Security Analysis of Skybrake DD5 immobilizer

Daniel Würsch

Institute of Computer Science
University of Tartu

27 August 2024

Table of Contents

1 Introduction

2 Black-box Analysis

3 Attack Vectors

4 Conclusion

About car immobilizers

- Aim to prevent car theft by immobilizing the car
- Additional security layer to already existing locking mechanism
- Authenticate authorized driver by transponder or smart key

Types of car immobilizers

Factory-fitted car immobilizer

- Installed by car manufacturer
- Integrated into regular key fob of car
- Mandatory in most countries for new cars

After-market car immobilizer

- Retrofitted for cars without secure factory-fitted car immobilizer
- Installed by authorized service partner
- Adaption driven by insurance policies

Skybrake DD5 by Autonams

Table of Contents

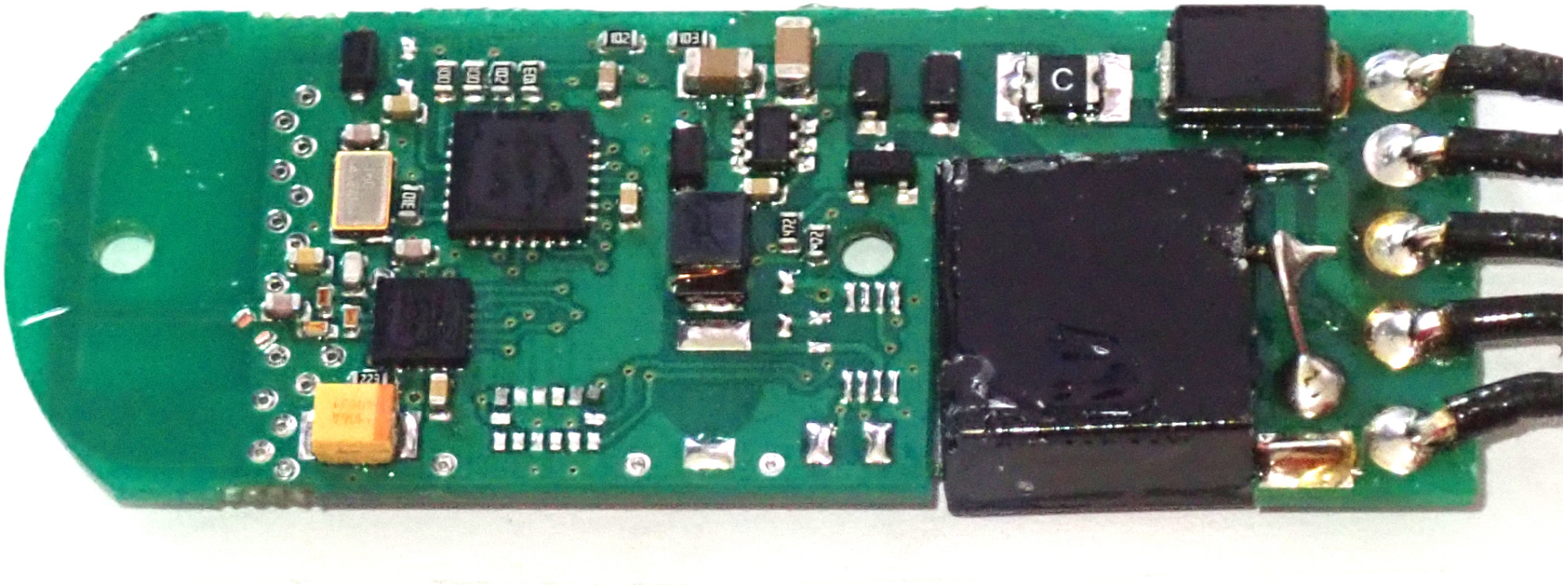
1 Introduction

2 Black-box Analysis

3 Attack Vectors

4 Conclusion

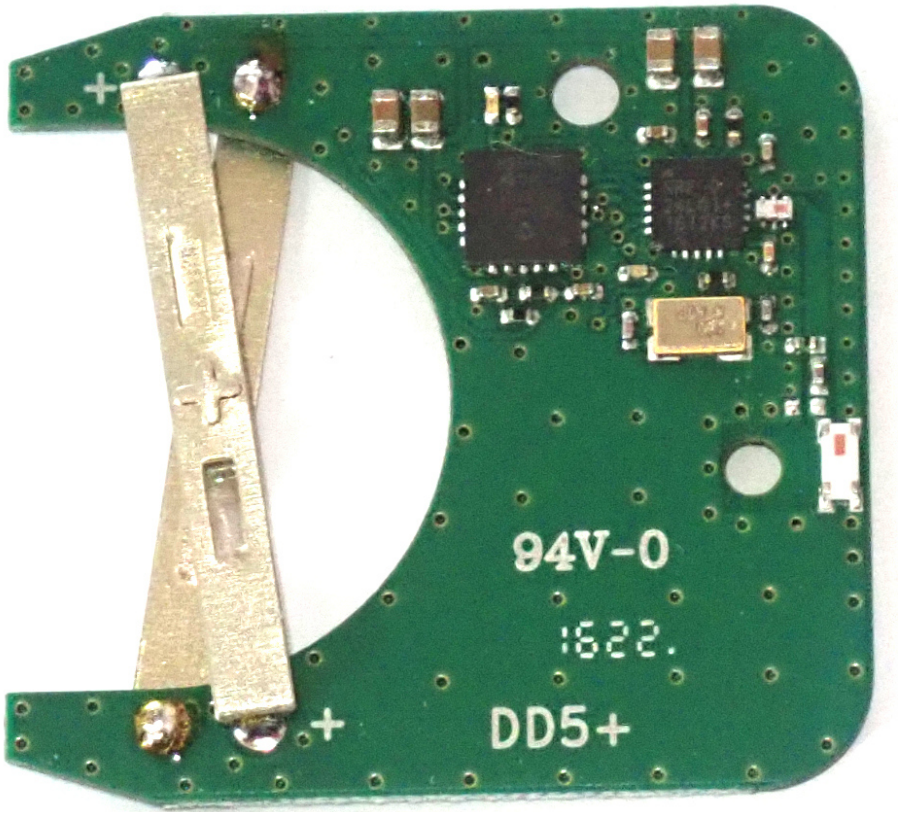
Visual inspection: Control unit



Microcontroller: Microchip PIC24F32KA302

Transceiver Chip: Nordic Semiconductor NRF24L01+

Visual inspection: Personal transceiver



Microcontroller:

Microchip PIC24F16KA101

Transceiver Chip:

