Fraunhofer FKIE

Hochschule Bonn-Rhein-Sieg
University of Applied Sciences

Felix Klör, Jan Bauer, Sachar Paulus, Michael Rademacher

Dude, Where's That Ship?

Stealthy Radio Attacks Against AIS Broadcasts

Introduction

Automatic Identification System (AIS)

- **Broadcast position and identification data of vessels**
- **Uses radio for decentralized data transmission**
- **Messages are not encrypted or authenticated**
- **Related work**

  DoS:

  - Continues jamming & slot starvation*

  Selective DoS:

  - Frequency hopping* & Timing attacks*

Display unit of a class-A AIS station

*Balduzzi et al. *"A Security Evaluation of AIS"*

Motivation

Improving the security of AIS

- **Security of AIS can only be improved by identifying new vulnerabilities**
- **Purpose of AIS: Safety of people and the environment**
  - Prevent collisions with other vessels or objects
  - Monitoring of busy waterways
  - Support SAR operations

Objective

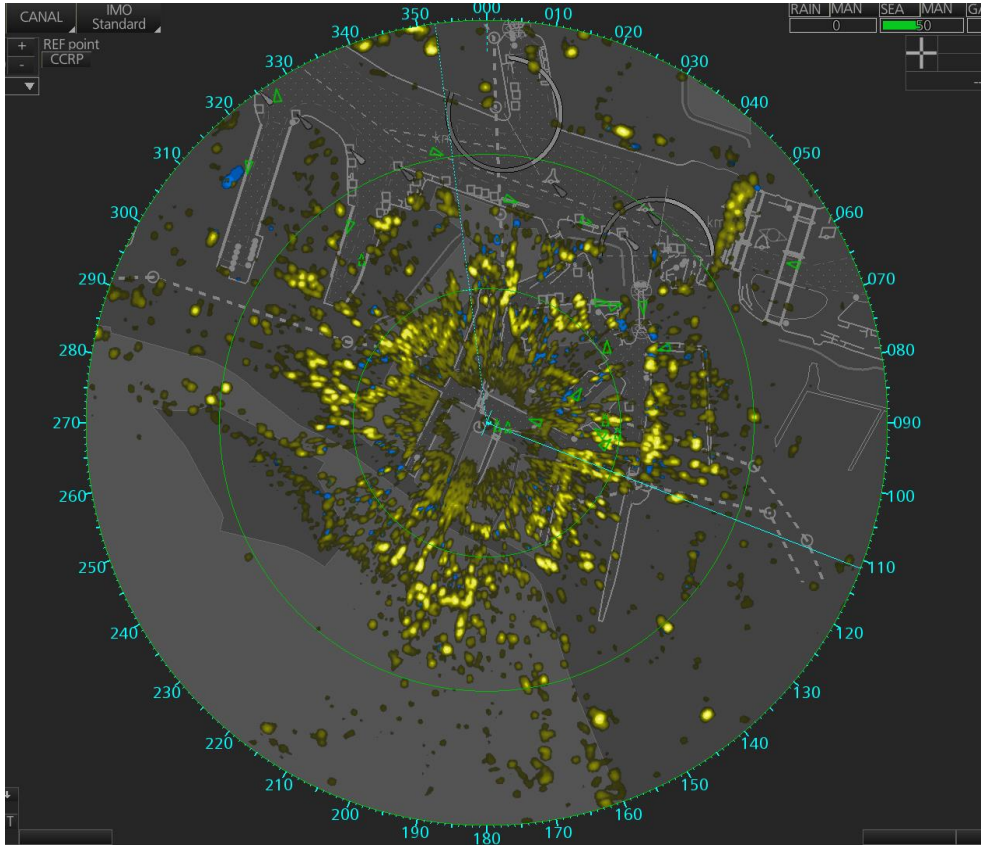
Finding a new attack vector

- ***What?***

  Let selected vessels disappear on the display of an AIS station.
  This could lead to a collision between different vessels.

- ***How?***

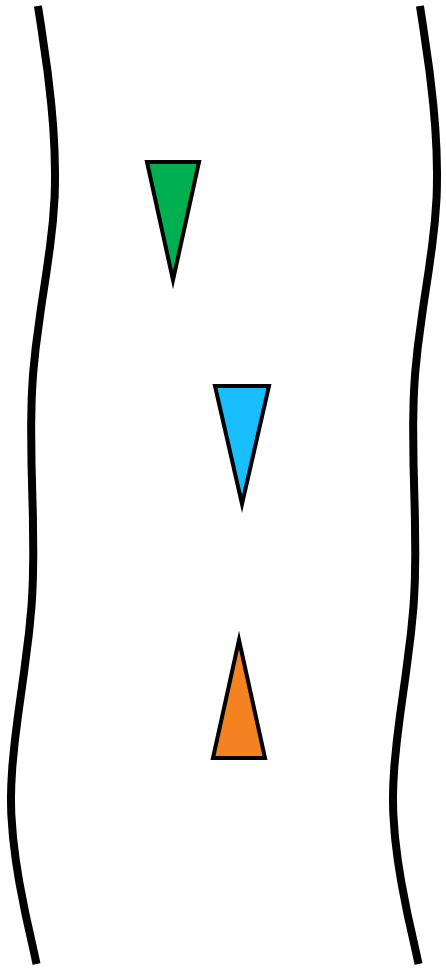
  Perform a sophisticated jamming attack that **only** jams the messages of a selected vessels.
  Exploiting the AIS channel access scheme.



