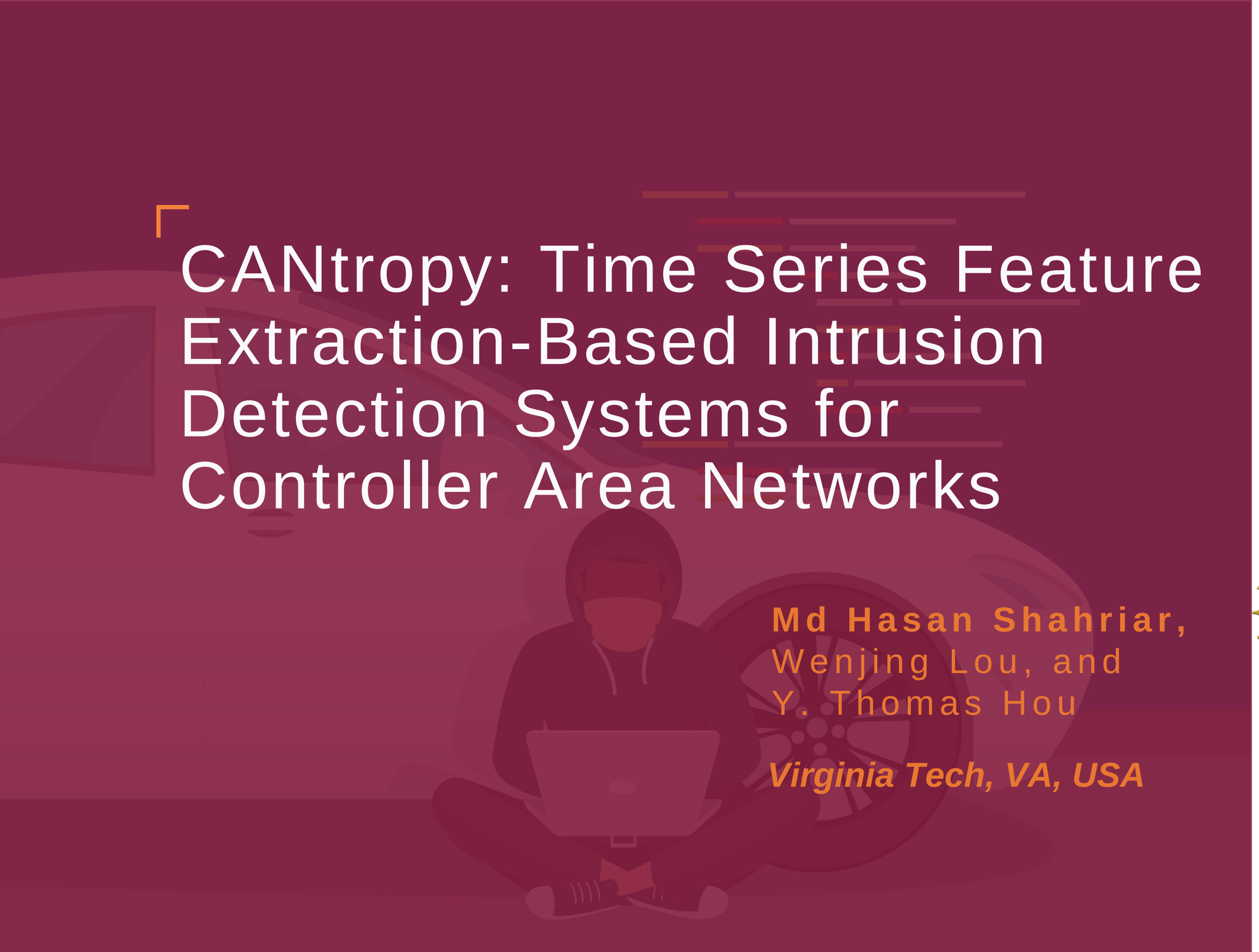
CANtropy: Time Series Feature Extraction-Based Intrusion Detection Systems for Controller Area Networks



Md Hasan Shahriar,
Wenjing Lou, and
Y. Thomas Hou

Virginia Tech, VA, USA

VehicleSec
Symposium on
Vehicle Security & Privacy

VIRGINIA TECH™

NSF

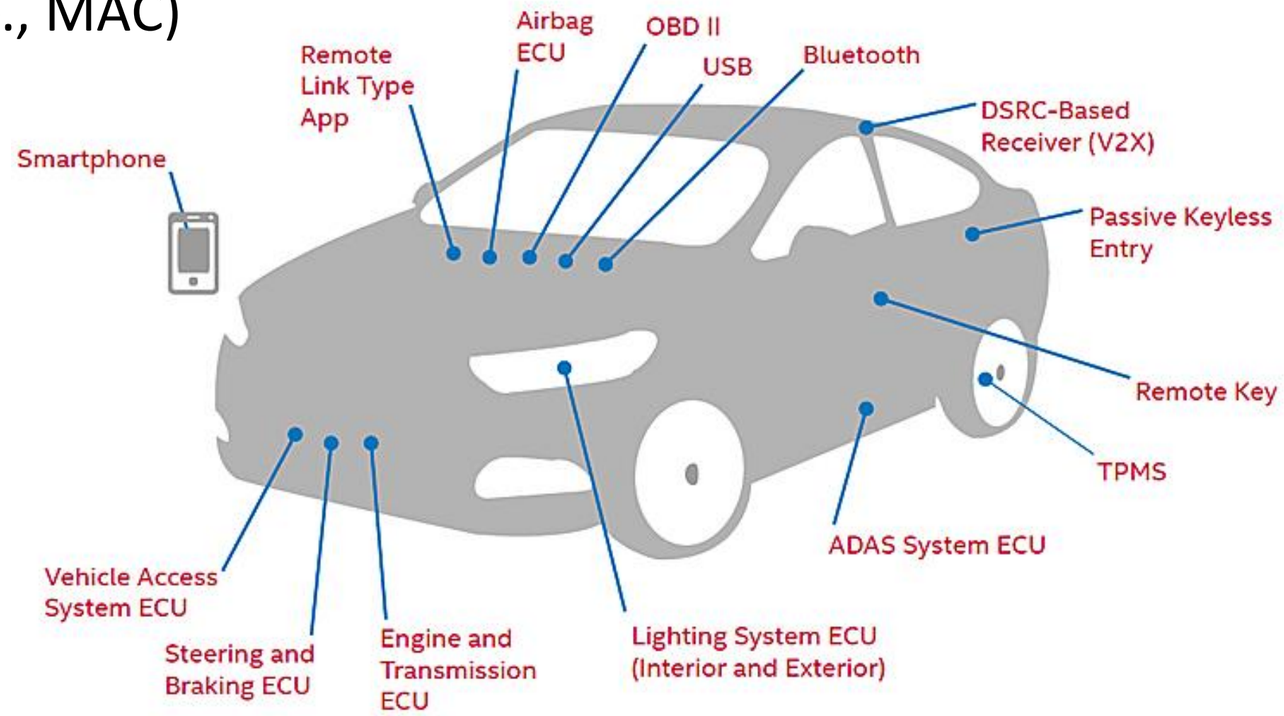
U.S. DEPARTMENT OF HOMELAND SECURITY

Commonwealth
Cyber Initiative

Attack Surface of Modern Vehicles

- 100+ dedicated electronic control units (ECUs)
- Data exchange though controller area networks (CAN) bus
- CAN protocol lacks security requirements (i.e., MAC)
- Hijacked ECUs can lose control of the car
- Example, Jeep hack by Miller and Valasek

