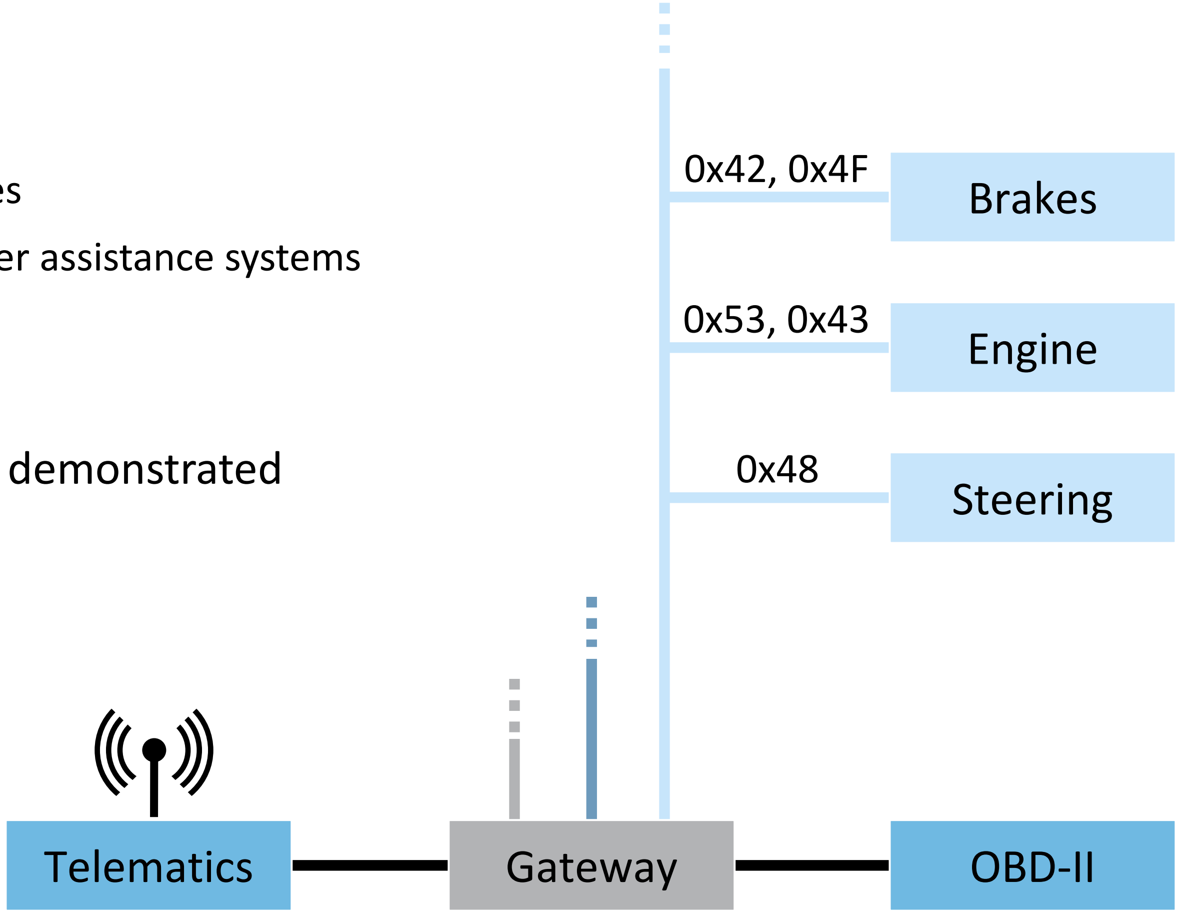
EASI: Edge-Based Sender Identification on Resource-Constrained Platforms for Automotive Networks

Marcel Kneib[1], Oleg Schell[2], Christopher Huth[3]

[1] Robert Bosch GmbH, RheinMain University
[2] Bosch Engineering GmbH, Karlsruhe Institute of Technology
[3] Robert Bosch GmbH

Introduction
Motivation

- Increased connectivity...
  - either by built-in or retrofitted (wireless) interfaces
  - required for comfort functions and advanced driver assistance systems
  - provides several additional attack vectors
- Attack potential is well known and successfully demonstrated
  - Miller and Valasek [43]
  - Tencent Keen Security Lab [62]
- Controller Area Network
  - Broadcasting without authenticity
  - 500 kb/s bandwidth
  - 64 bit payload

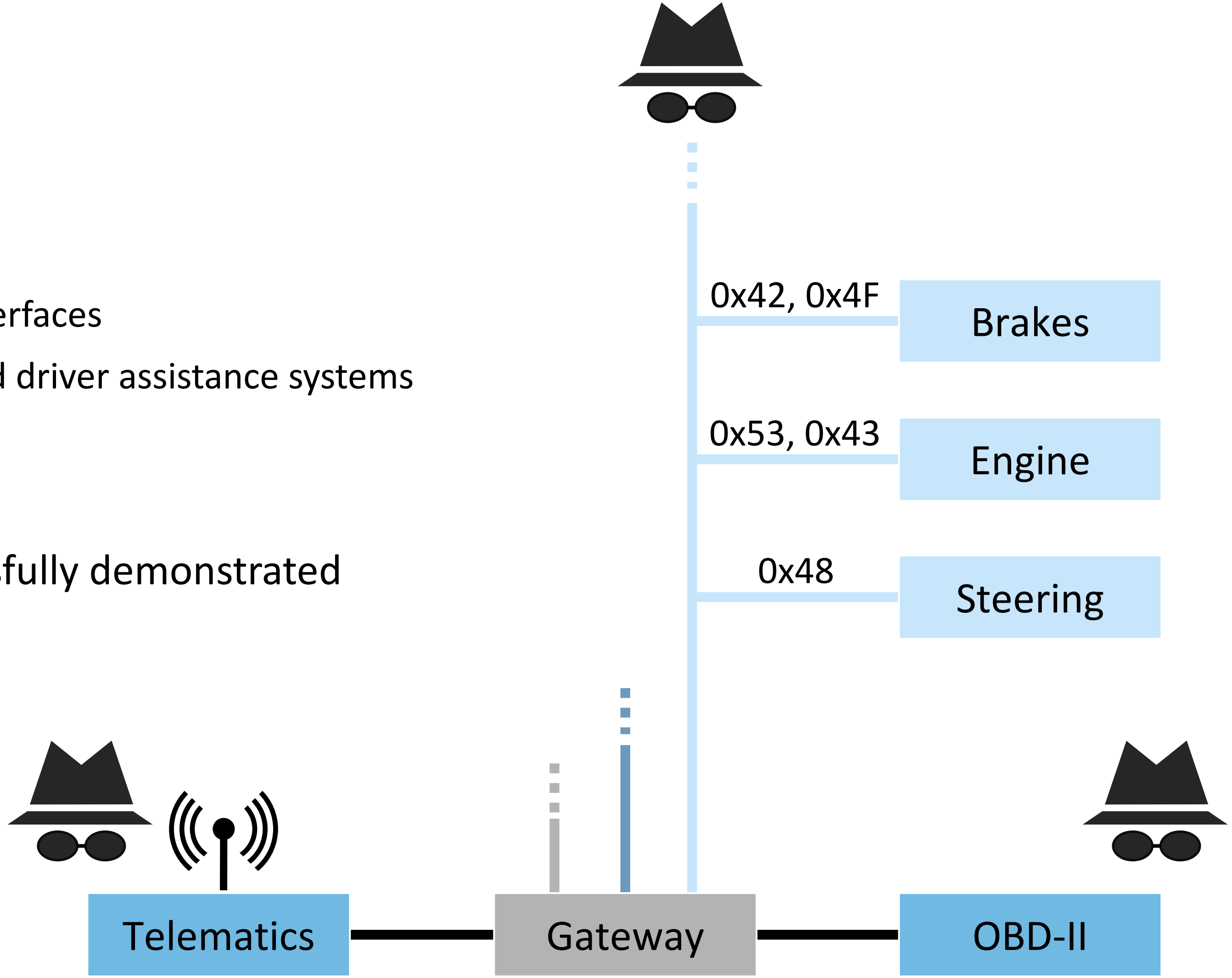


Introduction
Motivation

- Increased connectivity...
  - either by built-in or retrofitted (wireless) interfaces
  - required for comfort functions and advanced driver assistance systems
  - provides several additional attack vectors