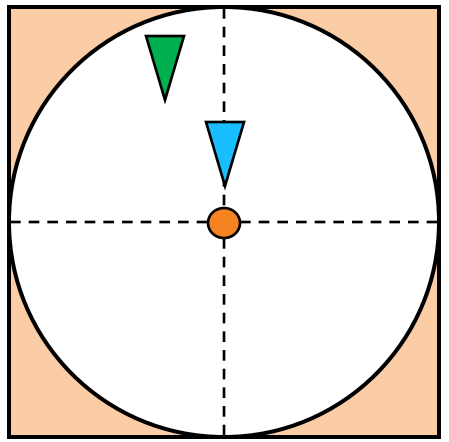
ECDIS unit: AIS & radar

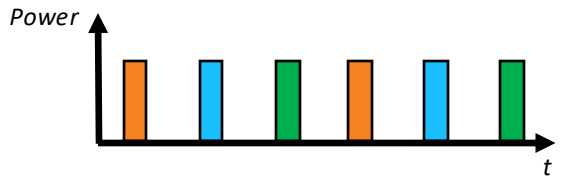
Attacking AIS: Basic idea

Benign scenario



Victim vessel

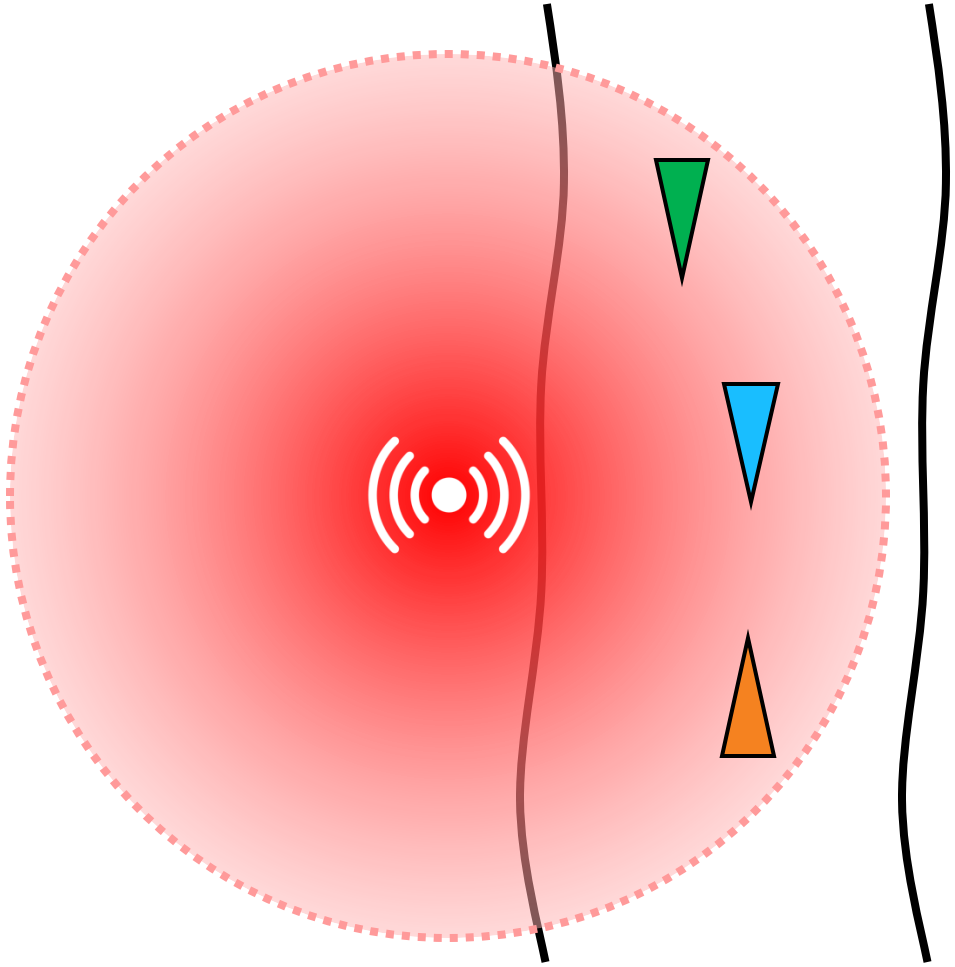




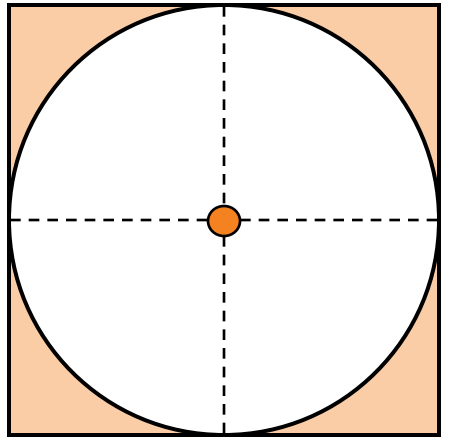
Simplified representation

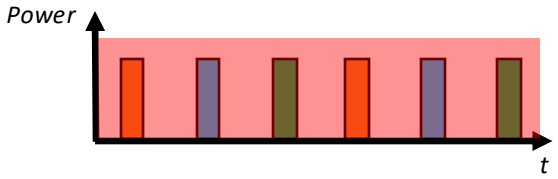
Attacking AIS: Basic idea

Continuous jamming



Victim vessel