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

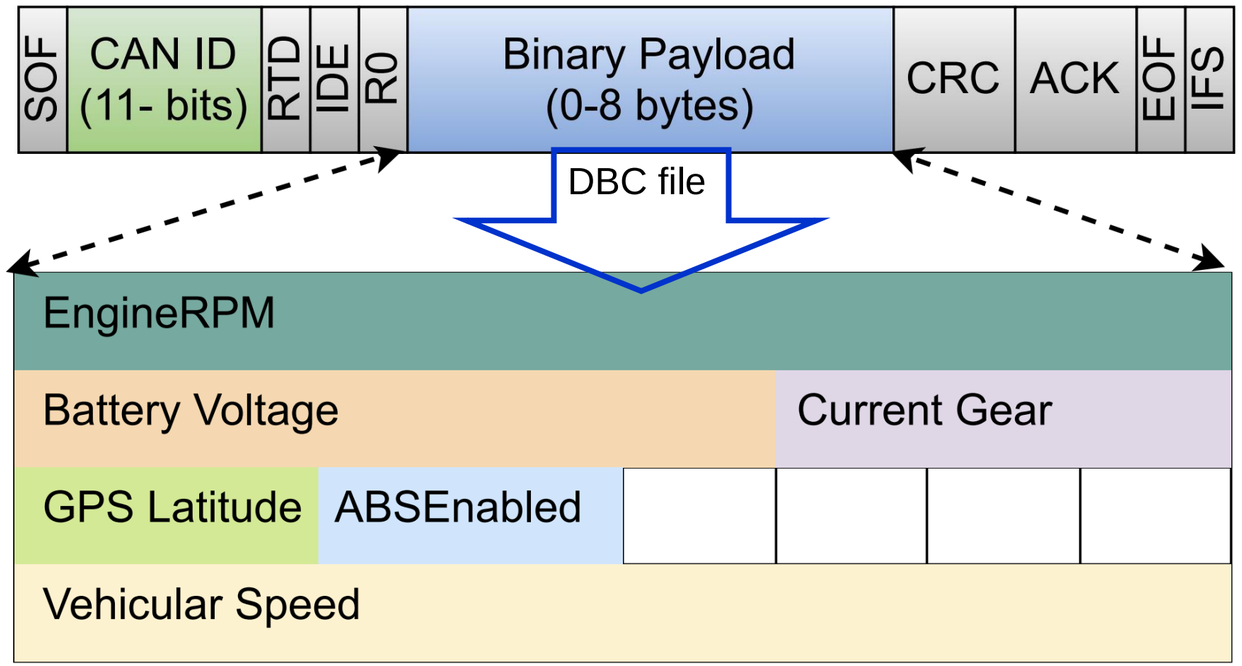


https://www.technologyrecord.com/Article/intel-tackles-security-risks-associated-with-connected-cars-47933

Controller Area Networks

CAN IDS fall into these major categories:

- **Physical Characteristics-based IDS**
  - Uses physical layer attributes (e.g., voltage)
- **CAN ID-based IDS**
  - Timing/sequence of frame arbitration IDs
- **Payload-based IDS**
  - Considers the data frame as a string of raw bits
- **<u>Signal-based IDS</u>**
  - **<u>Decodes raw binary bits to time-series signals</u>**
  - **<u>Uses time series of signal values as inputs</u>**

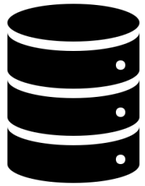


Decoded signals of four consecutive payloads

www.hackday.com/2013/10/22/can-hacking-the-in-vehicle-network/

Motivations

Limitations of Deep Learning based Signal-Level IDS

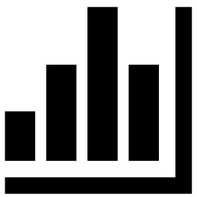


High Quality and
High Volume of Data

Optimized DL Model
(Grid-search Approach)

Powerful Computational
Platform

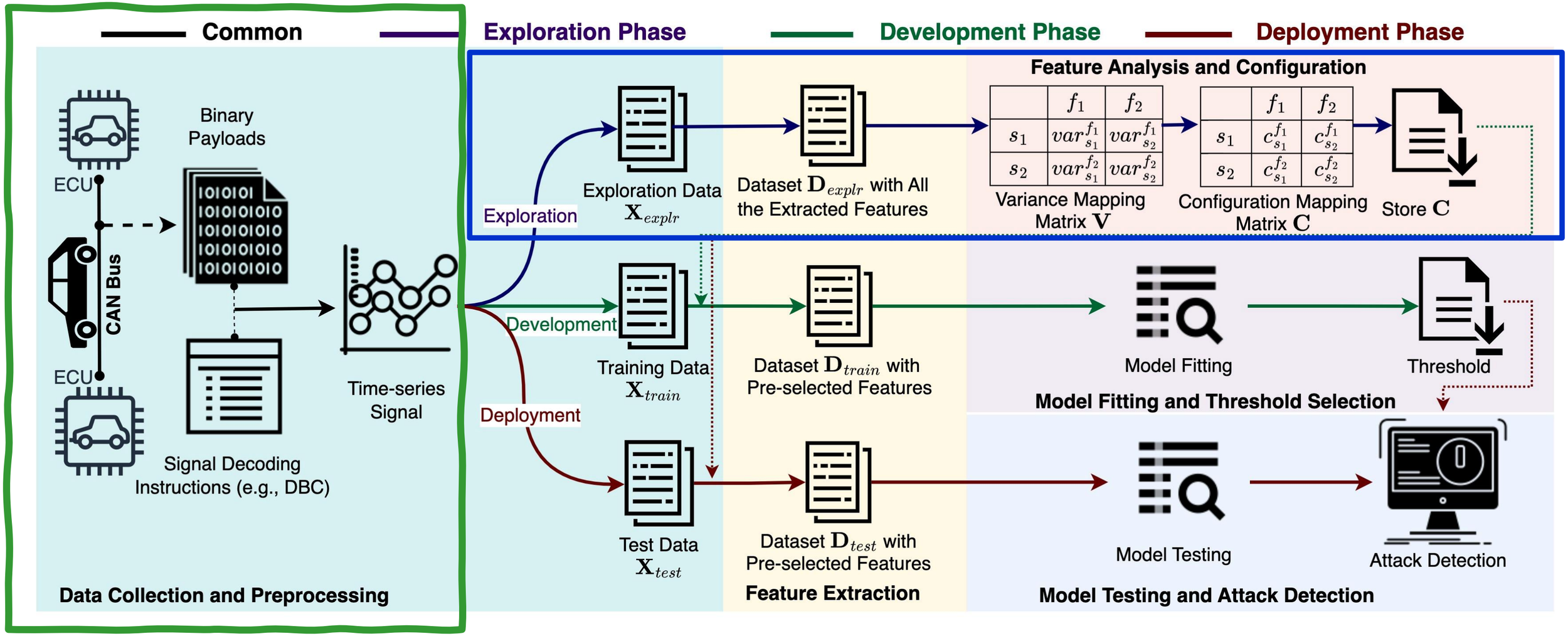
Limitations of Feature Extraction-based Signal-Level IDS