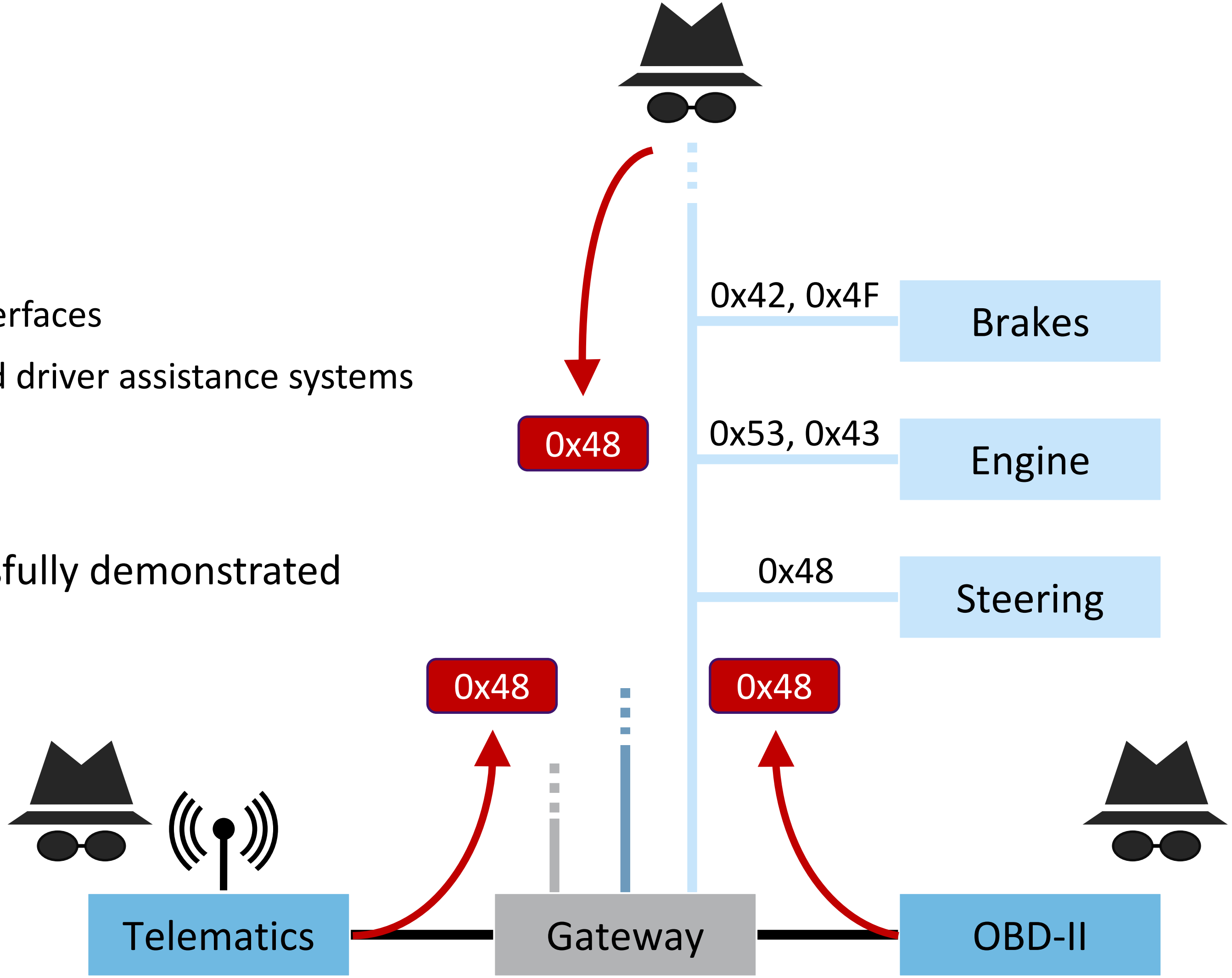
- Attack potential is well known and successfully demonstrated
  - Miller and Valasek [43]
  - Tencent Keen Security Lab [62]

- Controller Area Network
  - Broadcasting without authenticity
  - 500 kb/s bandwidth
  - 64 bit payload



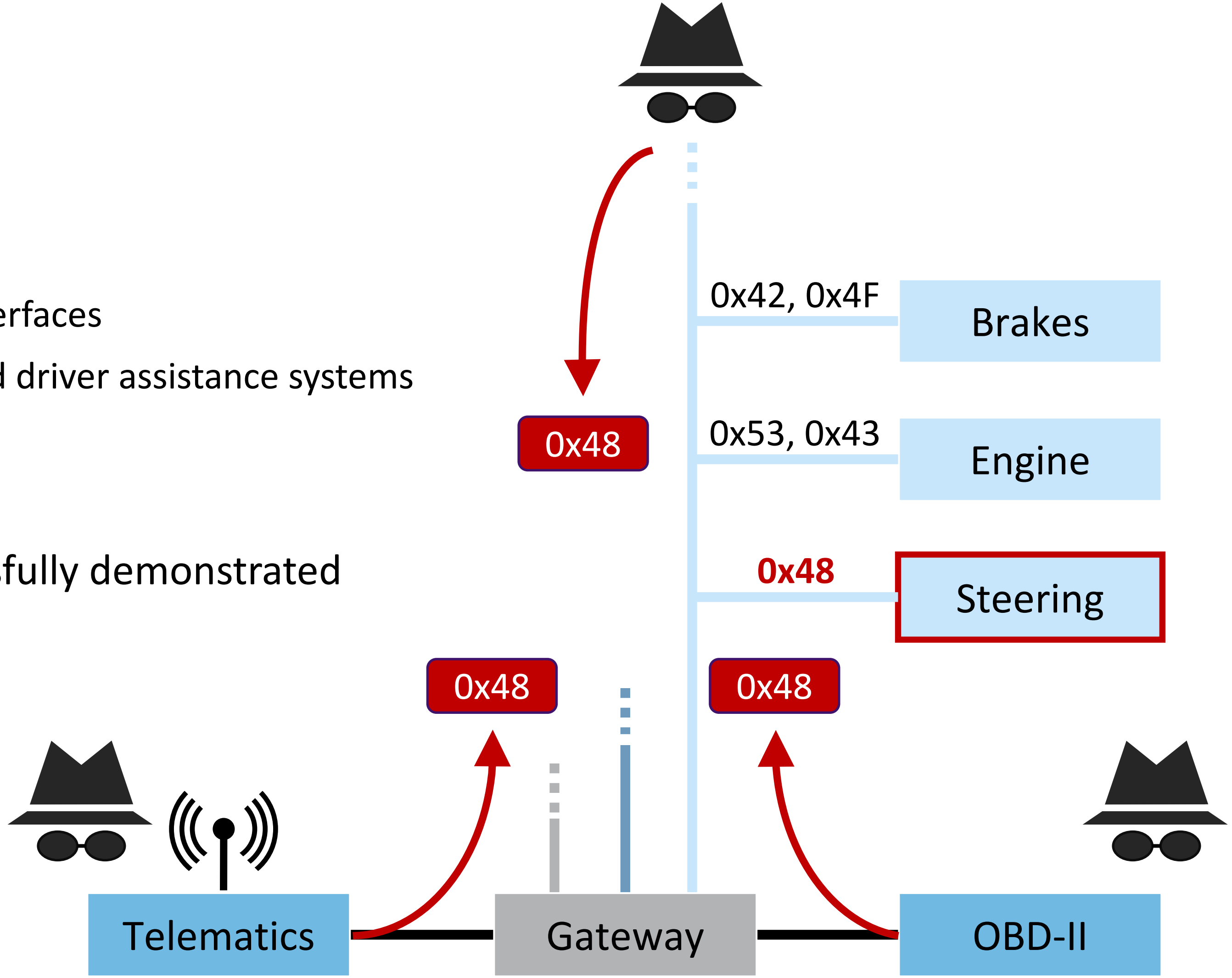
Introduction
Motivation

- Increased connectivity...
  - either by built-in or retrofitted (wireless) interfaces
  - required for comfort functions and advanced driver assistance systems
  - provides several additional attack vectors
- Attack potential is well known and successfully demonstrated
  - Miller and Valasek [43]
  - Tencent Keen Security Lab [62]
- Controller Area Network
  - Broadcasting without authenticity
  - 500 kb/s bandwidth
  - 64 bit payload



