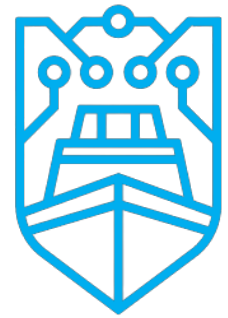
49th IEEE LCN

Hacking on the High Seas: How Automated Reverse-Engineering Can Assist Vulnerability Discovery of a Proprietary Communication Protocol

Gábor Visky, Alexander Rohl, Risto Vaarandi,
Sokratis Katsikas, Olaf Maennel

8-10 October 2024, Caen, France



MariCybERA

How Automated Reverse-Engineering Can Assist Vulnerability Discovery of a Proprietary Communication Protocol

Gábor Visky, Risto Vaarandi, Tallinn University of Technology

Sokratis Katsikas, Novegian Universitiy of Science and Technology

Olaf Maennel, Alexander Rohl The University of Adelaide

Agenda

Motivation

Methods

Results

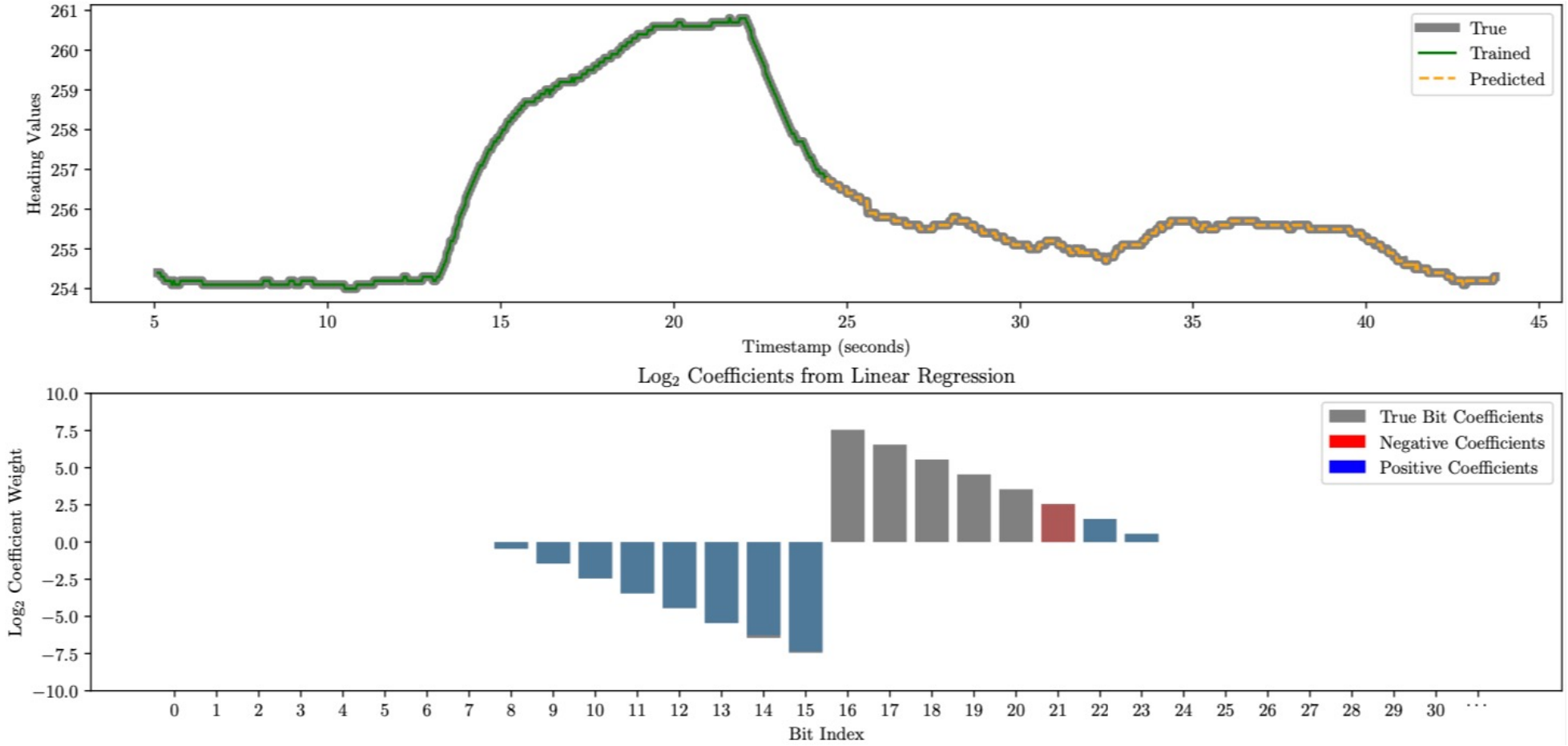
Motivation

There is room for improvement in the maritime sector regarding cyber security.