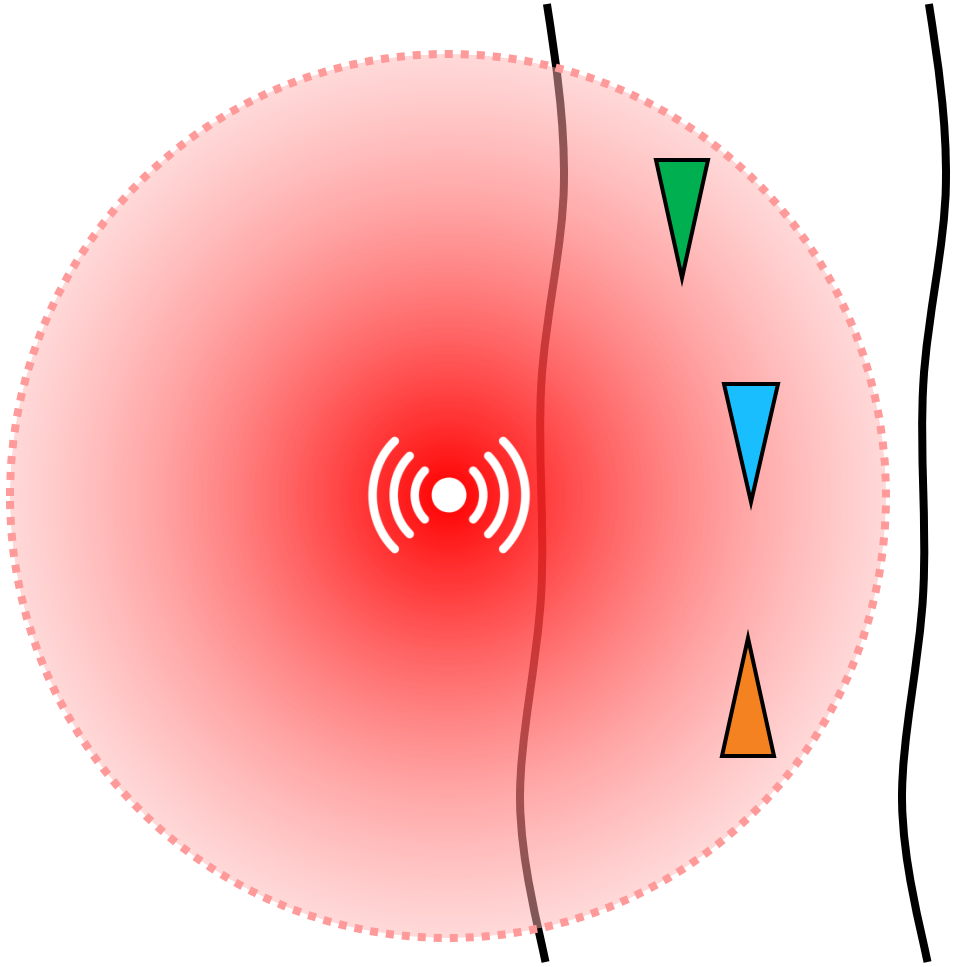




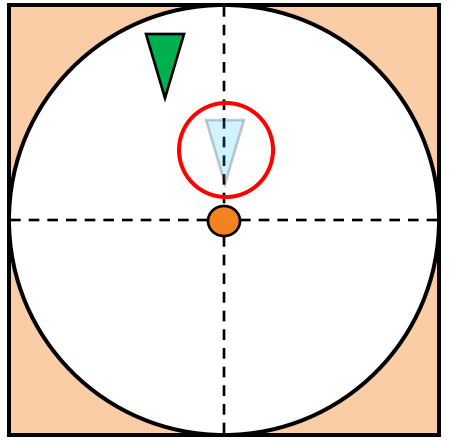
Simplified representation

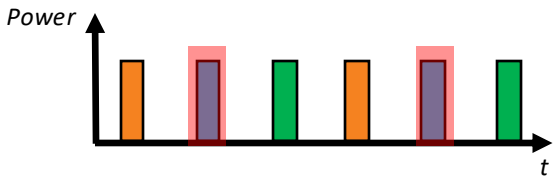
Attacking AIS: Basic idea

Selective jamming



Victim vessel



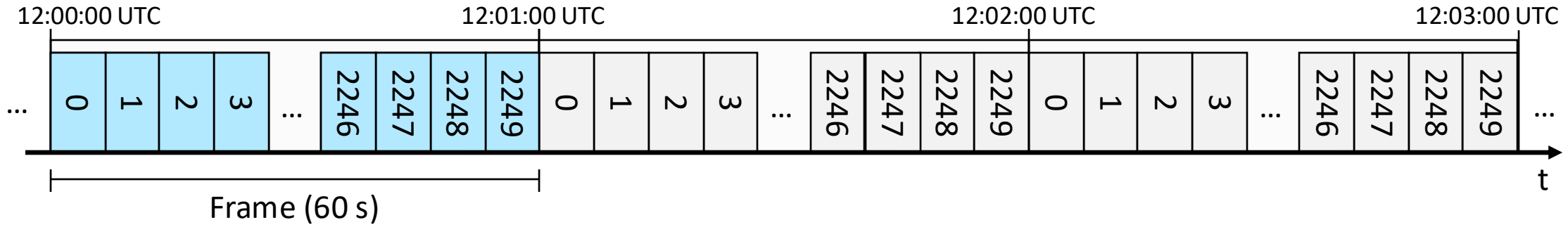


Simplified representation

AIS – Message scheduling algorithm

TDMA - Time Division Multiple Access

How could we jam individual messages?