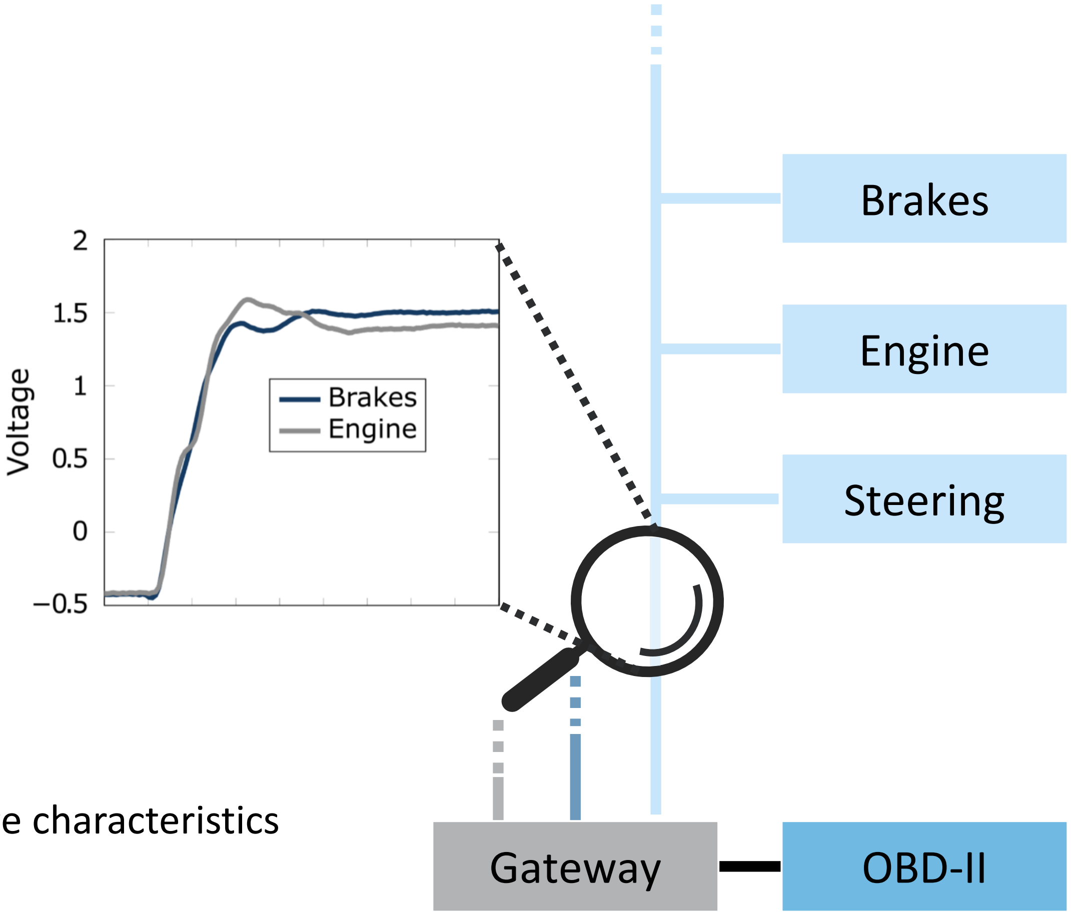
Introduction
Motivation

- Increased connectivity...
  - either by built-in or retrofitted (wireless) interfaces
  - required for comfort functions and advanced driver assistance systems
  - provides several additional attack vectors
- Attack potential is well known and successfully demonstrated
  - Miller and Valasek [43]
  - Tencent Keen Security Lab [62]
- Controller Area Network
  - Broadcasting without authenticity
  - 500 kb/s bandwidth
  - 64 bit payload



Introduction
Countermeasures

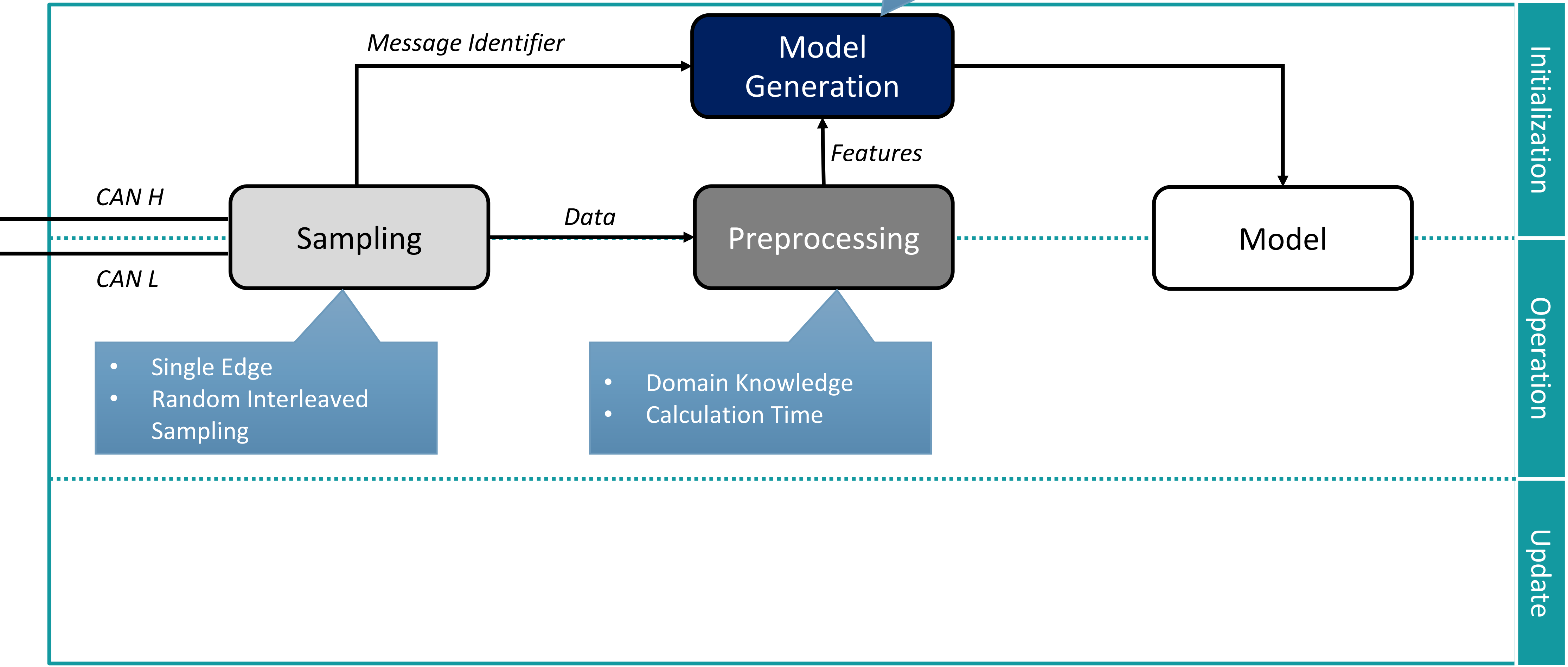
- Message Authentication Codes
  - Overhead, payload, broadcast, non-repudiation, ...
- Digital Signatures
- Intrusion Detection (Prevention) Systems
  - Signatures... only suitable for known attacks
  - Anomalies... prone to false positives
- Voltage-Based Sender Identification
  - Anomaly detection through exploitation of unique voltage characteristics
  - High detection rates
  - Low false positive rate
  - **High hardware demands**



Reduction of required resources!

EDGE BASED SENDER IDENTIFICATION

Edge-Based Sender Identification
Initialization Phase



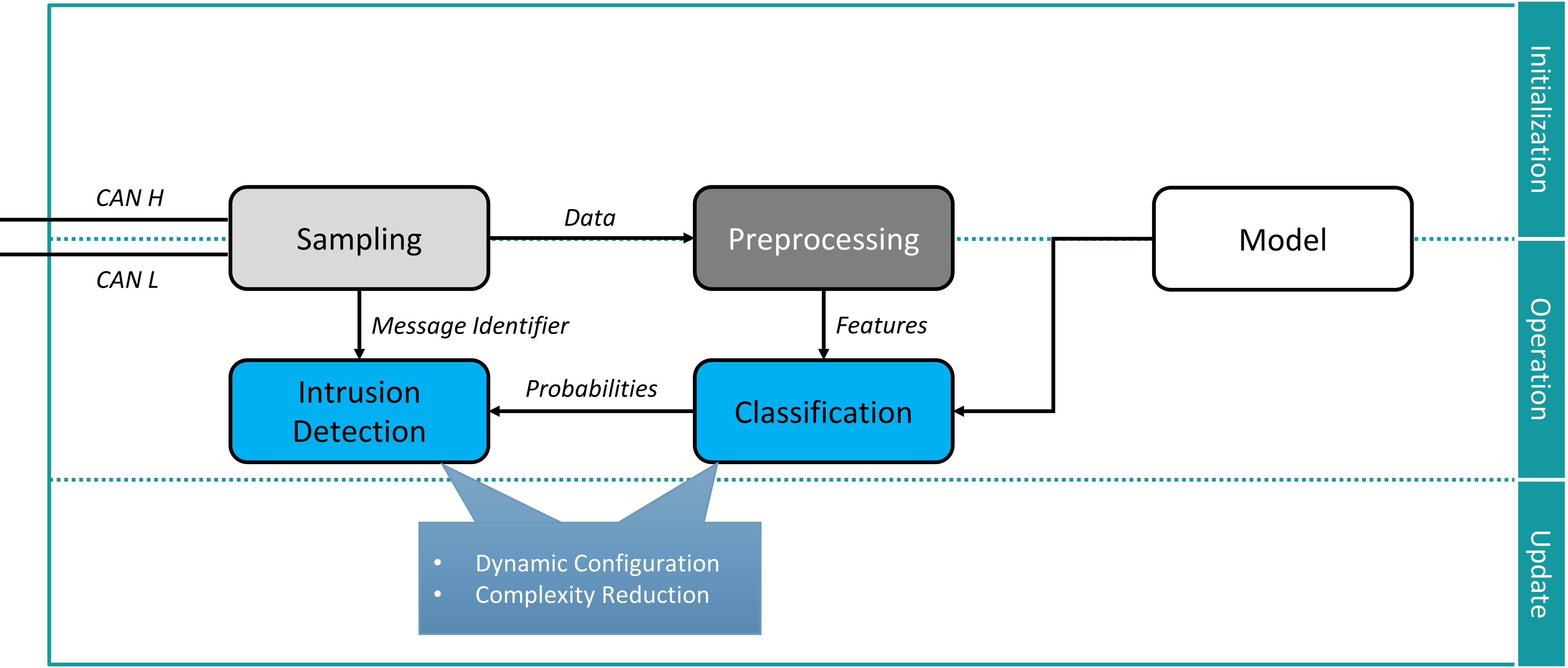
- Algorithm Assessment
- Dynamic Configuration