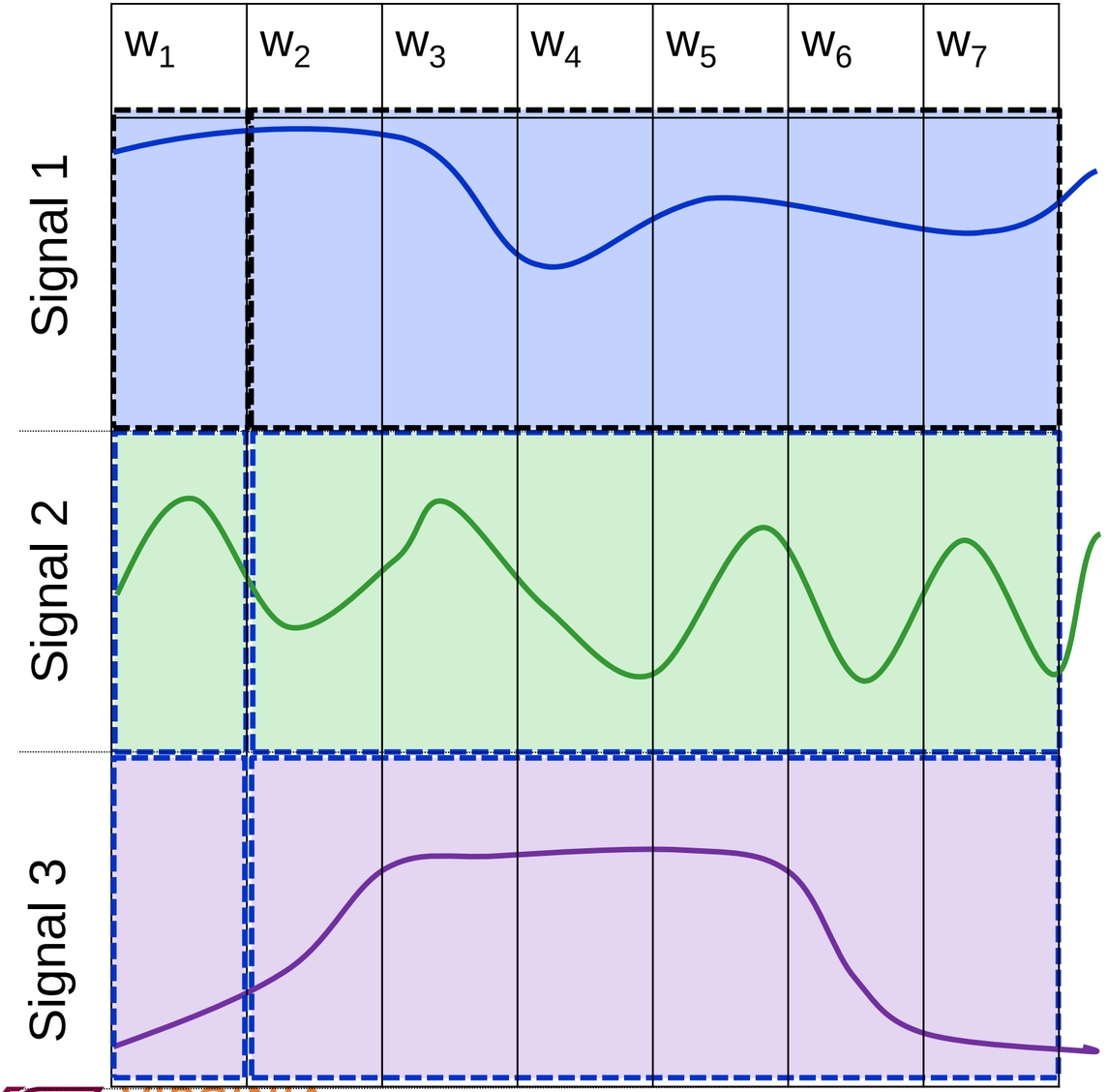
Limited Exploration in
Feature Functions

Extraction of
Unnecessary Features

An Overview of CANtropy



Exploration Phase: Feature Extraction



	w_1	w_2	w_3	w_4	w_5	w_6	w_7
Features of S_1	s_1f_1	✓	✓	✓	✓	✓	✓	✓
	s_1f_2	✓	✓	✓	✓	✓	✓	✓
	s_1f_3	✓	✓	✓	✓	✓	✓	✓
Features of S_2	s_2f_1	✓	✓	✓	✓	✓	✓	✓
	s_2f_2	✓	✓	✓	✓	✓	✓	✓
	s_2f_3	✓	✓	✓	✓	✓	✓	✓
Features of S_3	s_3f_1	✓	✓	✓	✓	✓	✓	✓
	s_3f_2	✓	✓	✓	✓	✓	✓	✓
	s_3f_3	✓	✓	✓	✓	✓	✓	✓

VIRGINIA TECH

Exploration Phase: Feature Analysis & Configuration

	w_1	w_2	w_3	w_4	w_5	w_6	w_7
s_1f_1	✓	✓	✓	✓	✓	✓	✓
s_1f_2	✓	✓	✓	✓	✓	✓	✓
s_1f_3	✓	✓	✓	✓	✓	✓	✓
s_2f_1	✓	✓	✓	✓	✓	✓	✓
s_2f_2	✓	✓	✓	✓	✓	✓	✓
s_2f_3	✓	✓	✓	✓	✓	✓	✓
s_3f_1	✓	✓	✓	✓	✓	✓	✓
s_3f_2	✓	✓	✓	✓	✓	✓	✓
s_3f_3	✓	✓	✓	✓	✓	✓	✓

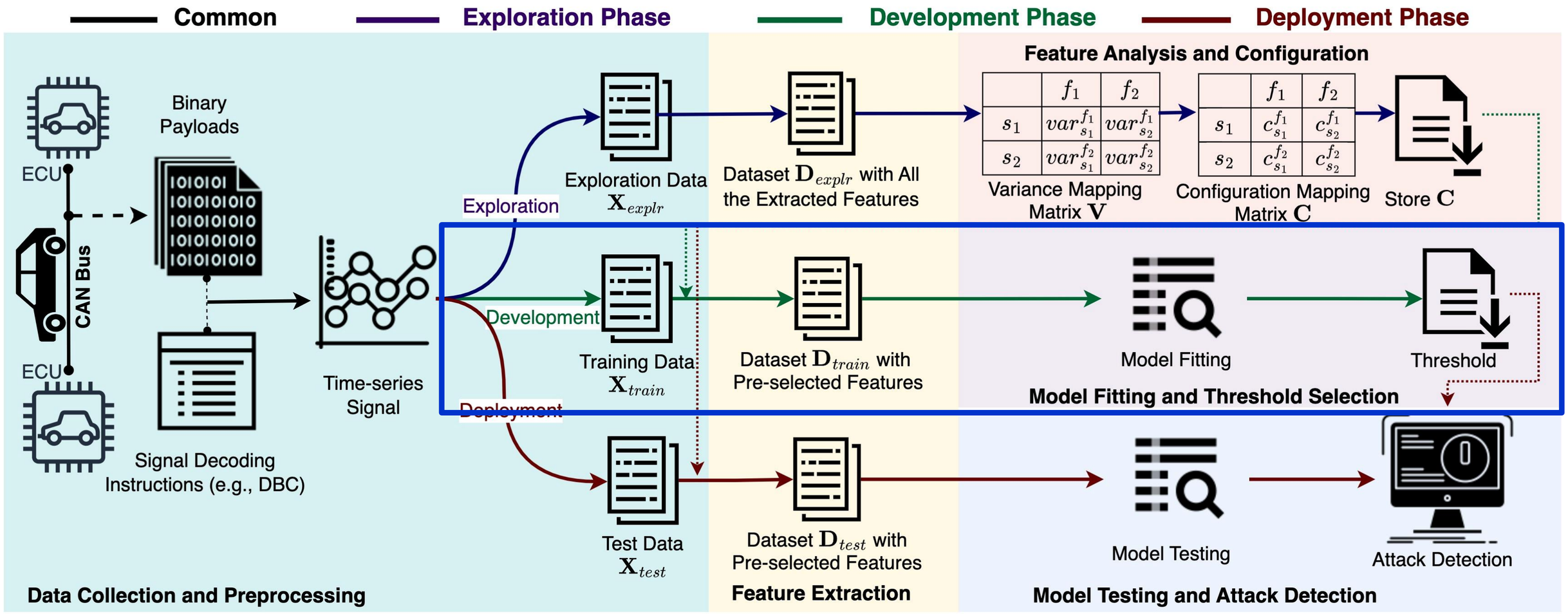
	f_1	f_2	f_3
s_1	●	●	●
s_2	●	●	●
s_3	●	●	●

Variance Mapping Matrix, V

	f_1	f_2	f_3
s_1	●	×	●
s_2	×	●	●
s_3	●	●	×

Configuration Mapping Matrix, C

An Overview of CANtropy



Development Phase: Feature Extraction & Model Fitting

	f_1	f_2	f_3
s_1	●	×	●
s_2	×	●	●
s_3	●	●	×

Configuration Mapping Matrix, C

	w_1	w_2	w_3	w_4	w_5	w_6	w_7
s_1f_1	✓	✓	✓	✓	✓	✓	✓
s_1f_2							
s_1f_3	✓	✓	✓	✓	✓	✓	✓
s_2f_1							
s_2f_2	✓	✓	✓	✓	✓	✓	✓
s_2f_3	✓	✓	✓	✓	✓	✓	✓
s_3f_1	✓	✓	✓	✓	✓	✓	✓
s_3f_2	✓	✓	✓	✓	✓	✓	✓
s_3f_3							