Nordic Semiconductor NRF24L01+

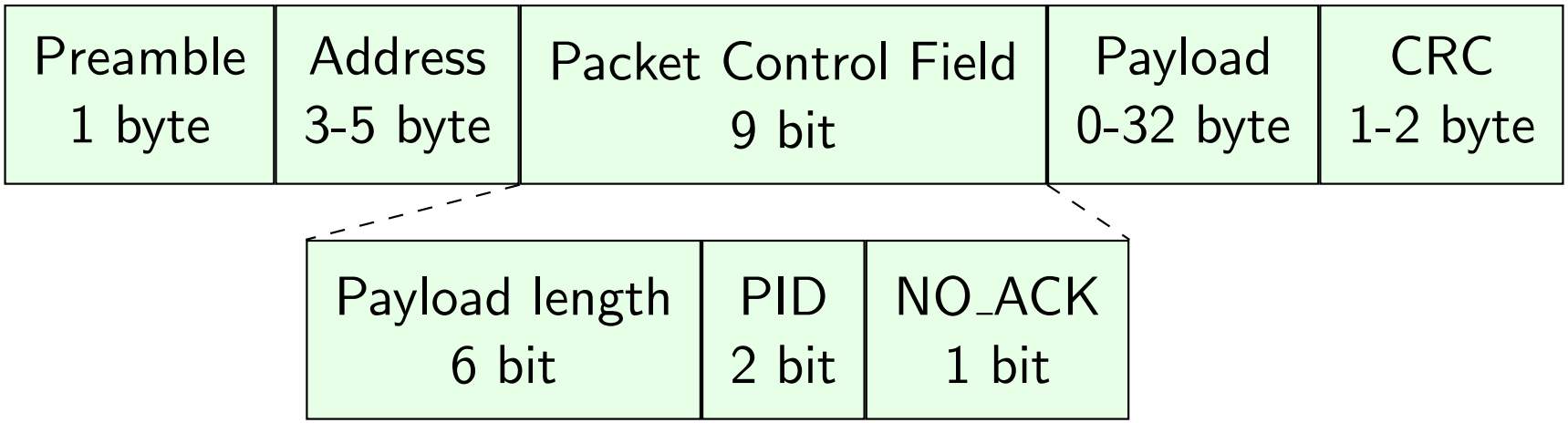
Capturing Messages

- Data available from the datasheet

  Modulation: Gaussian Frequency Shift Keying (GFSK)

  Frequency: 2400 – 2525 MHz (126 channels)