- Single Edge
- Random Interleaved Sampling

- Domain Knowledge
- Calculation Time

Edge-Based Sender Identification

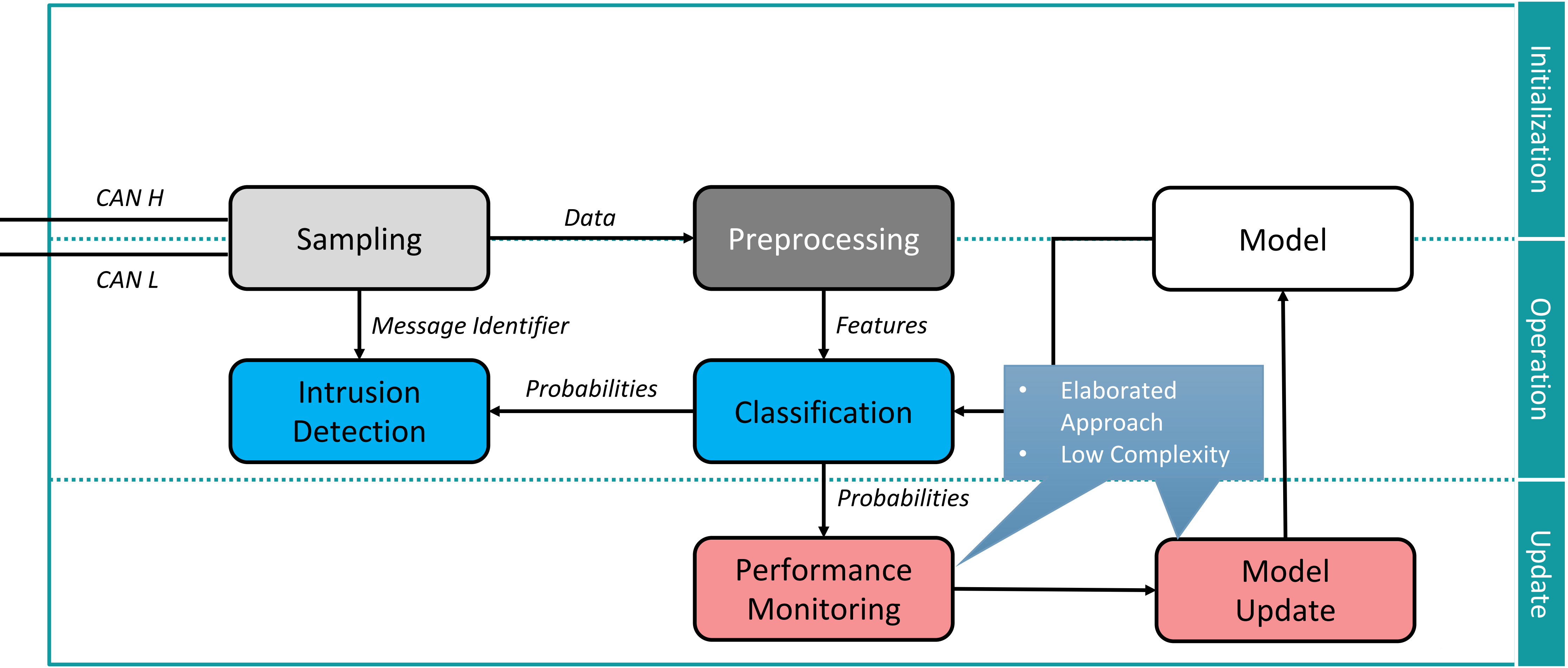
Operation Phase



- Dynamic Configuration
- Complexity Reduction

Edge-Based Sender Identification

Model Adjustments

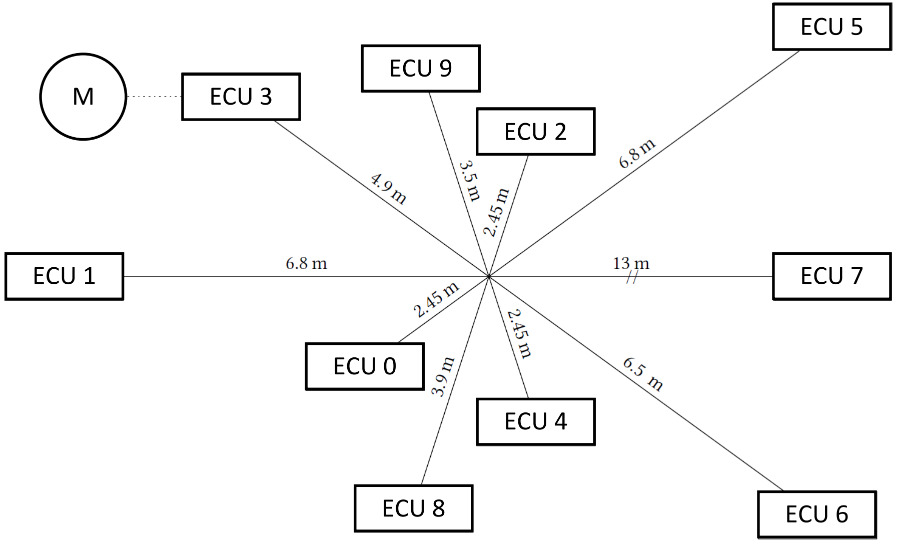


- Elaborated Approach
- Low Complexity

EVALUATION

Evaluation

General Evaluation



- Sender identification evaluation on PC with three setups
  - Focus on Logistic Regression
  - Avg. identification rate of 99.98 % → false alarm every 5000 frames
- Intrusion detection based on thresholds
  - Avg. detection rate of 99.8 % and no false positives

	Setup		Sender Identification		Intrusion Detection	
	ECUs	Frames			Normal	Attack
Prototype	10	48 000	99.99	Normal	100	0
				Attack	0.19	99.81
Fiat	6+2	35 000	100	Normal	100	0
				Attack	0.06	99.94
Porsche	6+2	9 000	99.86	Normal	100	0
				Attack	0.77	99.23

Evaluation
Varying Conditions

Summer journey with cool down phases

23°C (73.4°F) – 36°C (96.8°F)

3 trips & 17 000 frames

Sender Identification Rate: 99.99 %

No false positives

Winter journey for 5 days

-2°C (28.4°F) – 10°C (50°F)

9 trips & 65 000 frames

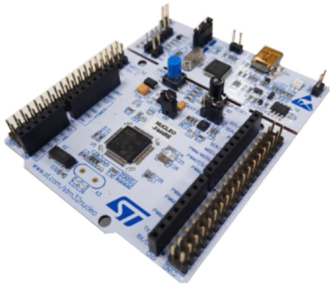
Electronic consumers (lights, wipers, heating, start-stop automatic, ...)

Sender Identification Rate: 99.99 %

No false positives

Detection Rate: 99.96 %

Evaluation
Embedded Implementation



System

- ARM Cortex-M4 180 MHz Microcontroller
- DSP for feature calculations
- Fiat 500 data set via UART