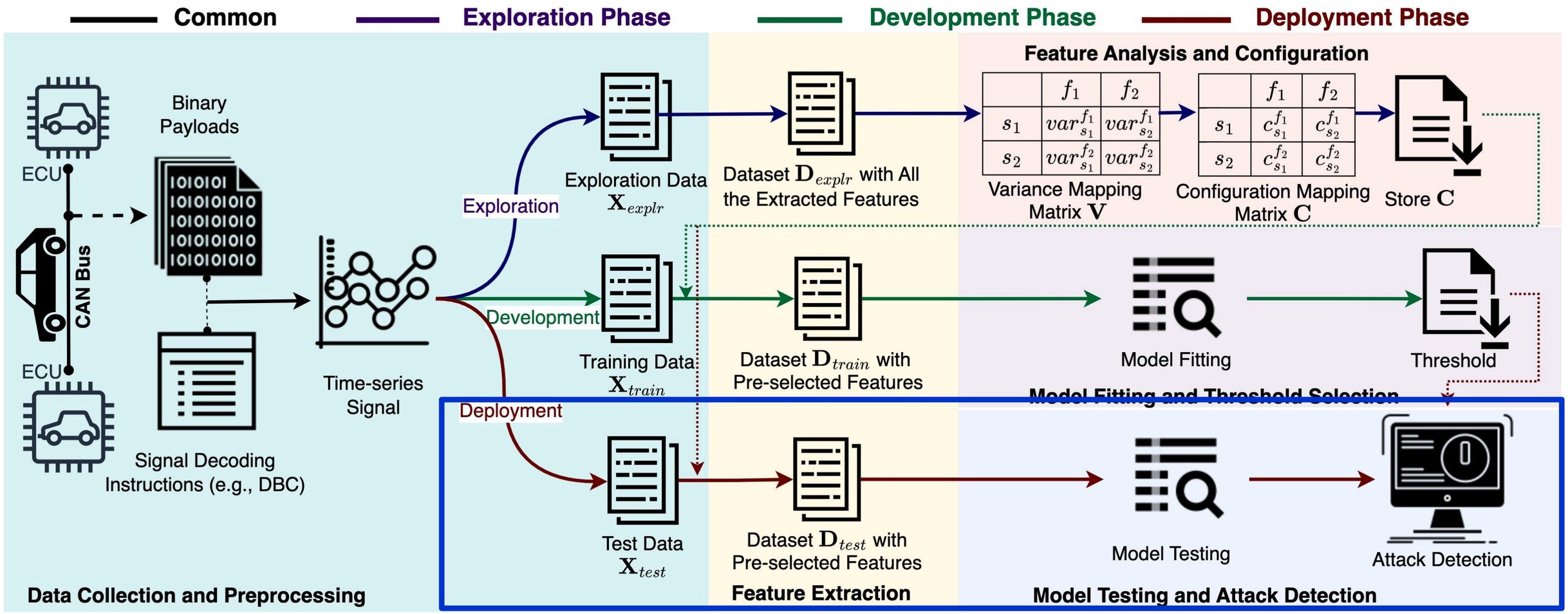
Minimum cumulative explained variance ratio (MCEVR)

Principal Component Analysis-based Reconstruction

Anomaly Score

Threshold

An Overview of CANtropy

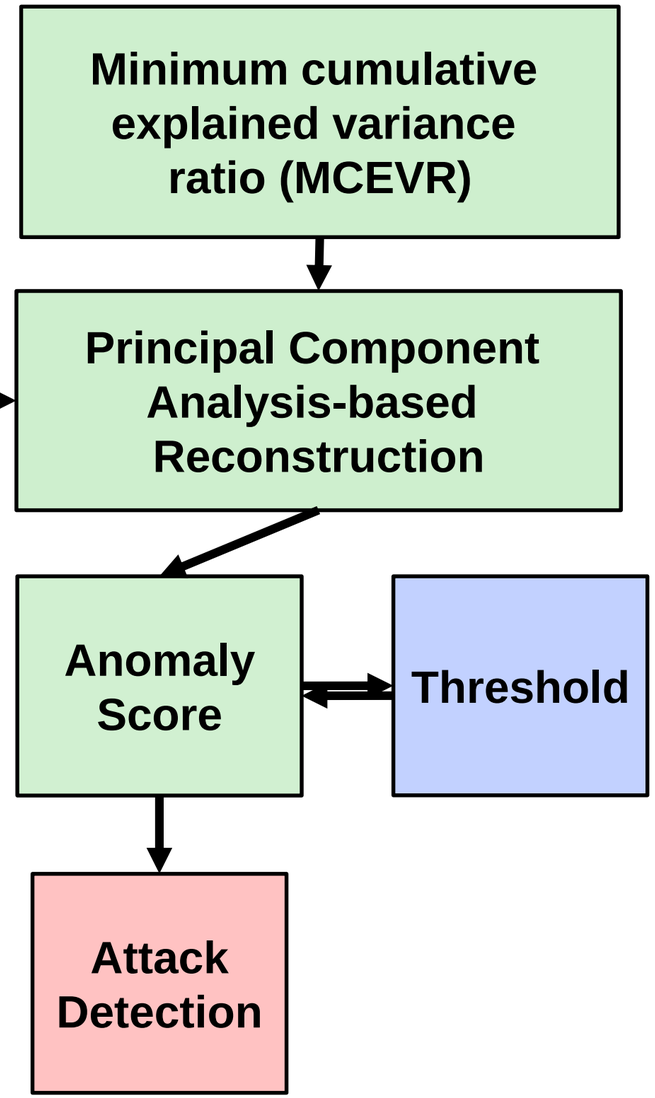


Deployment Phase: Feature Extraction & Model Testing

	f_1	f_2	f_3
s_1	●	×	●
s_2	×	●	●
s_3	●	●	×

Configuration Mapping Matrix, C

	w_1	w_2	w_3	w_4	w_5	w_6	w_7
s_1f_1	✓	✓	✓	✓	✓	✓	✓
s_1f_2							
s_1f_3	✓	✓	✓	✓	✓	✓	✓
s_2f_1							
s_2f_2	✓	✓	✓	✓	✓	✓	✓
s_2f_3	✓	✓	✓	✓	✓	✓	✓
s_3f_1	✓	✓	✓	✓	✓	✓	✓
s_3f_2	✓	✓	✓	✓	✓	✓	✓
s_3f_3							