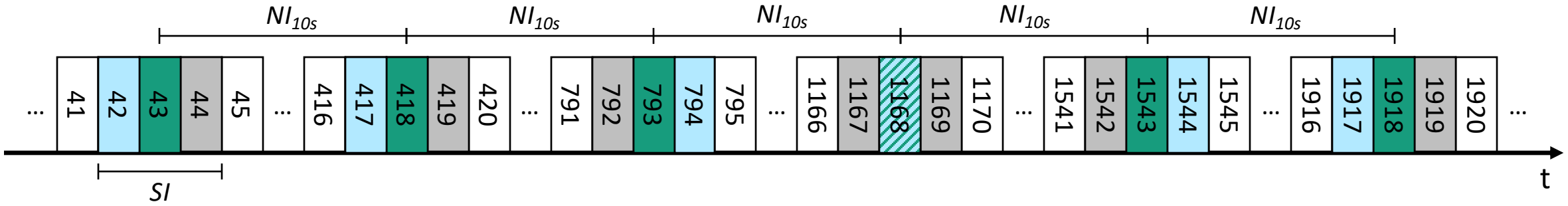
Simplified representation

AIS – Message scheduling algorithm

SOTDMA – Self Organizing Time Division Multiple Access

0 – 14 knots

10 seconds / 375 Slots



NTS NS

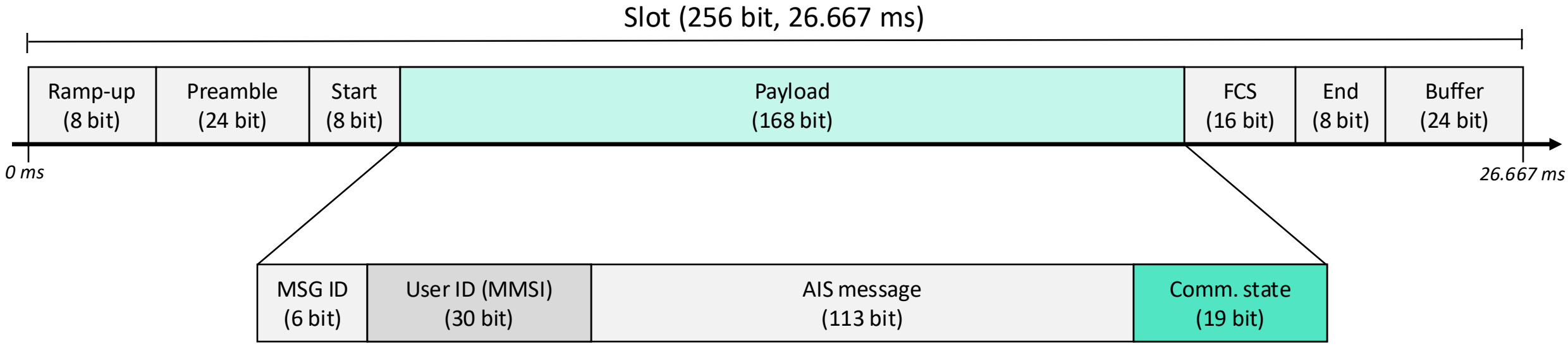
Communication state

Timeout	3 - 7
Slot offset	Timeout: 0
Slot number	Timeout: even

Simplified representation

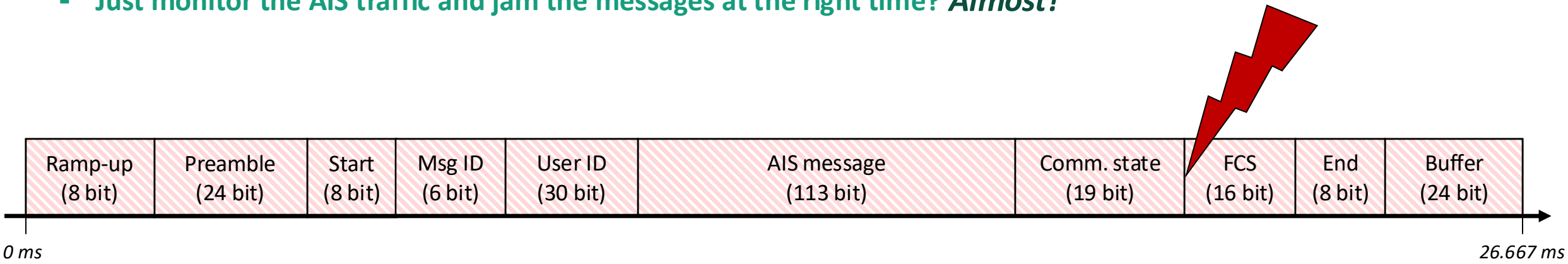
AIS – Message scheduling algorithm

SOTDMA message structure



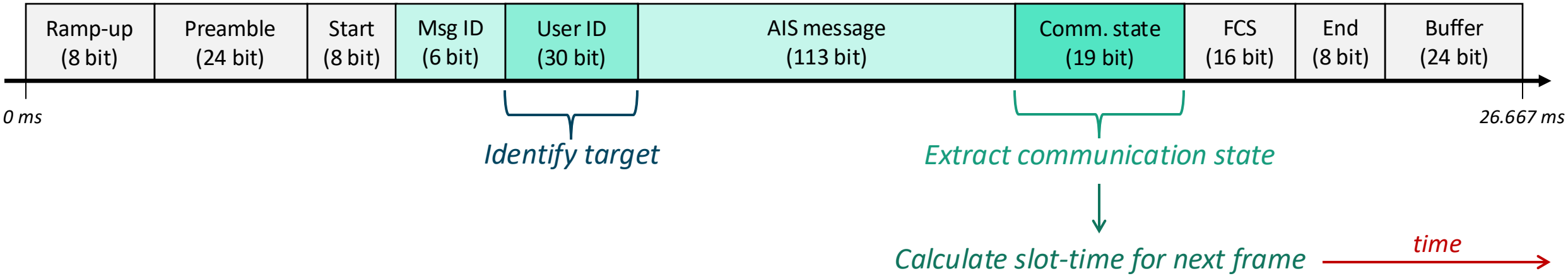
Selective jamming
Attack concept

- **Message transmission times are deterministic!**
- **Just monitor the AIS traffic and jam the messages at the right time? *Almost!***