Initialization Phase

- 200 frames with mini-batch from 8 ECUs
- **2.61s for model generation**

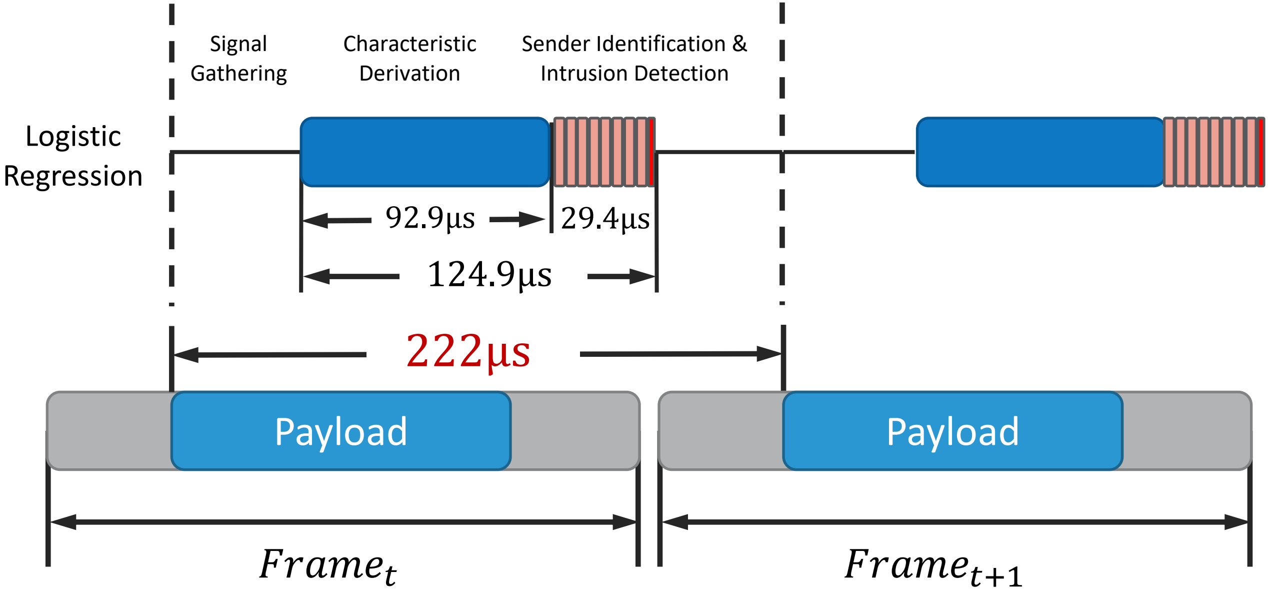
Operation Phase

- Classification with Logistic Regression
- **97µs – 125µs per frame**

→ **<u>Real-time capable</u>**

Performance

- No false positives & Sender Identification Rate 99.94 %



Conclusion

- Sender identification provides additional security for CAN networks

- EASI: Edge-Based Sender Identification
  - Reduction of resource requirements
  - Feasible on automotive-compatible hardware
  - High performance can be kept up under varying conditions
  - Refinement of performance monitoring & model adjustments

- Outlook
  - CAN with flexible data rate (CAN-FD)
  - Additional mitigations of signal drifts
  - On-board sampling

Thank you for your attention!

#LikeABosch

M.Sc.
Marcel Kneib

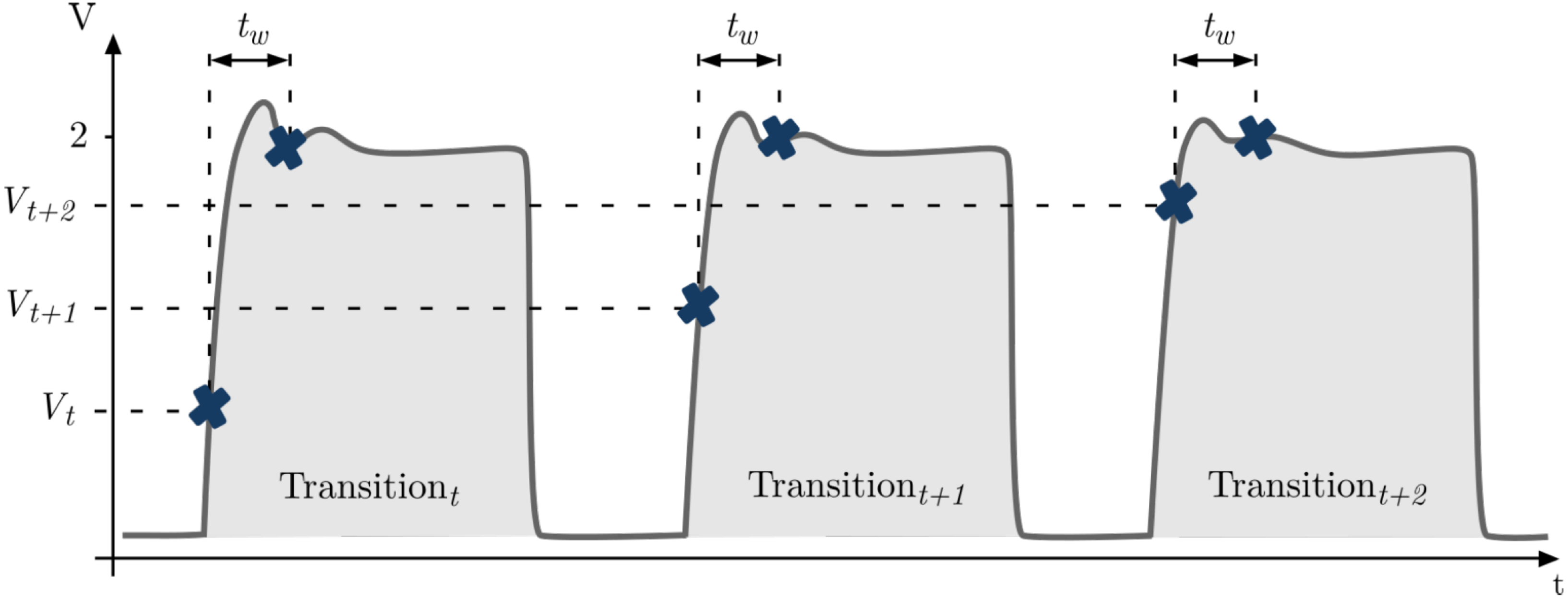
Automotive Electronics – Body Electronics
Product Security