Evaluation Setup

Dataset: SynCAN Dataset

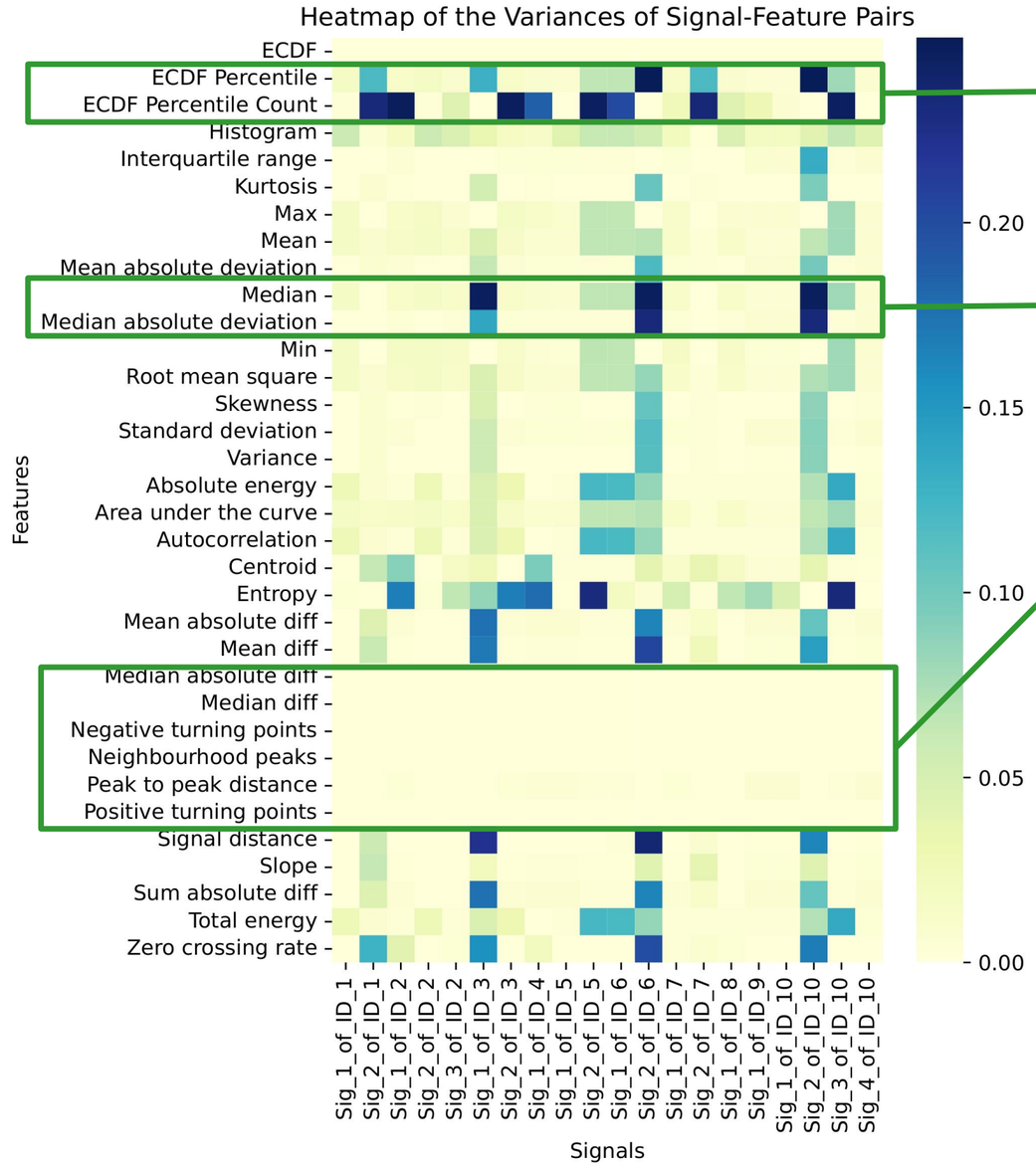
Feature Domains:`Temporal’, `Statistical', and `Both'

Evolution Metric: AUROC (Area under the ROC curve)

Baselines: CANet & CANShield

Hanselmann, Markus, et al. "CANet: An unsupervised intrusion detection system for high dimensional CAN bus data.”
Shahriar, Md Hasan, et al. "CANShield: Signal-based Intrusion Detection for Controller Area Networks."

Visualization of Variance Mapping Matrix



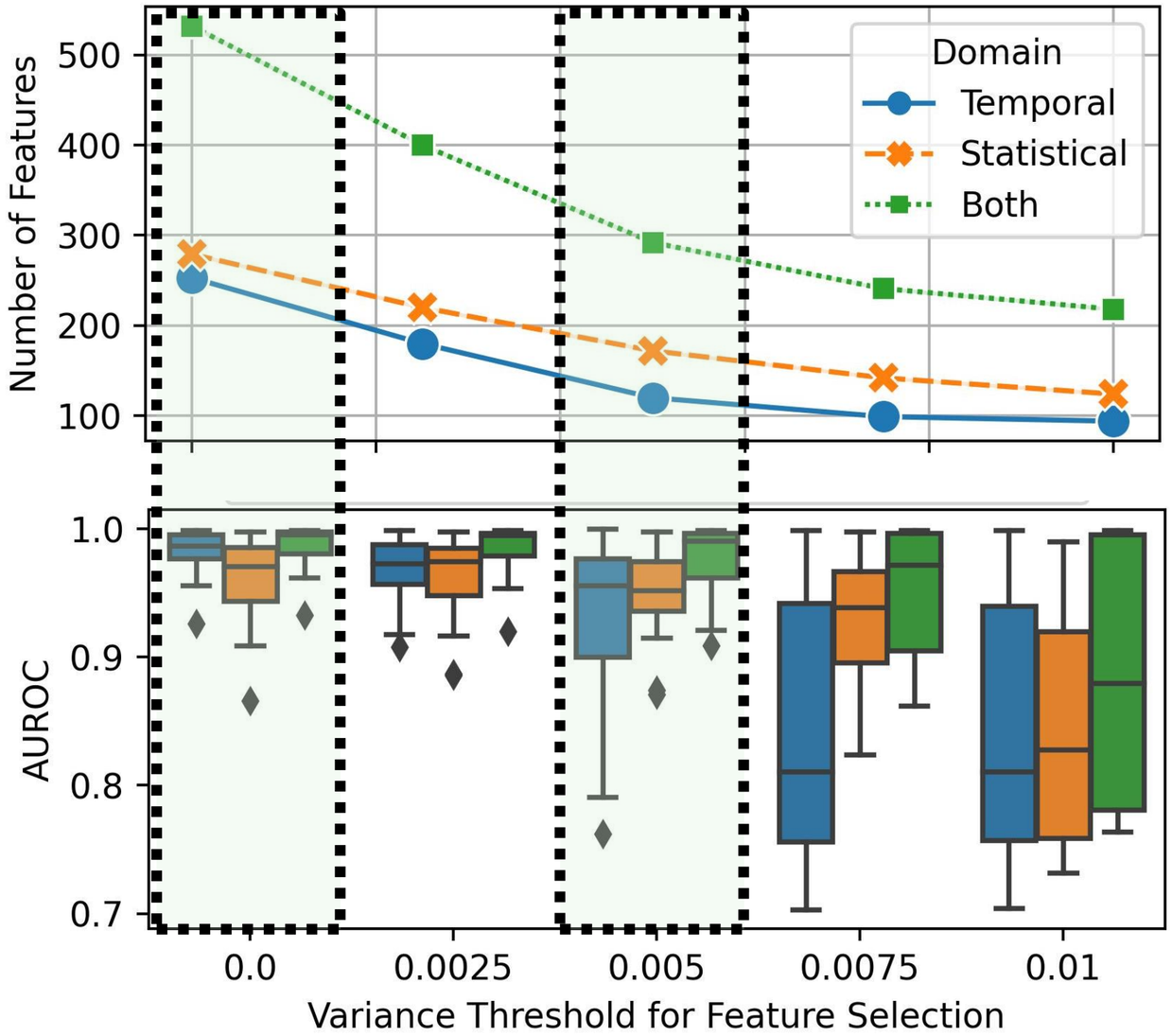
Some features have **high variances** for **most of the signals**

Some features have **high variances** for **some of the signals**

Some features have **no variance** for **any of the signal**

Signal-wise customization in feature extraction is effective.

Performance vs Number of Features



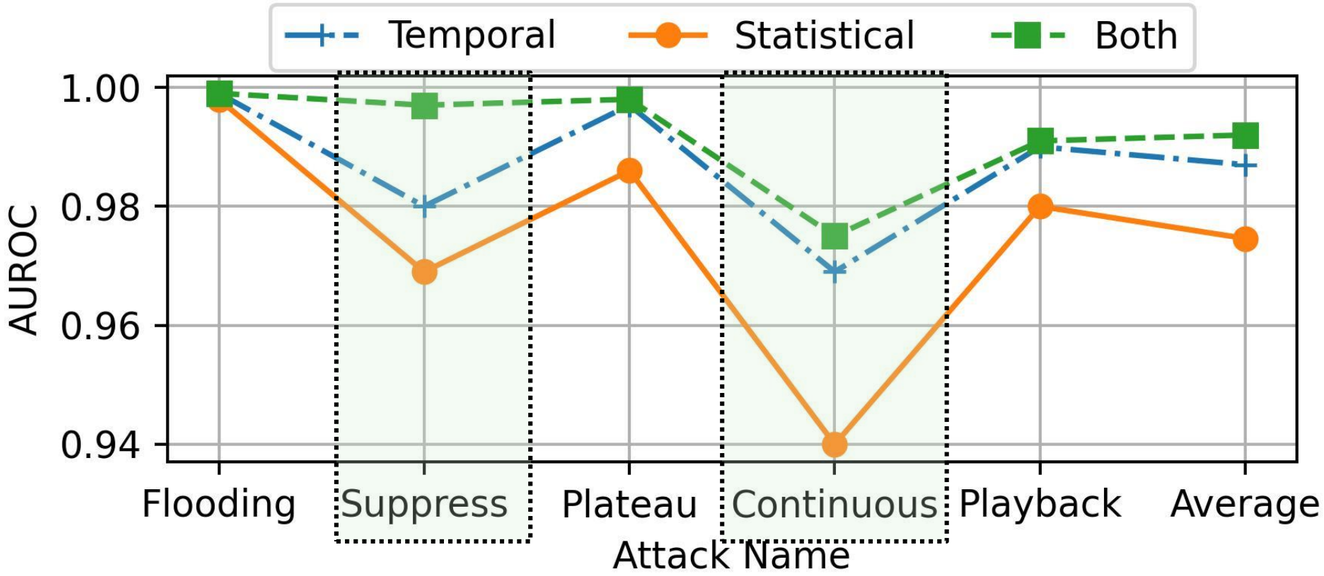
Model with all the signal-feature provides the best detection performance.