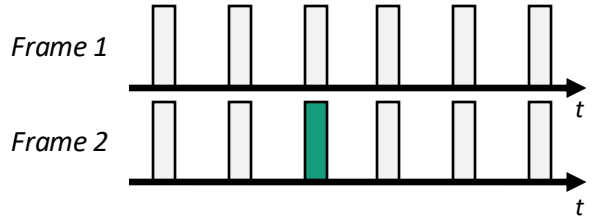
Selective jamming
Attack procedure

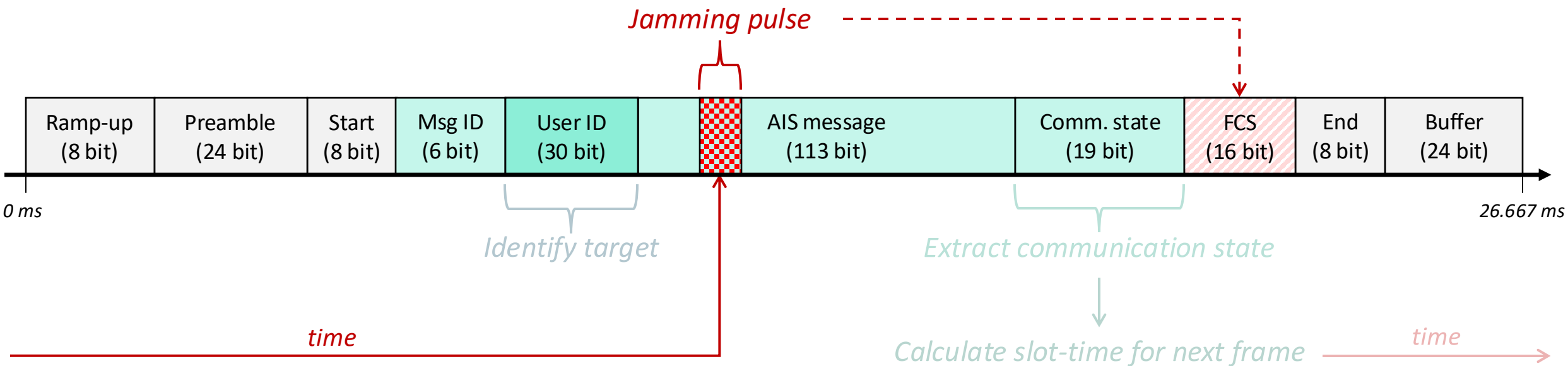
Frame 1



Selective jamming
Attack procedure

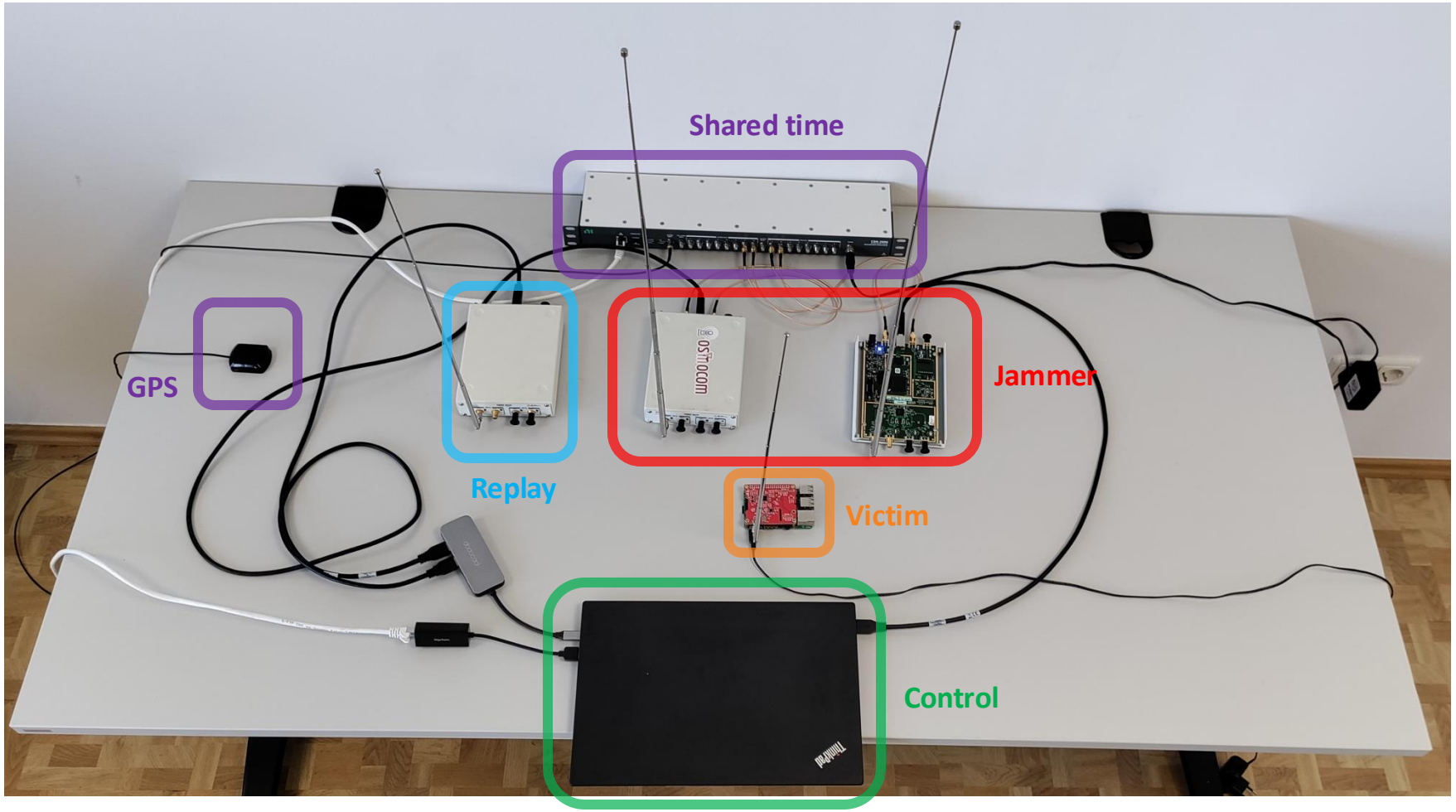
Frame 2





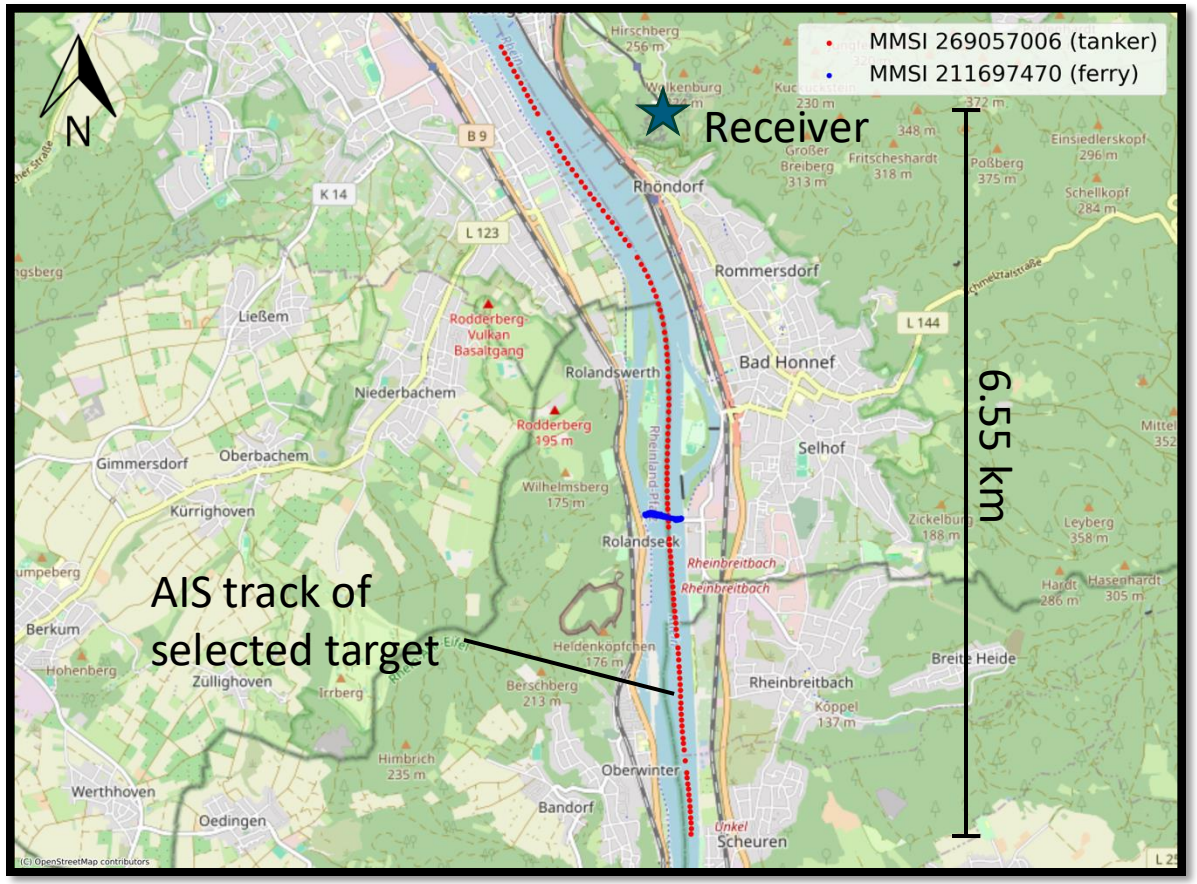
Selective jamming

Laboratory experiment – setup



Selective jamming