Marcel.Kneib@de.bosch.com

BACKUP

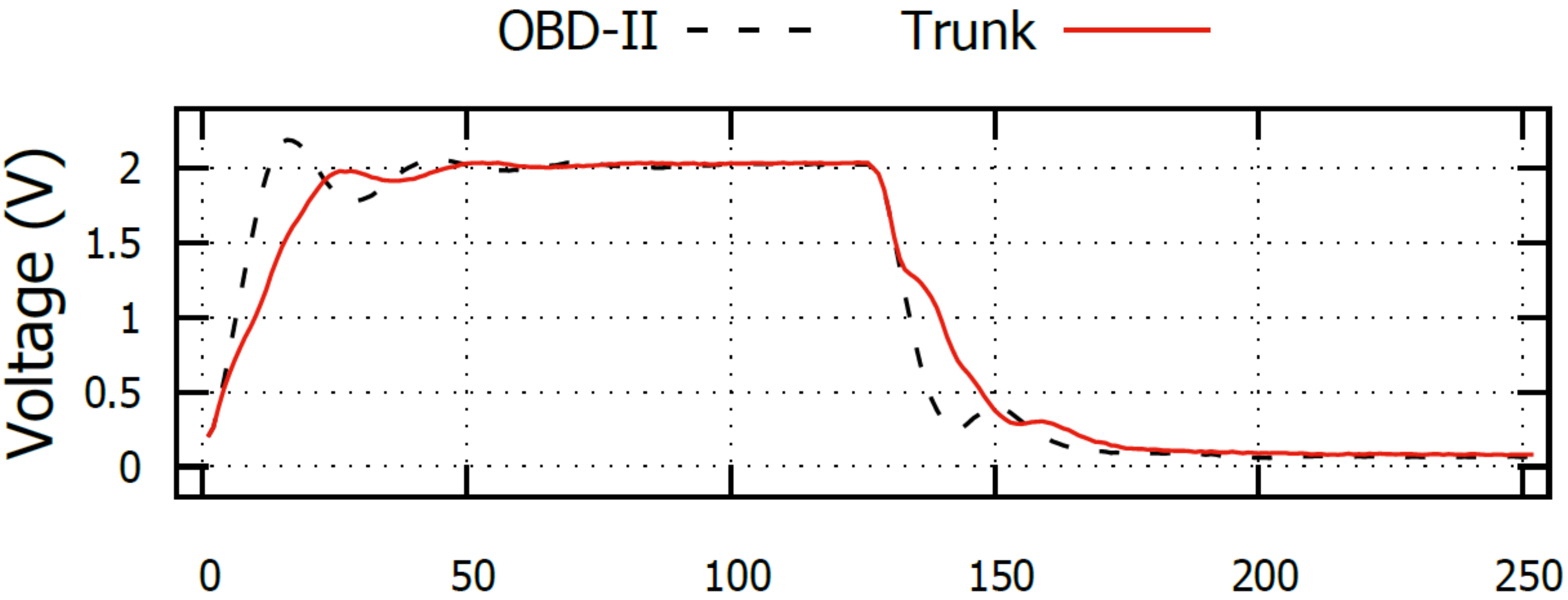
Backup

Random Interleaved Sampling

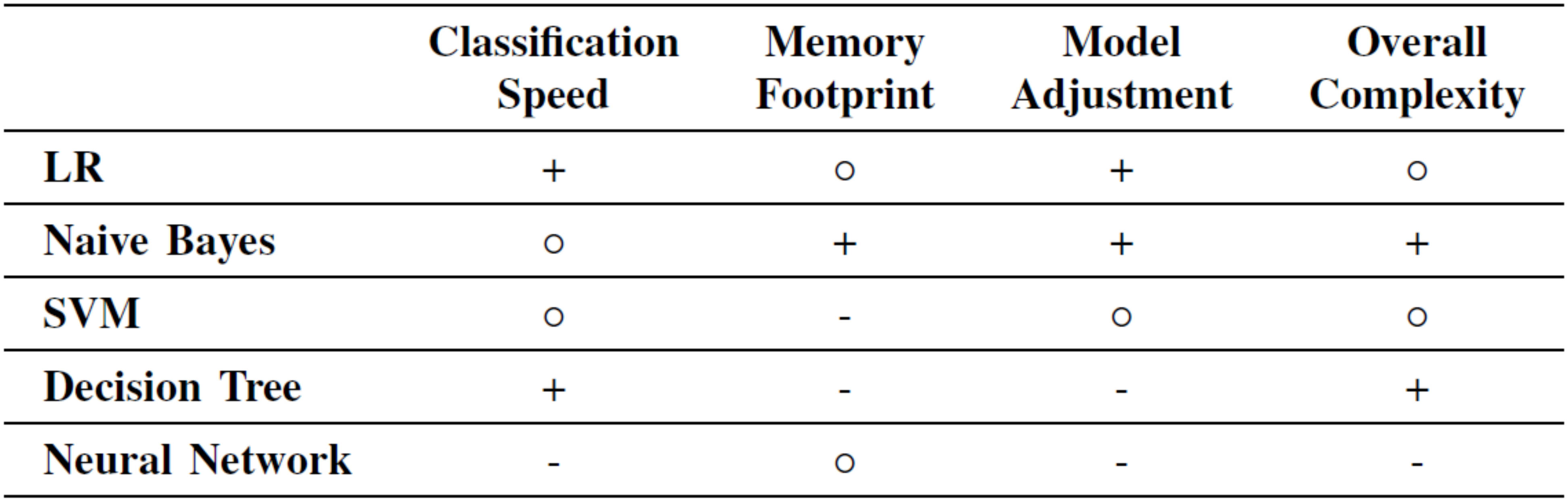


Backup

Measuring Point

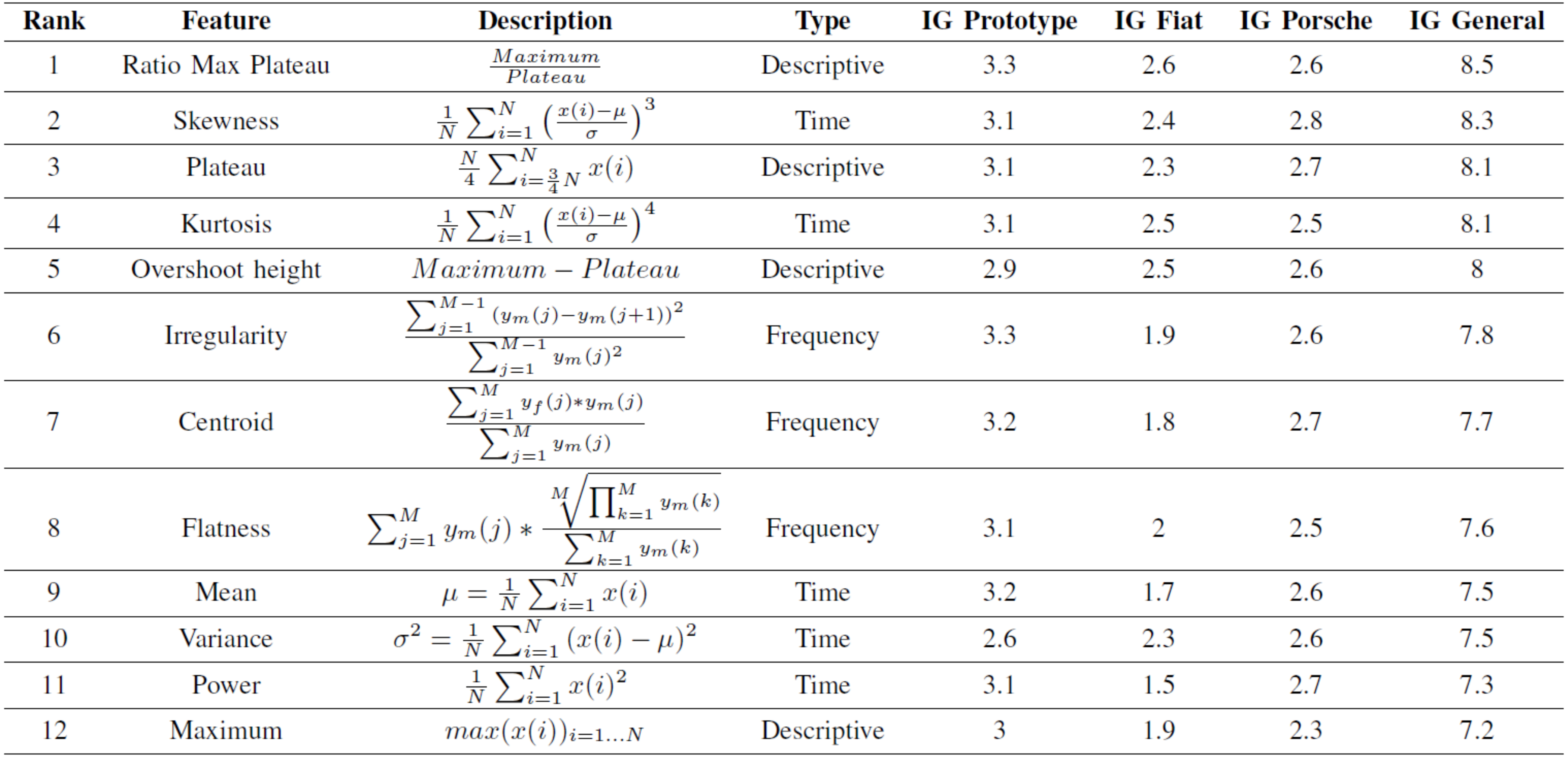


Backup
Algorithm Assessment



	Classification Speed	Memory Footprint	Model Adjustment	Overall Complexity
LR	+	o	+	o
Naive Bayes	o	+	+	+
SVM	o	-	o	o
Decision Tree	+	-	-	+
Neural Network	-	o	-	-