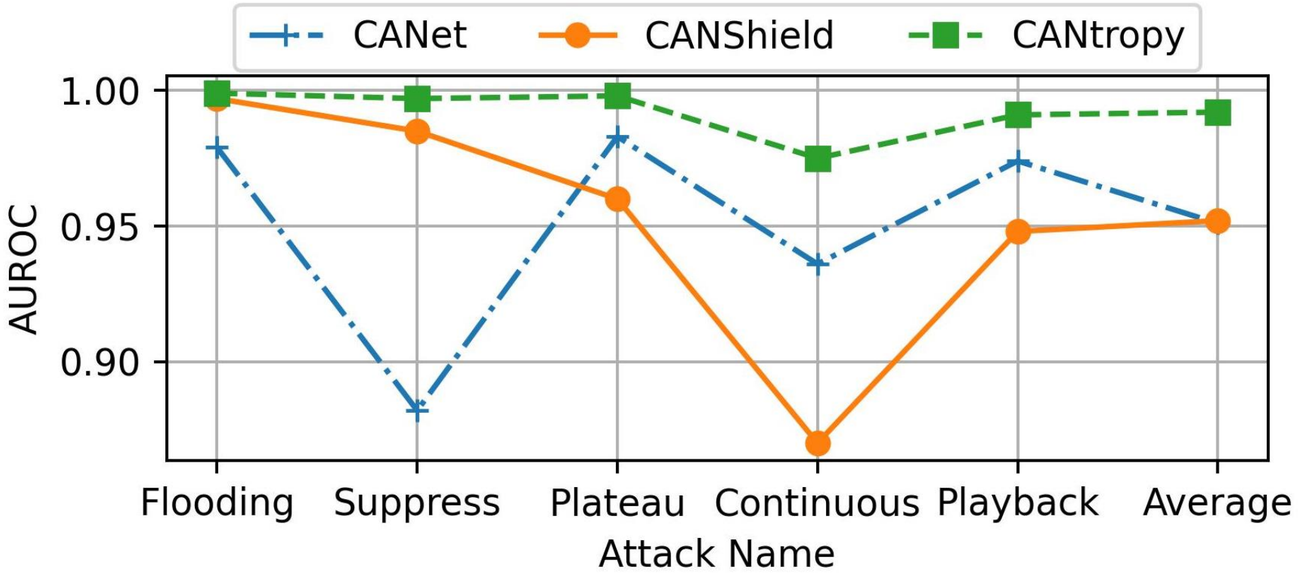
Model-based on temporal or statistical features only is more susceptible to the variance threshold.

Model accuracy and robustness are enhanced by combining features from both domains.

Attack-wise Performance

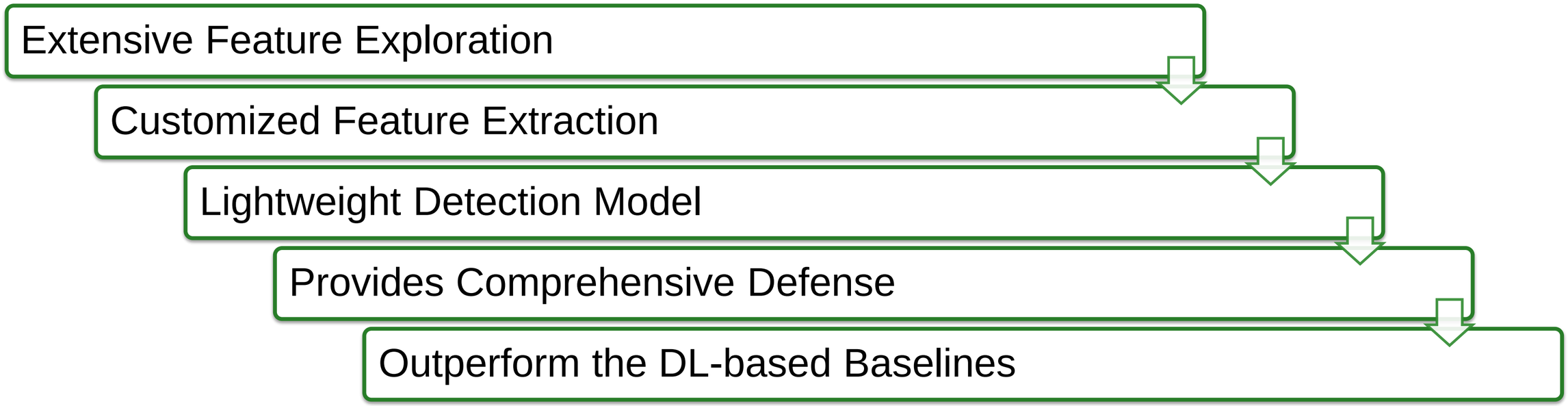
Combining features from ‘Both’ the domains improves the detection of **continuous** and **suppress** attacks.



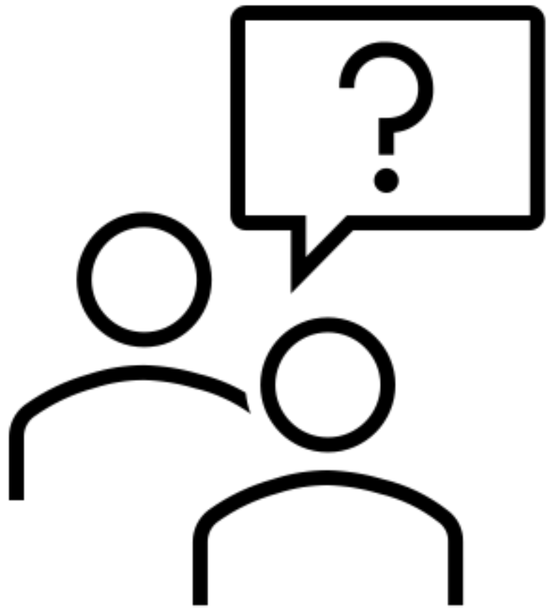


CANtropy outperforms the baselines in most of the attacks and provides an average AUROC score of 0.992.