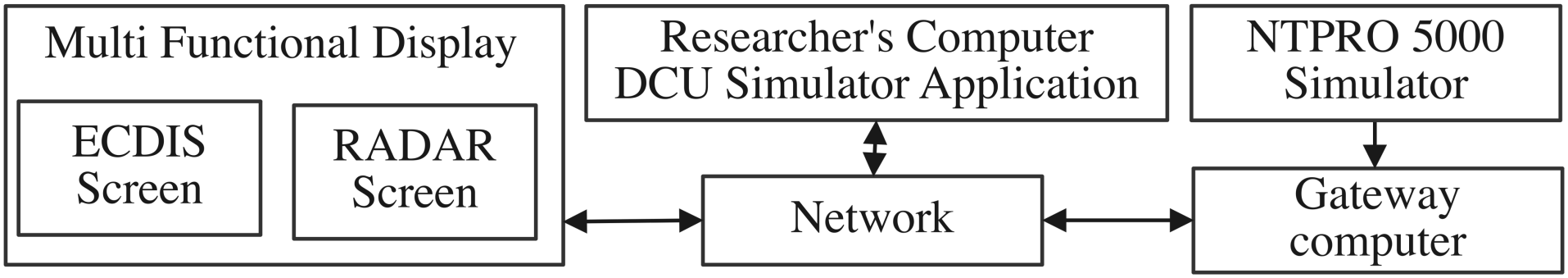
A high number of standardised and proprietary protocols are used in the field.

Manual reverse engineering of an unknown protocol is very demanding.