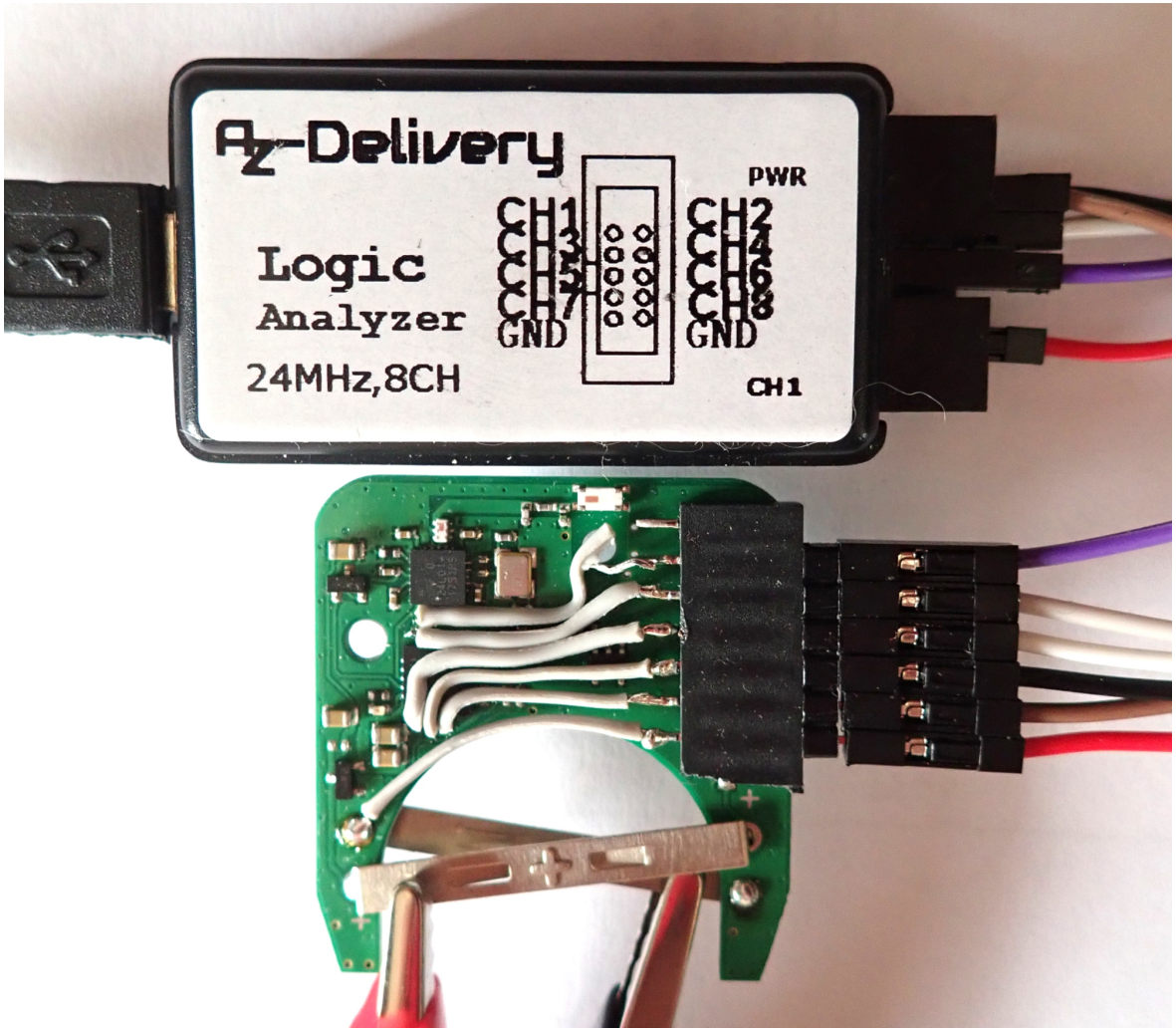
  Packet format as shown below



- Just capture data using a software defined radio (SDR)?