Summary of CANtropy



- Thanks

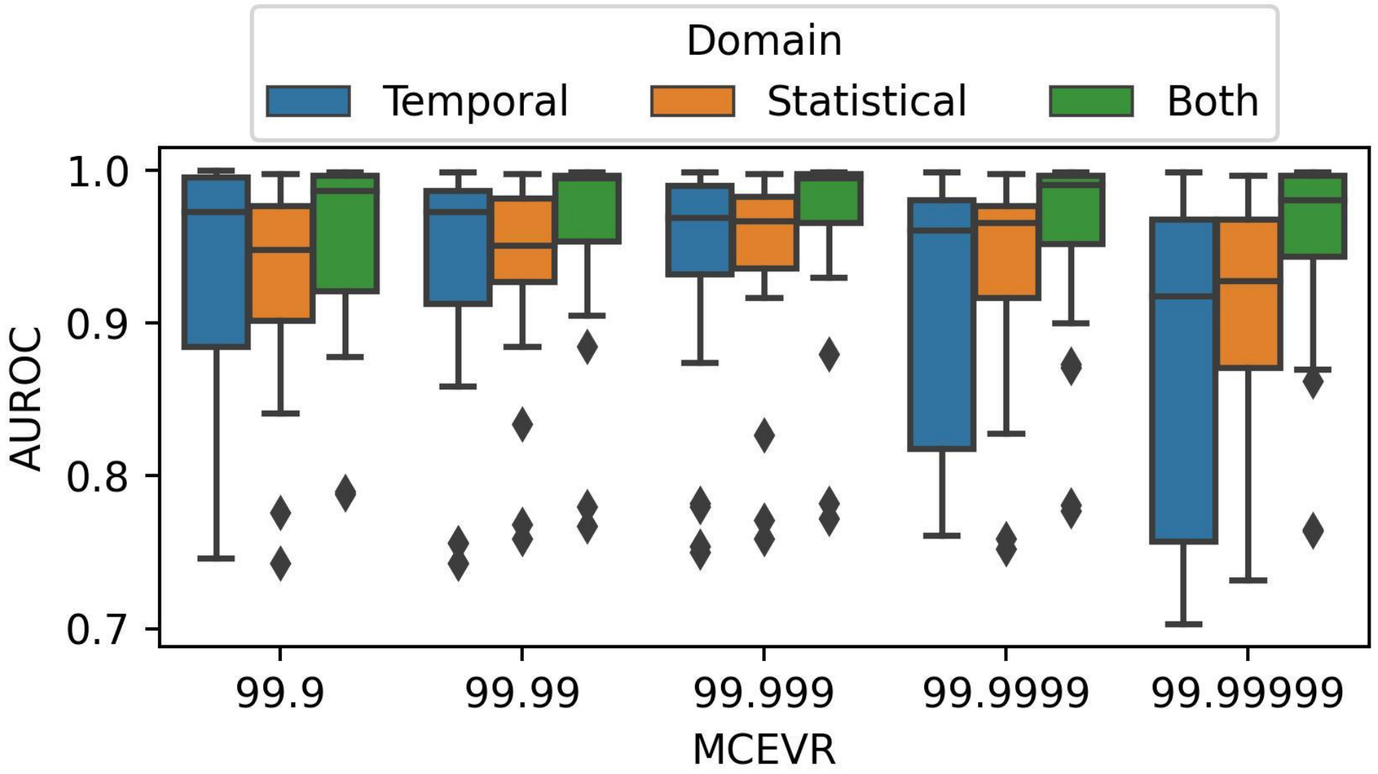


- Additional Slides

Evaluation | MCEVR

Observation:

- Retaining 99.999% variance during the PCA provides the best representation of the data and maximizes the detection performances (AUROC) of different types of attacks.
- Considering both features in a single detector makes the detection efficient.



Scalability Analysis

- CANtropy inference **scalable**
  - Feature extraction takes 80 ms per window with all the features
  - The inference only takes 0.52 ms per window for all the features
  - Hence the total upper limit for full interference is 80.52 ms
    - Which is still under the human perception time of 0.7 sec.
- CANtropy needs to fit the PCA model with the training data
  - Making it **lightweight, and easily transferable**.

Limitations

- **CANtropy considers a step size as the same length of the window**
  - We consider a step size of 500 in these evaluation
  - CANet and CANShield considered a step size of 1
  - CANtropy's performance may differ step size of 1
- **Feature extraction of CANtropy takes longer time compared to the baselines**
  - If the transmission interval CAN bus is around 2m
    - Wait for approximately 40 messages to run the inference again

Attack Model

- Access the CAN bus using:
  - Infotainment, ADAS systems, OBD-II port, etc.
- Turn off any ECU or launch a masquerade attack.

Fabrication attacks

- A compromised ECU injects malicious IDs and data

Suspension attacks

- A legitimate ECU is turned off/incapacitated

Masquerade attacks

- A legitimate ECU is turned off and injects malicious data with its ID

Design Objectives

Effective Data Representation

- Extract the most relevant features for an effective learning

Detecting Advanced Attacks

- Implement a lightweight IDS to detect a variety of CAN attacks

Near real-time detection with near-zero false positives

- Respond to intrusions with near-zero false-positive rate
- Low inference time for timely attack detection

CANtropy | Feature Extraction & Exploration Algorithms

Algorithm 1 Feature Extraction

Input: List of signals $\mathcal{S} = [s_1, s_2, \cdots, s_n]$
List of features, $\mathcal{F} = [f_1, f_2, \cdots, f_m]$,
Configuration matrix, $\mathbf{C} \in \mathbb{R}^{n \times m}$, CAN signal dataset, $\mathbf{X} \in \mathbb{R}^{t \times n}$
Output: Generated dataset, $\mathbf{D}$

Initialize empty 2D dataset $\mathbf{D}$ = [,]
for signal $s_i \in \mathcal{S}$ **do**
    for feature $f_j \in \mathcal{F}$ **do**
        if C[i,j] == 1 **then**
            Generate feature $s_i f_j$ shifting a of window w over $\mathbf{X}$
            Add new feature $s_i f_j$ to dataset $\mathbf{D}$
        end if
    end for
end for
Save new dataset $\mathbf{D}$ for development or deployment phase

Algorithm 2 Feature Analysis and Variance Matrix

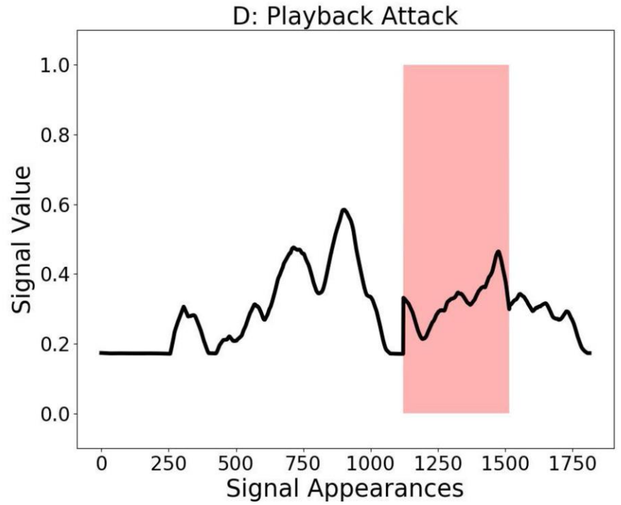
Input: List of signals $\mathcal{S} = [s_1, s_2, \cdots, s_n]$
List of features, $\mathcal{F} = [f_1, f_2, \cdots, f_m]$,
Variance threshold $var\_th \in \mathbb{R}$
CAN signal dataset, $\mathbf{X} \in \mathbb{R}^{t \times n}$
Variables: Configuration matrix $\mathbf{C} \in \mathbb{R}^{n \times m} \leftarrow \mathbf{0}$
Output: Variance matrix, $\mathbf{V} \in \mathbb{R}^{n \times m}$, Configuration matrix, $\mathbf{C}$

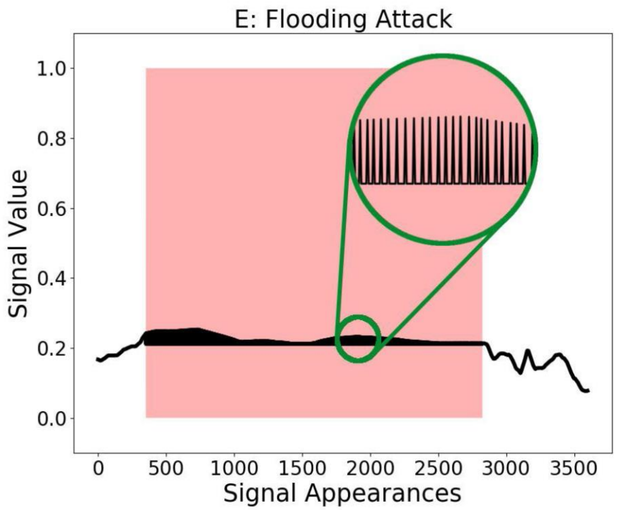
for signal $s_i \in \mathcal{S}$ **do**
    for feature $f_j \in \mathcal{F}$ **do**
        Generate feature $s_i f_j$ by shifting a of window w over $\mathbf{X}$
        Calculate variance $var_{s_i}^{f_j}$ of $s_i f_j$, assign it to $\mathbf{V}[i, j]$
        if $\mathbf{V}[i, j] > var_{th}$ **then**
            $\mathbf{C}[i, j] = 1$
        end if
    end for
end for
Store configuration matrix $\mathbf{C}$ for future feature generation