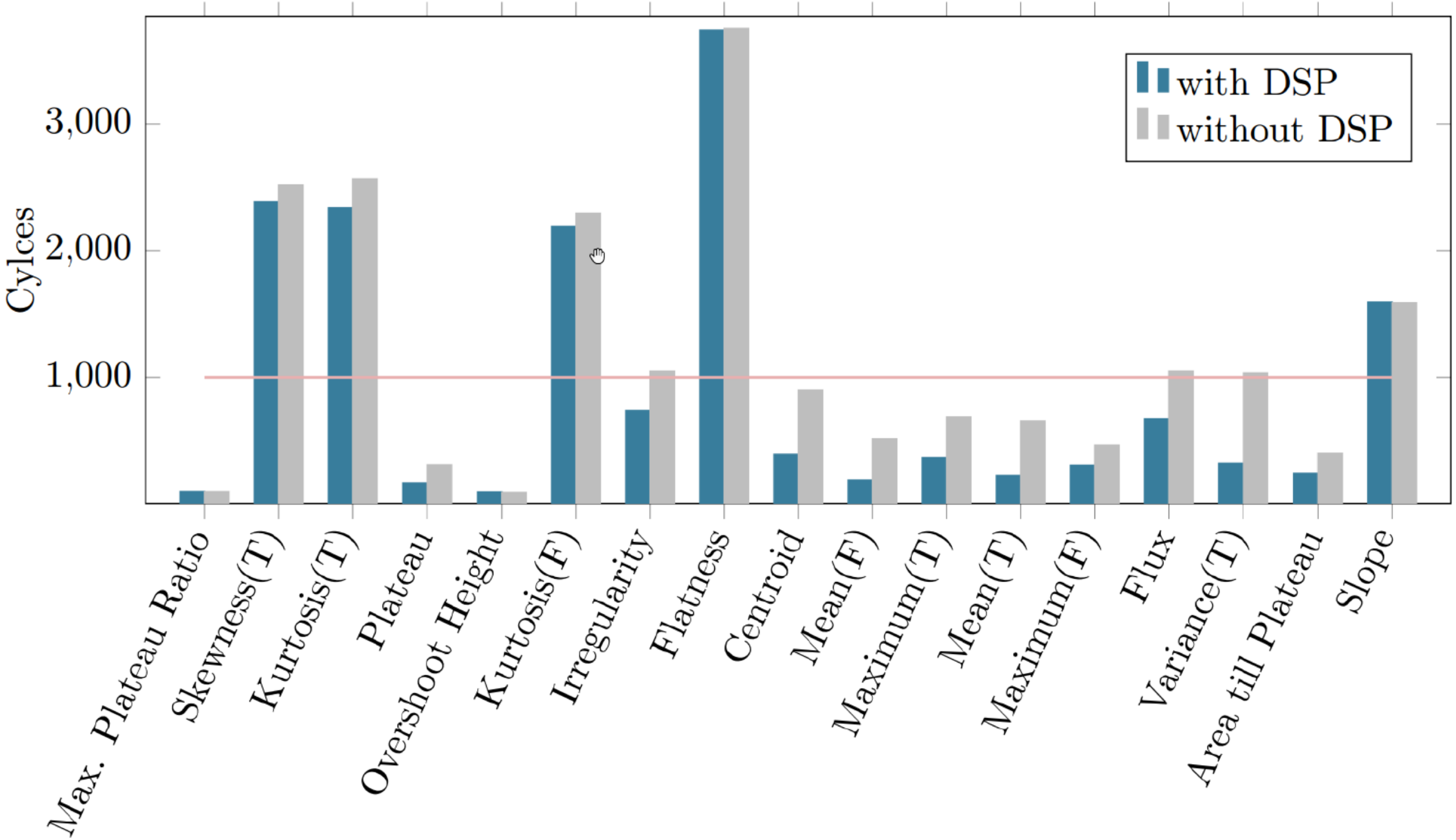
Backup
Features



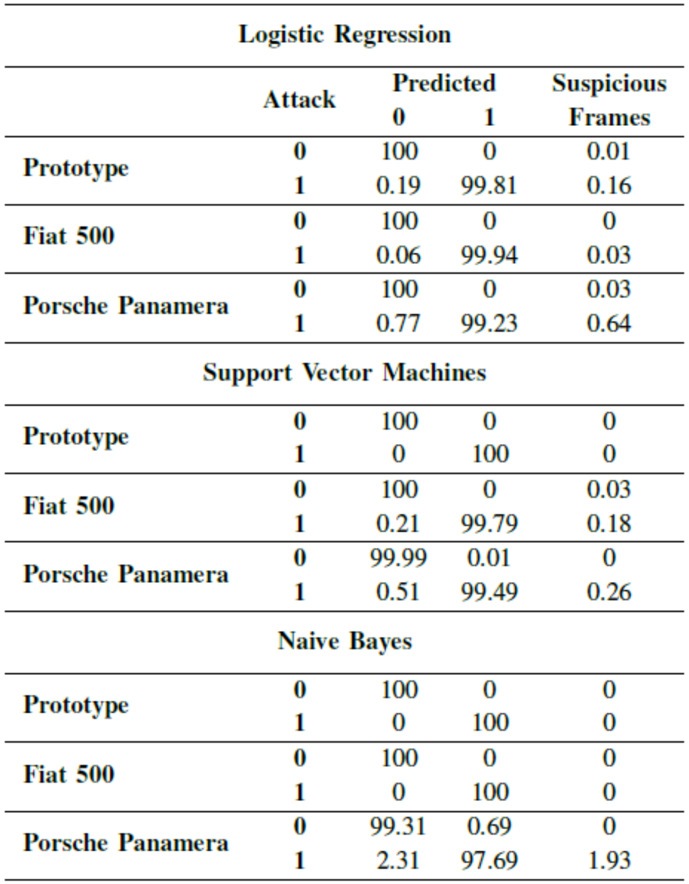
Rank	Feature	Description	Type	IG Prototype	IG Fiat	IG Porsche	IG General
1	Ratio Max Plateau	$\frac{Maximum}{Plateau}$	Descriptive	3.3	2.6	2.6	8.5
2	Skewness	$\frac{1}{N}\sum_{i=1}^{N}\left(\frac{x(i)-\mu}{\sigma}\right)^3$	Time	3.1	2.4	2.8	8.3
3	Plateau	$\frac{N}{4}\sum_{i=\frac{3}{4}N}^{N} x(i)$	Descriptive	3.1	2.3	2.7	8.1
4	Kurtosis	$\frac{1}{N}\sum_{i=1}^{N}\left(\frac{x(i)-\mu}{\sigma}\right)^4$	Time	3.1	2.5	2.5	8.1
5	Overshoot height	$Maximum - Plateau$	Descriptive	2.9	2.5	2.6	8
6	Irregularity	$\frac{\sum_{j=1}^{M-1}(y_m(j)-y_m(j+1))^2}{\sum_{j=1}^{M-1} y_m(j)^2}$	Frequency	3.3	1.9	2.6	7.8
7	Centroid	$\frac{\sum_{j=1}^{M} y_f(j)*y_m(j)}{\sum_{j=1}^{M} y_m(j)}$	Frequency	3.2	1.8	2.7	7.7
8	Flatness	$\sum_{j=1}^{M} y_m(j) * \frac{\sqrt[M]{\prod_{k=1}^{M} y_m(k)}}{\sum_{k=1}^{M} y_m(k)}$	Frequency	3.1	2	2.5	7.6
9	Mean	$\mu = \frac{1}{N}\sum_{i=1}^{N} x(i)$	Time	3.2	1.7	2.6	7.5
10	Variance	$\sigma^2 = \frac{1}{N}\sum_{i=1}^{N} (x(i)-\mu)^2$	Time	2.6	2.3	2.6	7.5
11	Power	$\frac{1}{N}\sum_{i=1}^{N} x(i)^2$	Time	3.1	1.5	2.7	7.3
12	Maximum	$max(x(i))_{i=1...N}$	Descriptive	3	1.9	2.3	7.2

Backup

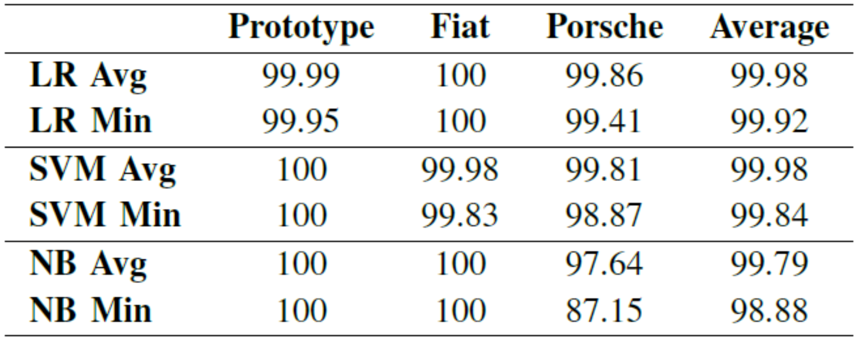
Features Calculation Time



Backup
Performance

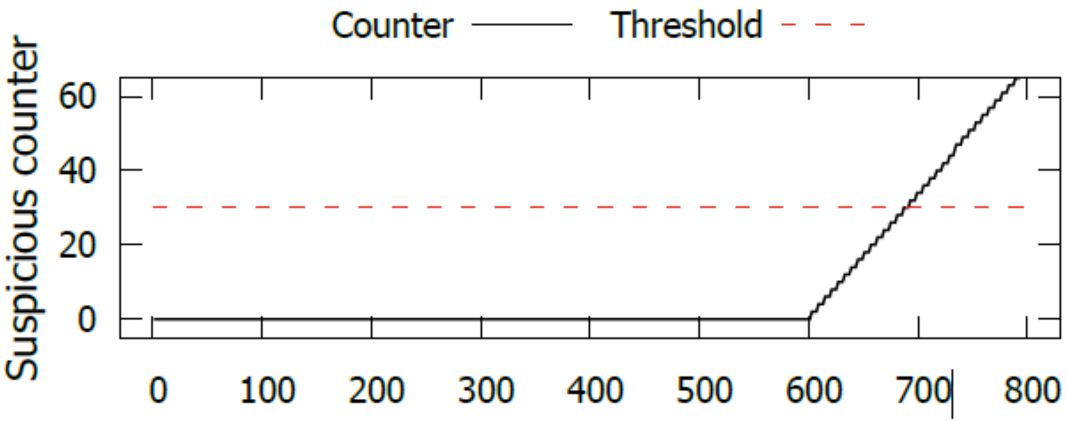


	Attack	Predicted		Suspicious
		0	1	Frames
Logistic Regression				
Prototype	**0**	100	0	0.01
	1	0.19	99.81	0.16
Fiat 500	**0**	100	0	0
	1	0.06	99.94	0.03
Porsche Panamera	**0**	100	0	0.03
	1	0.77	99.23	0.64
Support Vector Machines				
Prototype	**0**	100	0	0
	1	0	100	0
Fiat 500	**0**	100	0	0.03
	1	0.21	99.79	0.18
Porsche Panamera	**0**	99.99	0.01	0
	1	0.51	99.49	0.26
Naive Bayes				
Prototype	**0**	100	0	0
	1	0	100	0
Fiat 500	**0**	100	0	0
	1	0	100	0
Porsche Panamera	**0**	99.31	0.69	0
	1	2.31	97.69	1.93