Automated Protocol Reverse Engineering

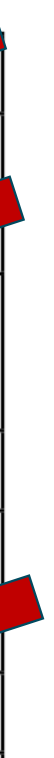


Research Environment

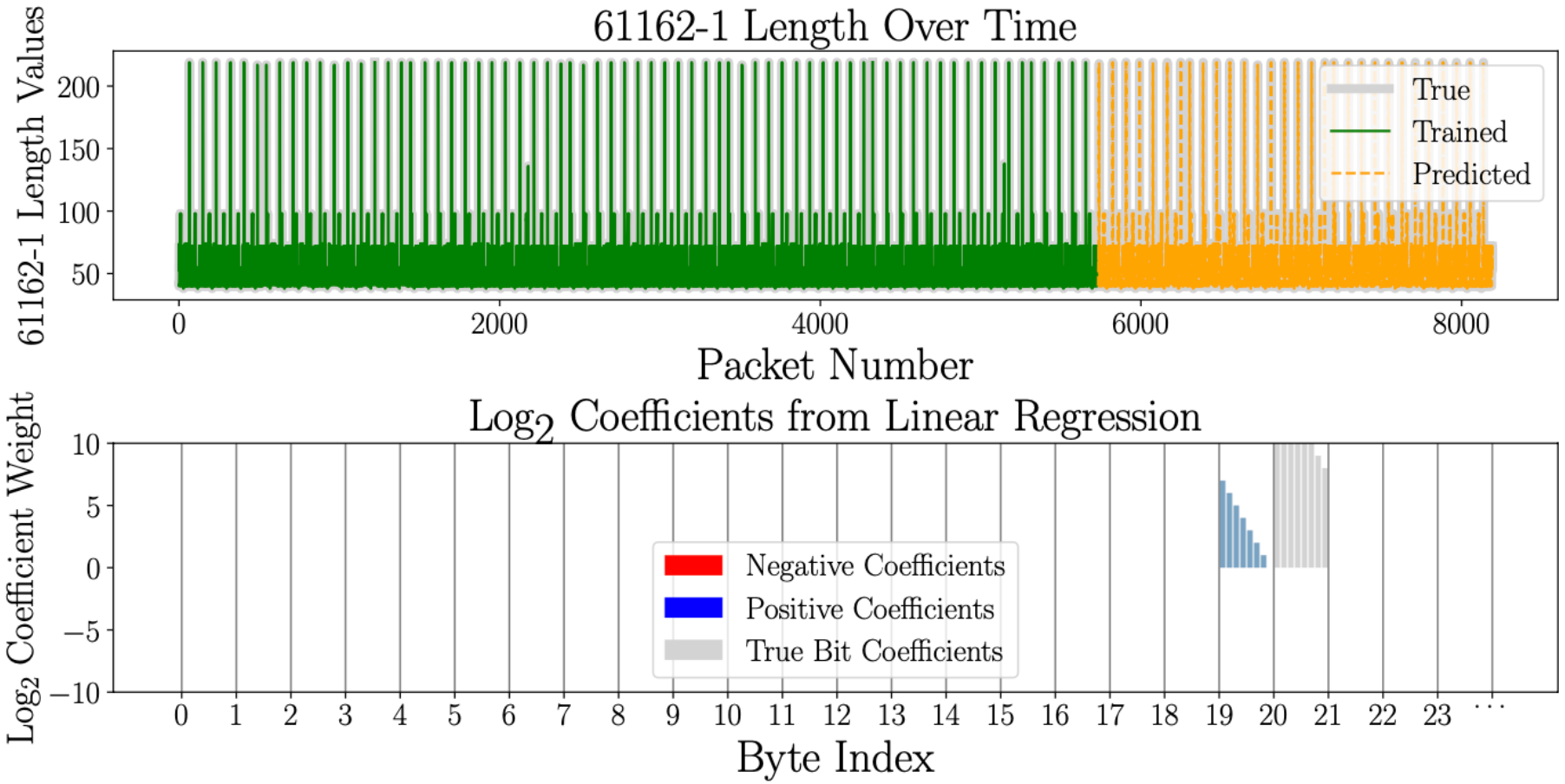


Wärtsilä (Transas) Communication Protocol

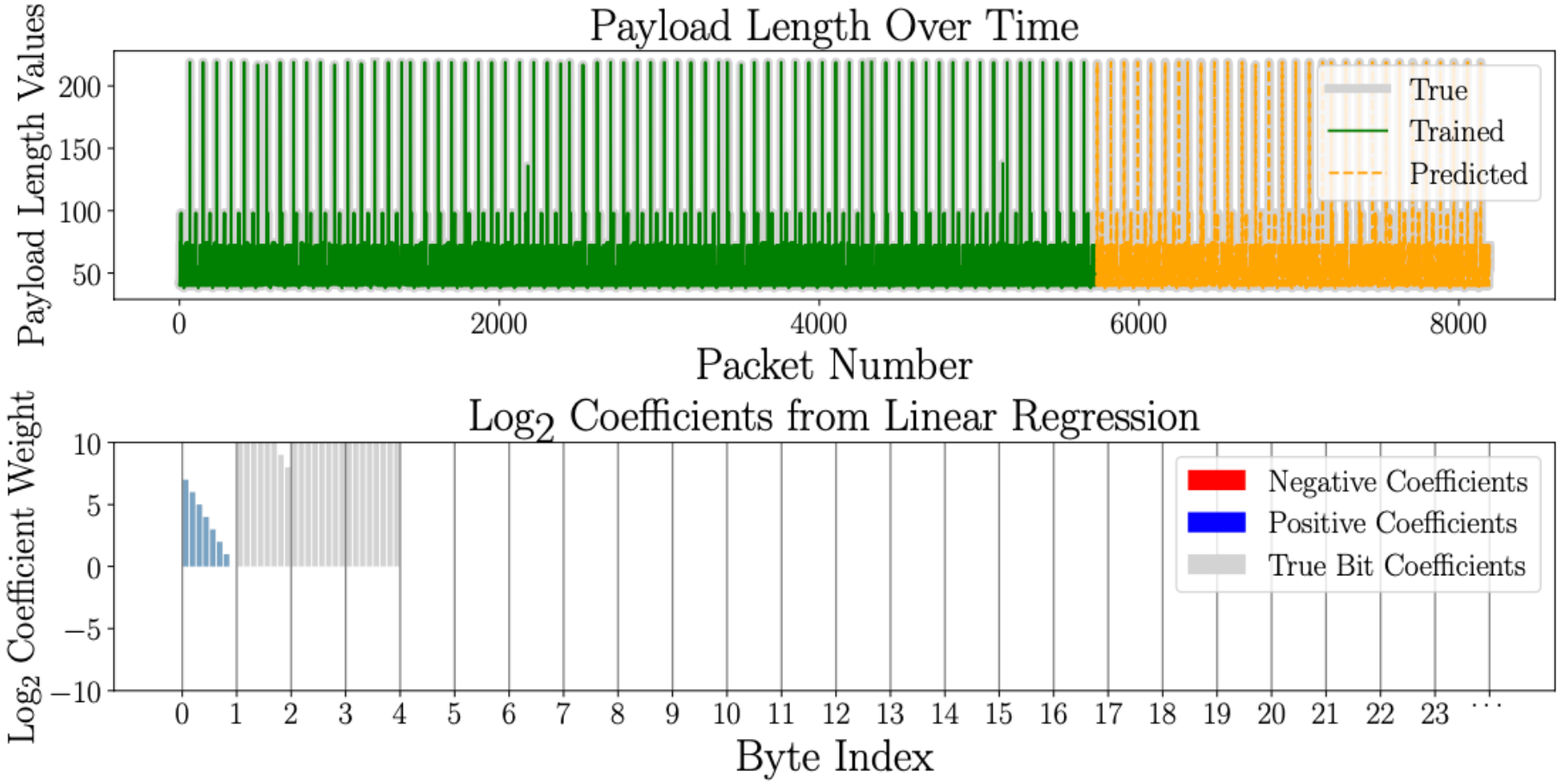
Offset	Function	Example value
00	Full length of the payload	44 00 00 00
04	Unknown/static	00
05	Timestamp Continuously increasing value	fe a7 cc 6e 9c 00 00 00
13	Sender's (DCU) IP	0a 8c 21 07
17	Message type	01
18	Channel number arrived	04
19	Length of 61162-1 data	31 00
21	Static	13 00
23	IEC61162-1 data	24 56 4d 2c 0d 0a