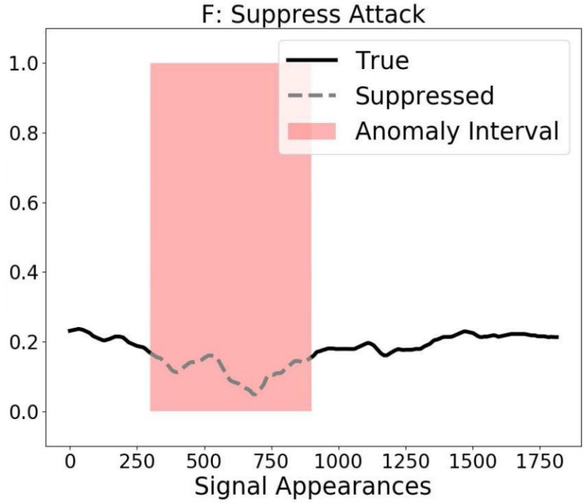
Dataset - SynCAN

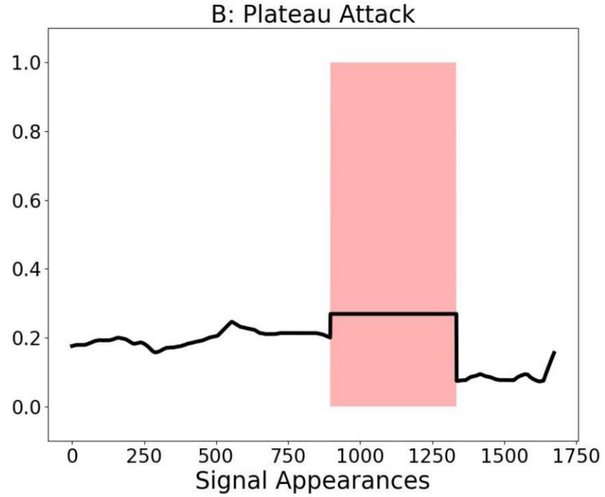
Description of masquerade attacks in SynCAN dataset

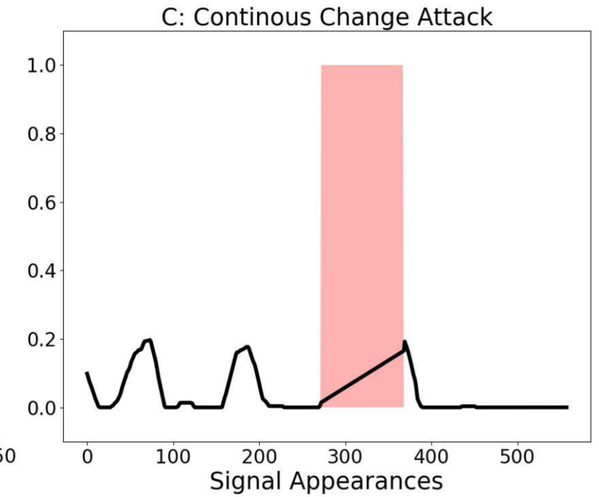
Attack Name	Attack Type	Description
Flooding	Fabrication	Frequently injects high-priority messages.
Suppress	Suspension	Prevent an ECU from transmission.
Plaeau	Masquerade	Broadcasts a constant value.
Continuous		Broadcasts continuously changing values.
Playback		Broadcasts a series of recorded values.











VIRGINIA TECH

Hanselman et al. "CANet: An unsupervised intrusion detection system for high dimensional CAN bus data." IEEE Access

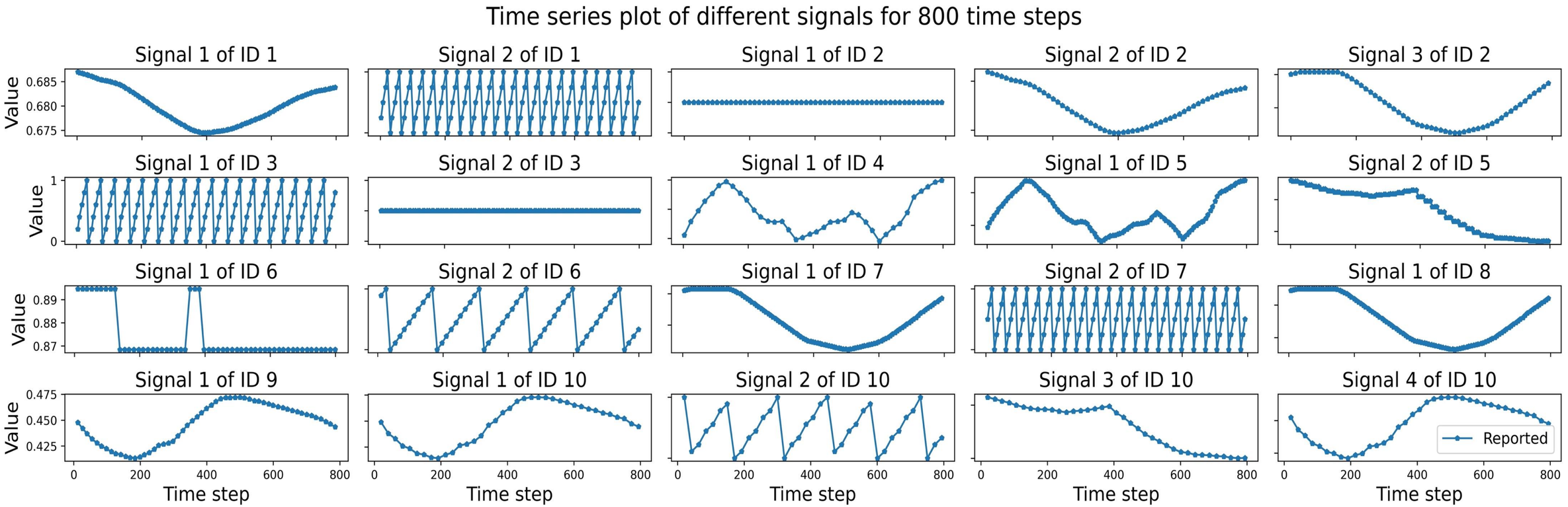
List of Feature Functions

Index	Domain	Feature
1	Statistical	ECDF
2	Statistical	ECDF Percentile
3	Statistical	ECDF Percentile Count
4	Statistical	Histogram
5	Statistical	Interquartile range
6	Statistical	Kurtosis
7	Statistical	Max
8	Statistical	Mean
9	Statistical	Mean absolute deviation
10	Statistical	Median
11	Statistical	Median absolute deviation
12	Statistical	Min
13	Statistical	Root mean square
14	Statistical	Skewness
15	Statistical	Standard deviation
16	Statistical	Variance

Index	Domain	Feature
17	Temporal	Absolute energy
18	Temporal	Area under the curve
19	Temporal	Autocorrelation
20	Temporal	Centroid
21	Temporal	Entropy
22	Temporal	Mean absolute diff
23	Temporal	Mean diff
24	Temporal	Median absolute diff
25	Temporal	Median diff
26	Temporal	Negative turning points
27	Temporal	Neighbourhood peaks
28	Temporal	Peak to peak distance
29	Temporal	Positive turning points
30	Temporal	Signal distance
31	Temporal	Slope
32	Temporal	Sum absolute diff
33	Temporal	Total energy
34	Temporal	Zero crossing rate

Experiments | Time Series Plot of SynCAN Dataset

- Markers indicates the arrival of corresponding CAN message.
- Different CAN IDs has different reporting periods.



Experiments | Reporting Periods of SynCAN

- There are three groups of CAN IDs.
- Reporting periods are around 7, 13, and 22 time steps.