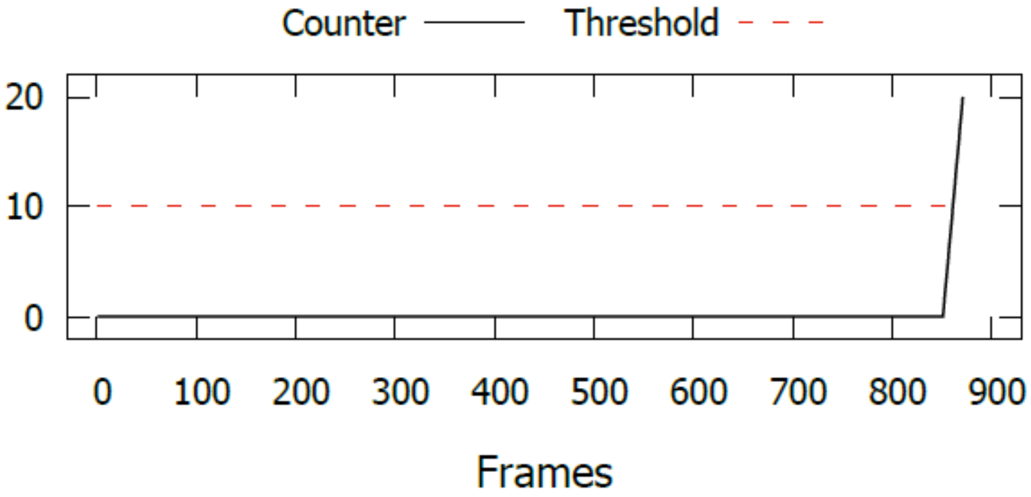


	Prototype	Fiat	Porsche	Average
LR Avg	99.99	100	99.86	99.98
LR Min	99.95	100	99.41	99.92
SVM Avg	100	99.98	99.81	99.98
SVM Min	100	99.83	98.87	99.84
NB Avg	100	100	97.64	99.79
NB Min	100	100	87.15	98.88

Backup
Additional and unmonitored ECU Attack



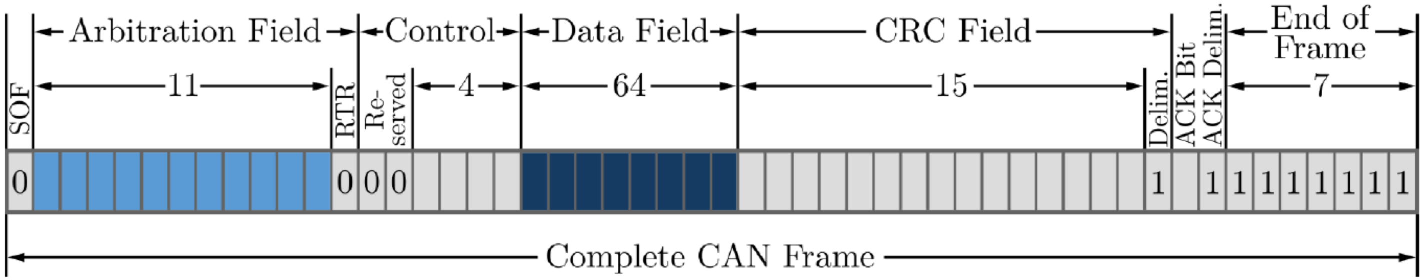
Additional ECU Attack

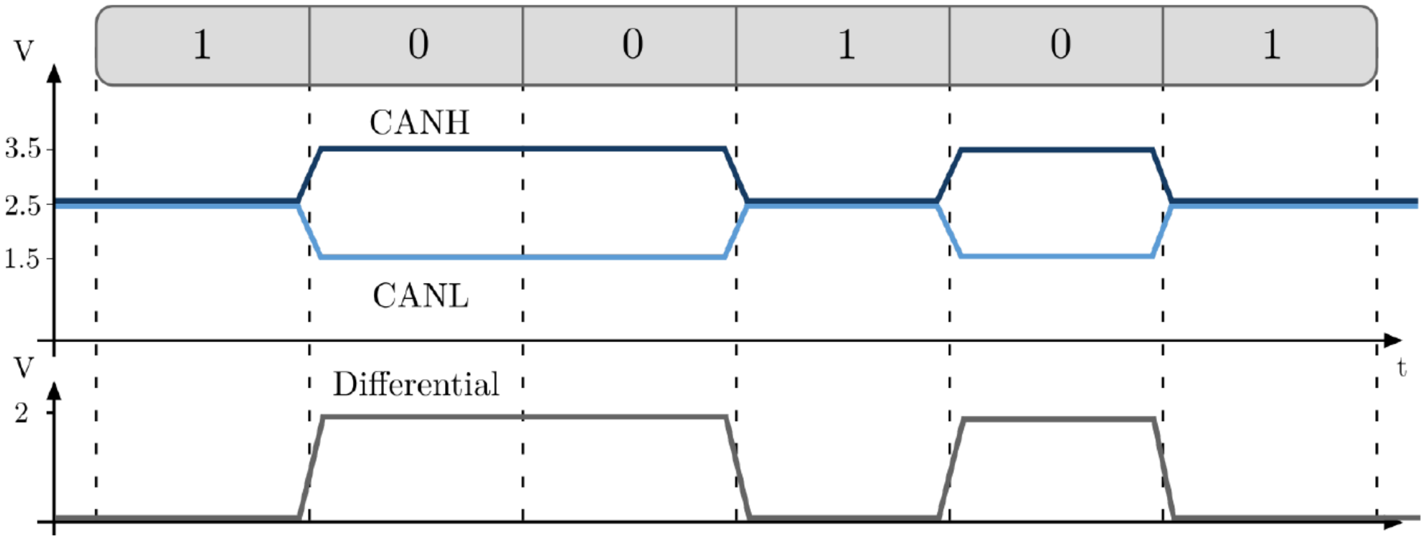


Unknown ECU Attack

Backup

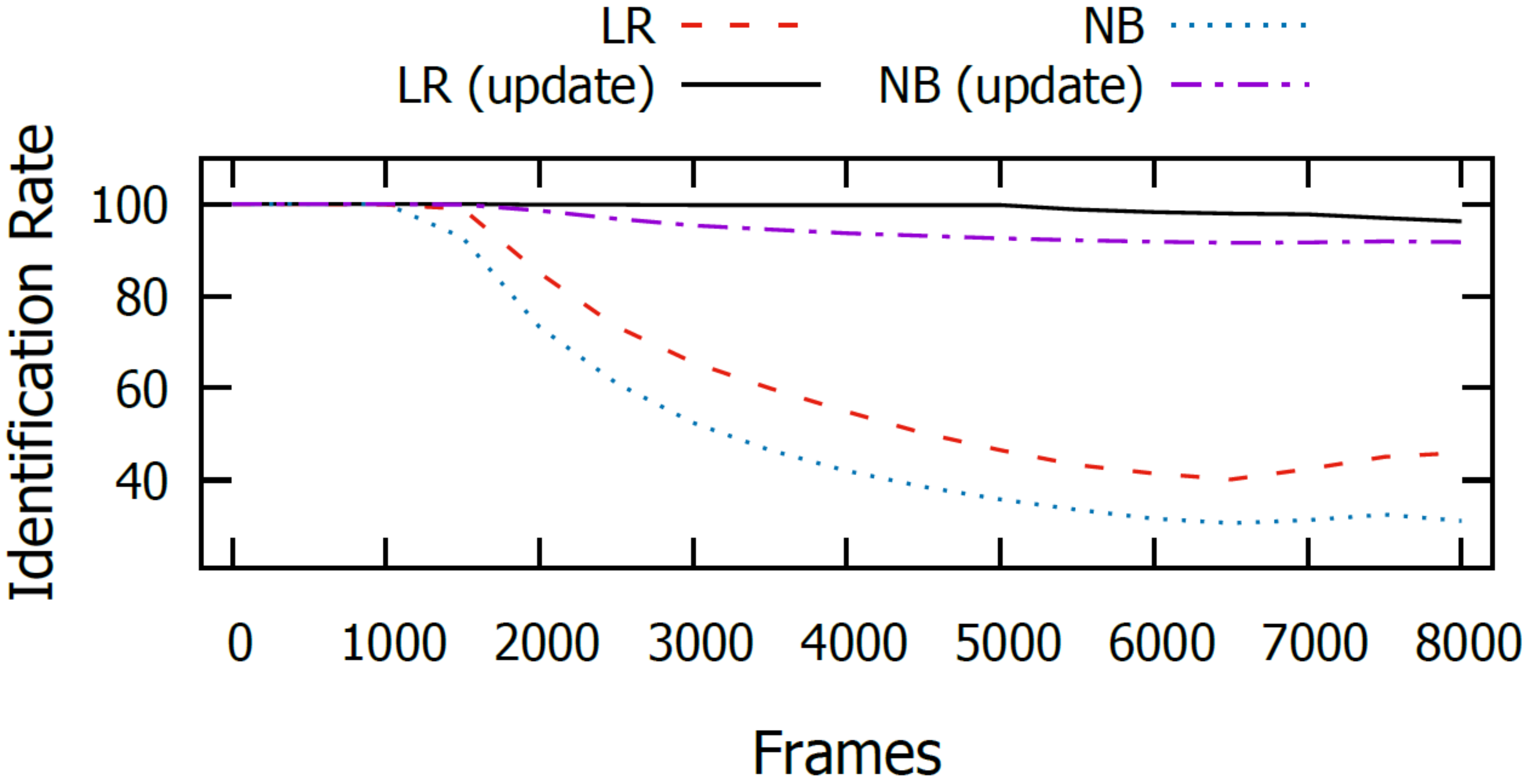
CAN Frame and Signaling





Backup

Update Mechanism


LR
NB
LR (update)
NB (update)
Identification Rate
Frames