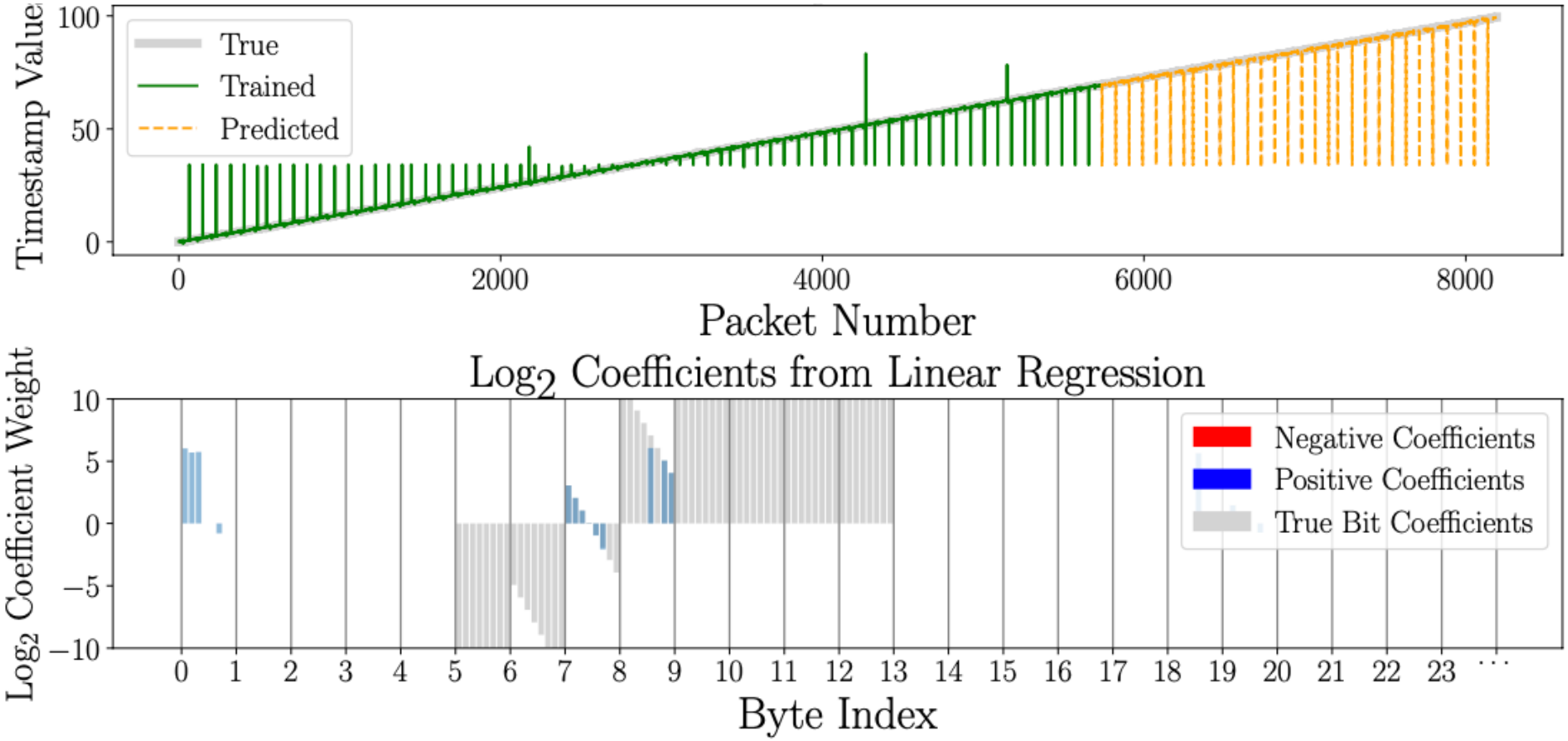
NMEA Sentence Length Field



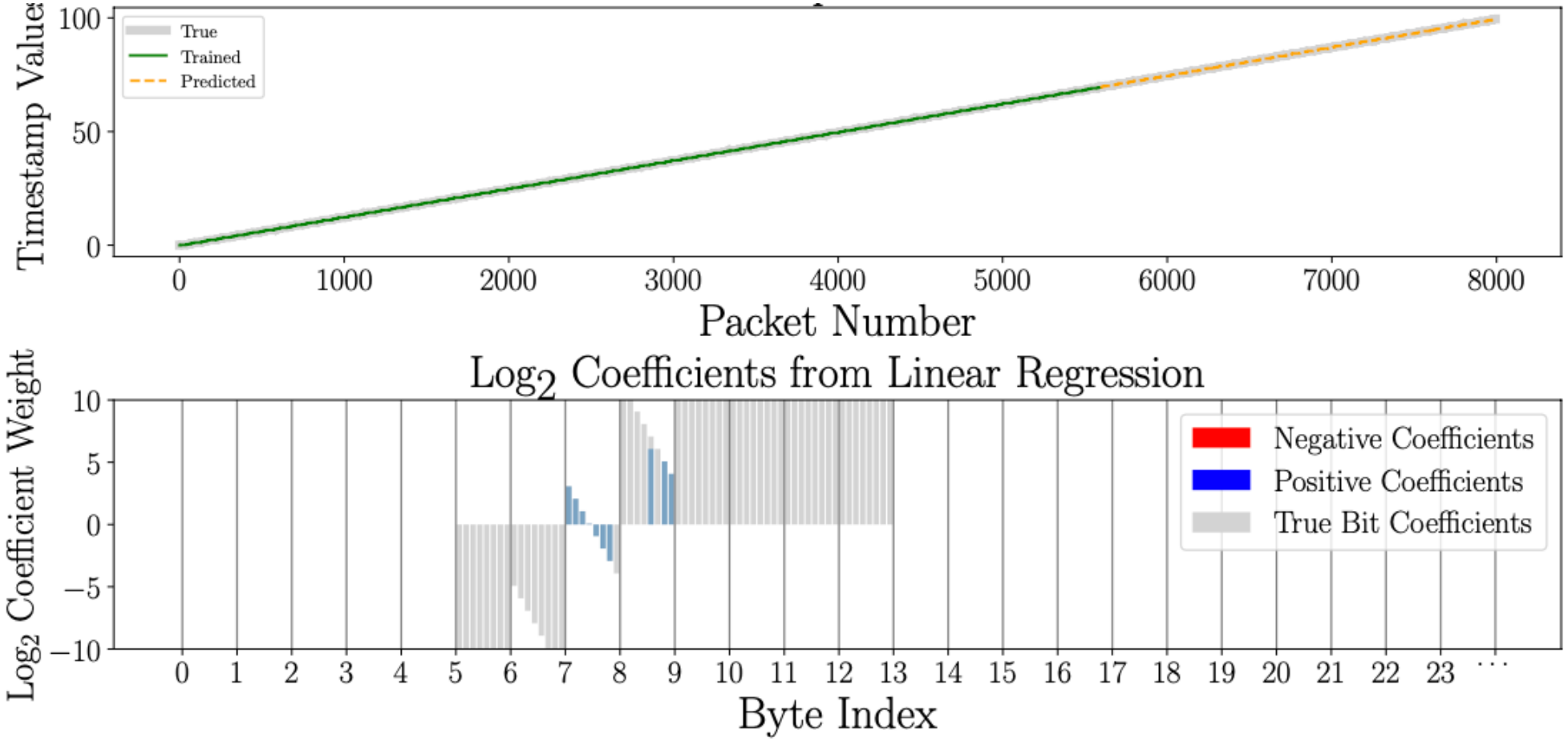
Payload Length



Timestamp


Timestamp Value
100
50
0
True
Trained
Predicted
0
2000
4000
6000
8000
Packet Number
Log2 Coefficients from Linear Regression
Log2 Coefficient Weight
10
5
0
−5
−10
Negative Coefficients
Positive Coefficients
True Bit Coefficients