Laboratory experiment – record real AIS data

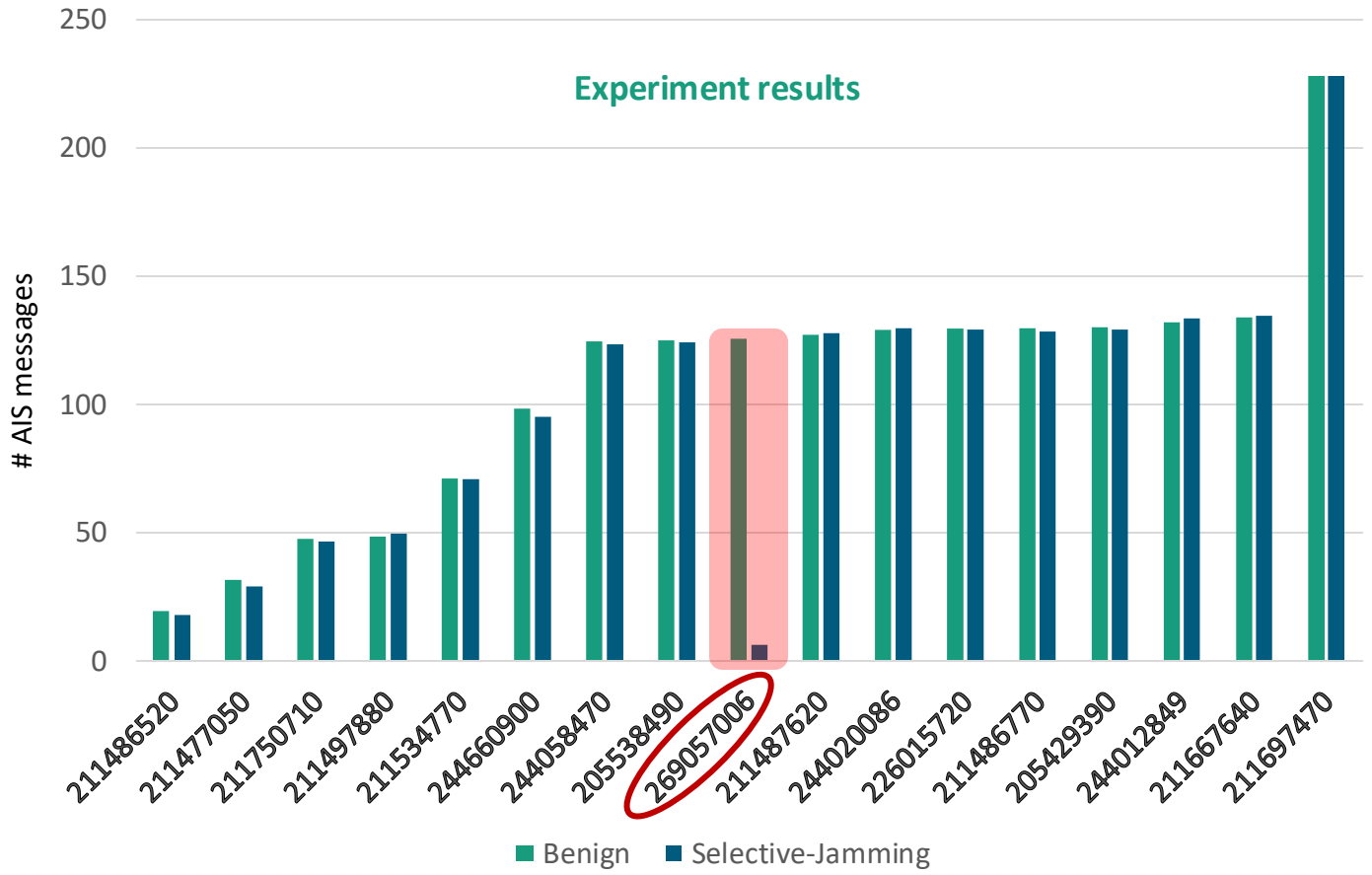


Selective jamming

Laboratory experiment – results

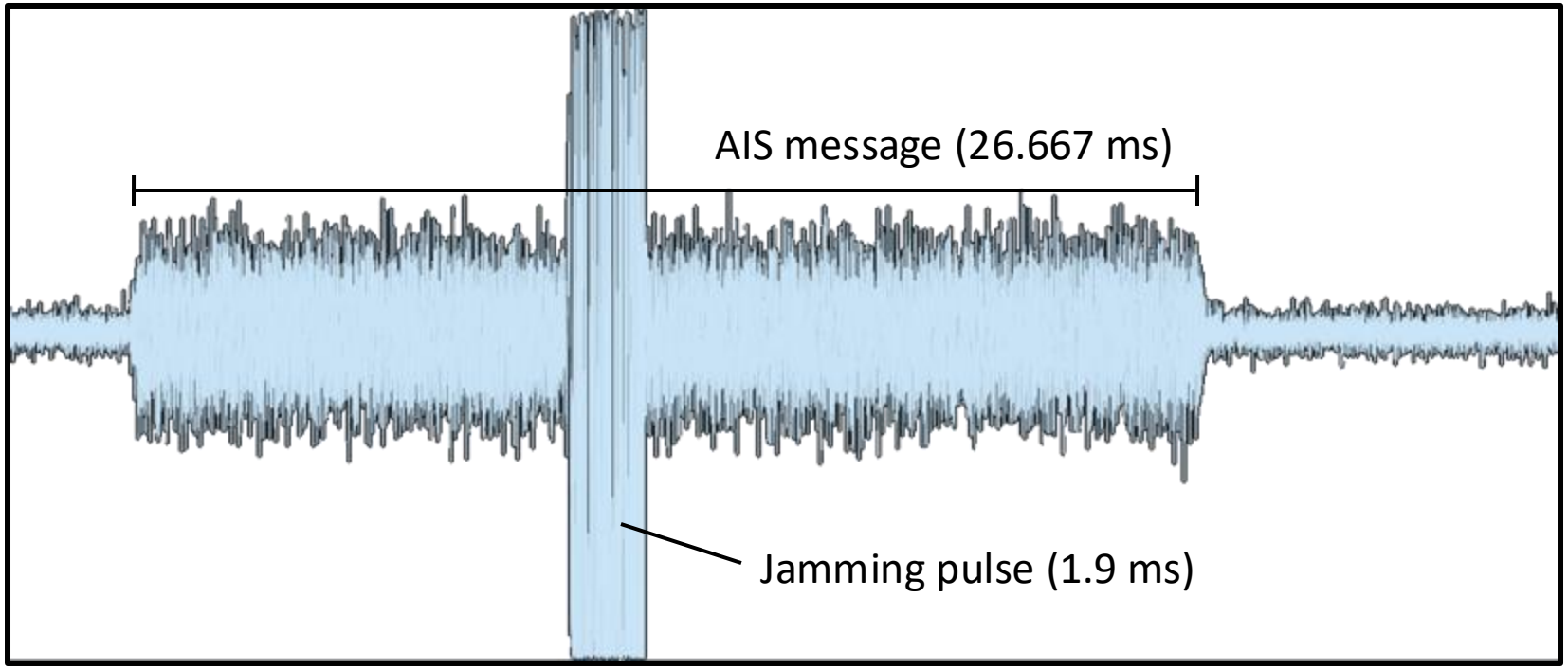
AIS recording stats

Duration	21.5 min
Size	10.32 GB
Individual vessels	30
All AIS messages	2178
Messages / Type	*1* (1806), *3* (243), *5* (56), *8* (59)