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 ...
Byte Index

Corrected Timestamp

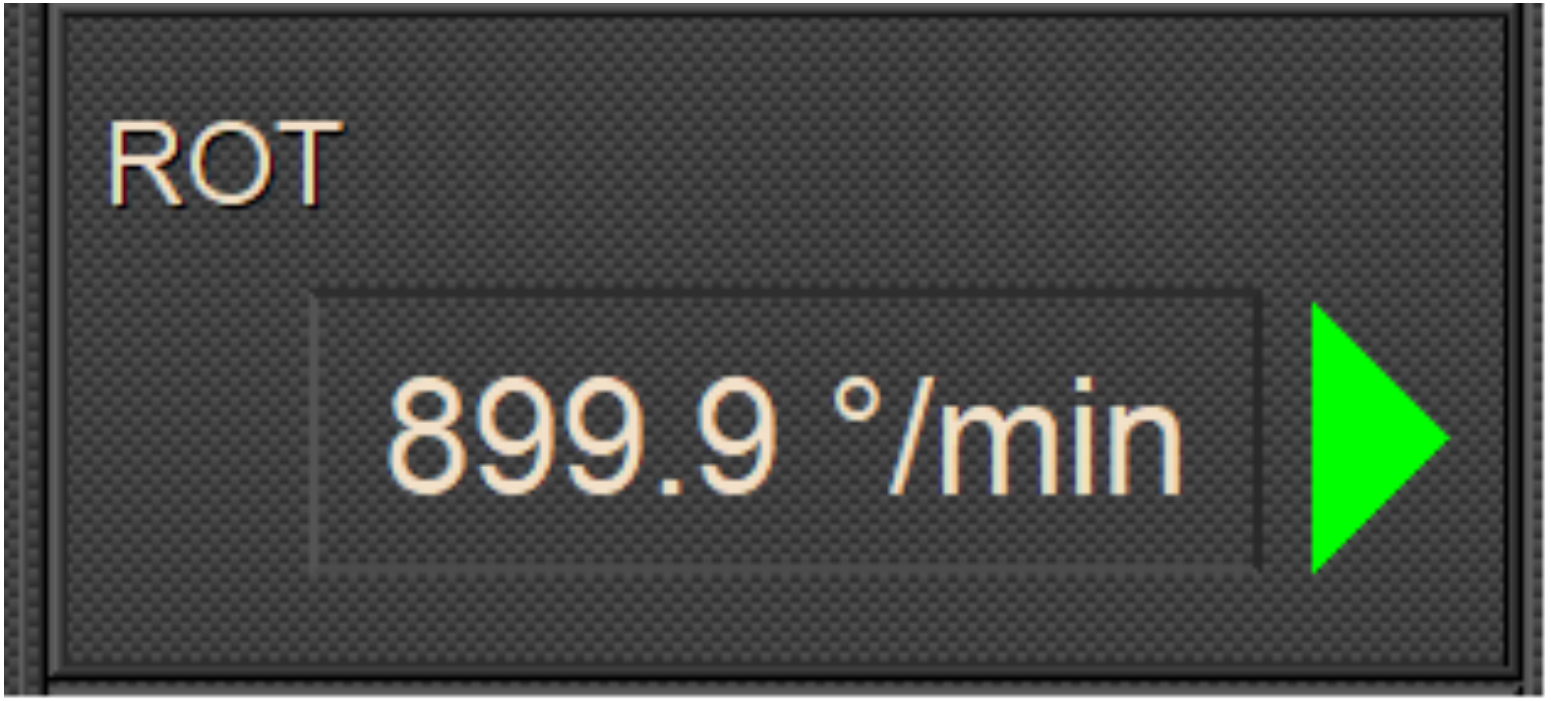


STRIDE Methodology

Threat identification

Authenticity	**S**poofing
Integrity	**T**ampering
Non-repudiation	**R**epudiation
Confidentiality	**I**nformation Disclosure
Availability	**D**enial of Service
Authorization	**E**levation of Privilege

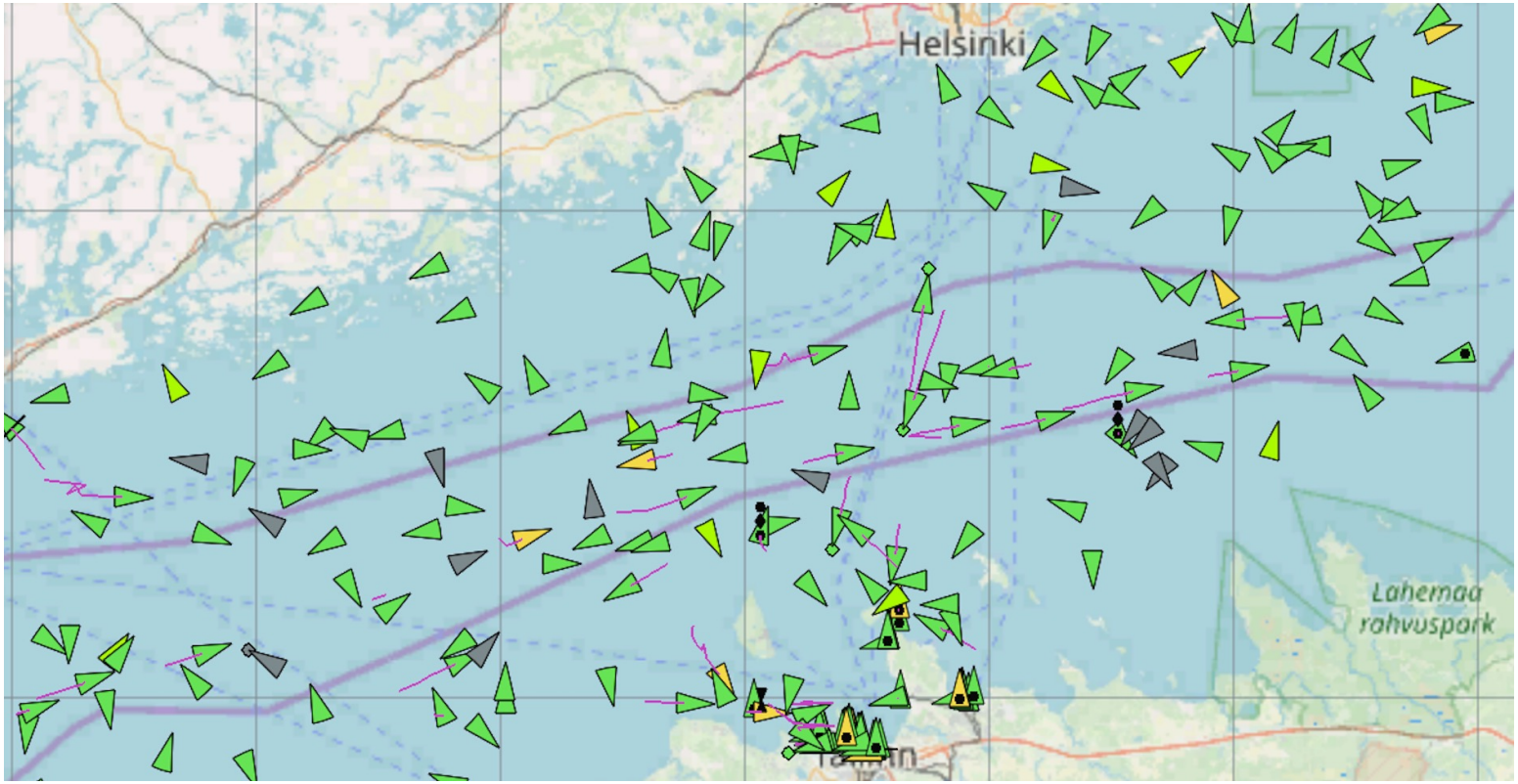
Successful attack - Spoofing



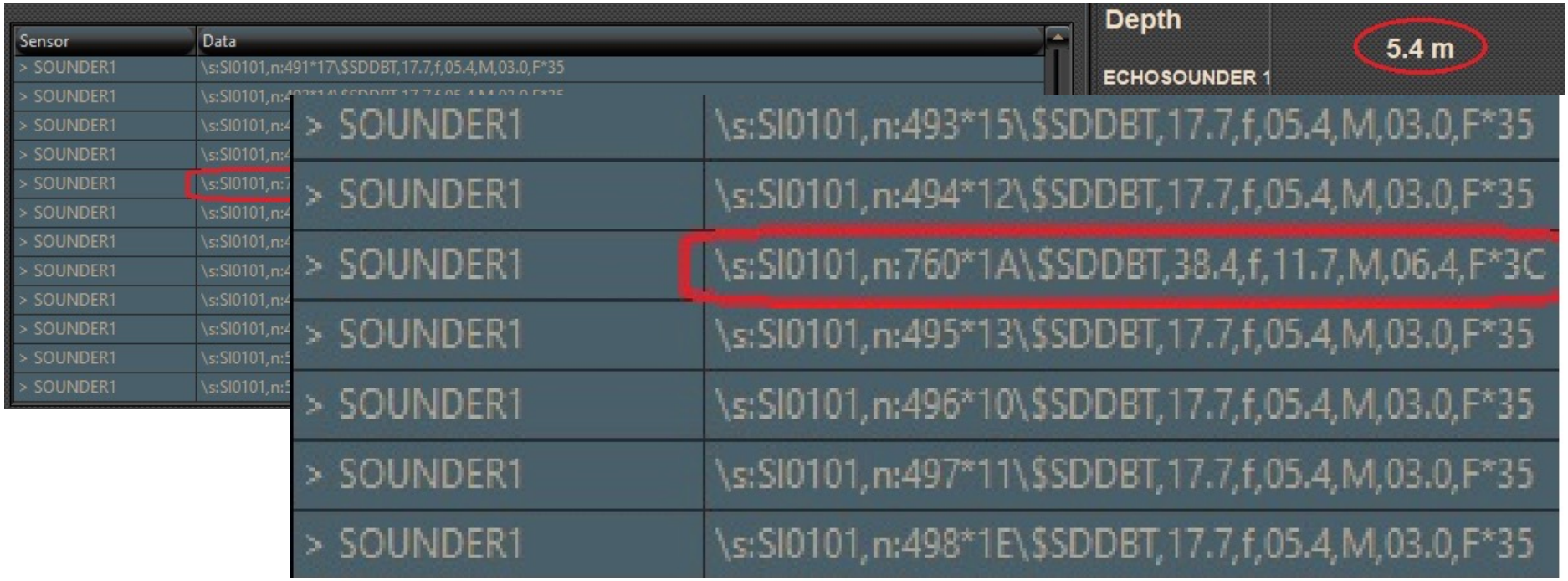
Successful attack – Information Disclosure

```
0000  02 00 00 00 45 00 00 85  9e 6e 40 00 80 06 00 00   ····E··· ·n@·····
0010  0a 8c 21 07 0a 8c 21 07  c3 63 ef 2c ee 6a d9 11   ··!···!· ·c·,·j··
0020  86 b2 b6 80 50 18 27 f6  c2 61 00 00 59 00 00 00   ····P·'· ·a··Y···
0030  00 c6 53 d3 6e 9c 00 00  00 0a 8c 21 07 01 00 46   ··S·n··· ···!···F
0040  00 13 00 24 47 50 47 47  41 2c 31 33 30 30 30 30   ···$GPGG A,130000
0050  2c 34 39 35 33 2e 38 31  38 32 34 31 2c 4e 2c 30   ,4953.81 8241,N,0
0060  30 36 31 36 2e 39 39 30  38 37 38 2c 57 2c 32 2c   0616.990 878,W,2,
0070  34 2c 30 2e 39 2c 31 31  2e 30 2c 4d 2c 2c 2c 31   4,0.9,11 .0,M,,,1
0080  2c 38 39 36 2a 30 32 0d  0a                       ,896*02· ·
```

Successful attack - Tampering



Successful attack – Water depth modification



IEEE NTNU TAL TECH MariCybERA THE UNIVERSITY of ADELAIDE

Conclusion

APRE can be successfully used on this protocol.

The introduced details of the proprietary protocol can be directly used in cyber-related operations.

The executed attacks show the protocol's weaknesses exploitation.

MariCybERA

Thanks for your attention!

This research was funded by the EU Horizon2020 project MariCybERA (agreement No 952360)

https://maricybera.taltech.ee/

IEEE NTNU TAL TECH MariCybERA THE UNIVERSITY of ADELAIDE