Selective jamming

Single message jammed



Conclusion / Future Work

1. ***Identification of a new jamming attack which can selectively jam messages from individual ships.***

2. ***Implement the attack with the help of GNU radio and SDRs.***

3. ***Demonstrate in a laboratory experiment that this attack can be carried out successfully.***

Future work:

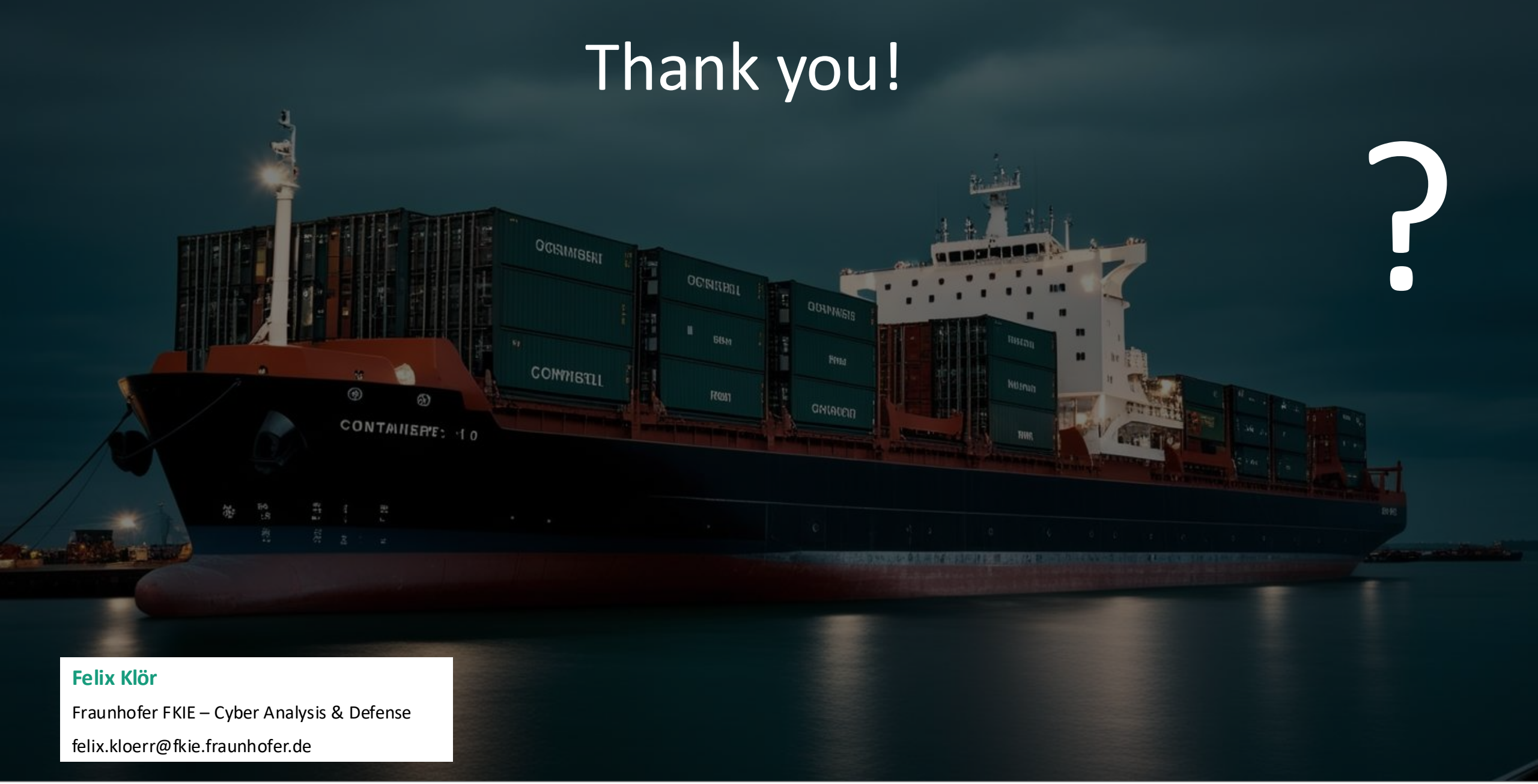
- Perform the attack against real hardware

- Overshadowing / TDMA true spoofing

- Support multiple targets / edge cases

@Fraunhofer CML

Thank you!



?

Felix Klör

Fraunhofer FKIE – Cyber Analysis & Defense

felix.kloerr@fkie.fraunhofer.de