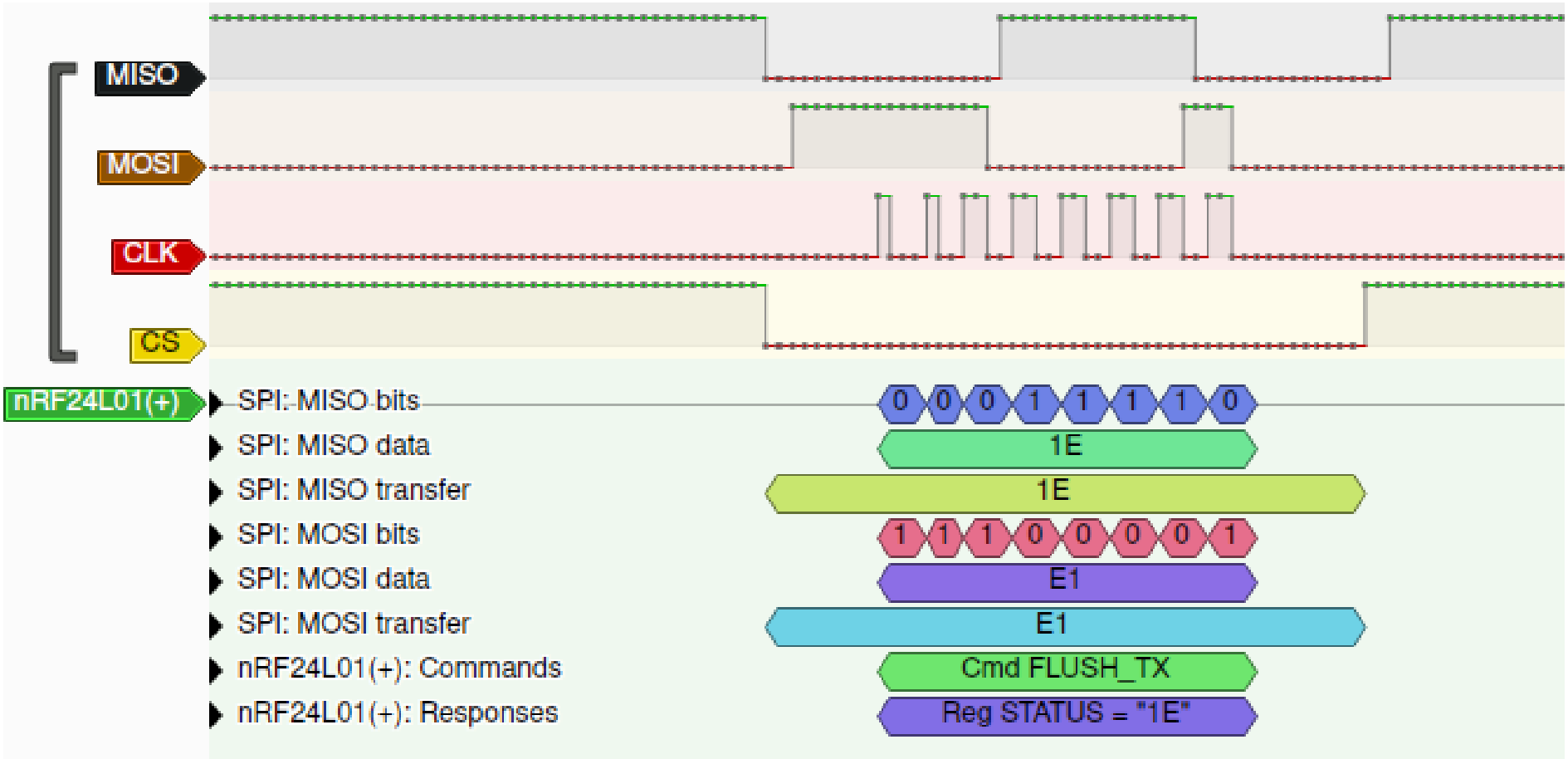
Serial Peripheral Interface

Capturing Signals



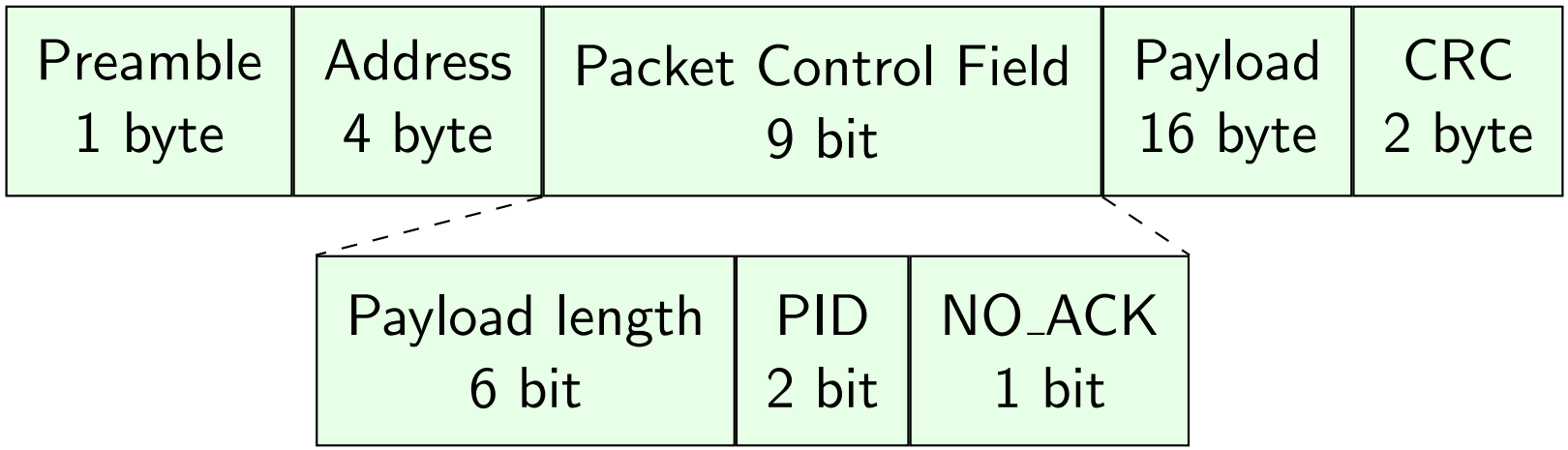
Serial Peripheral Interface

Decoding Signals

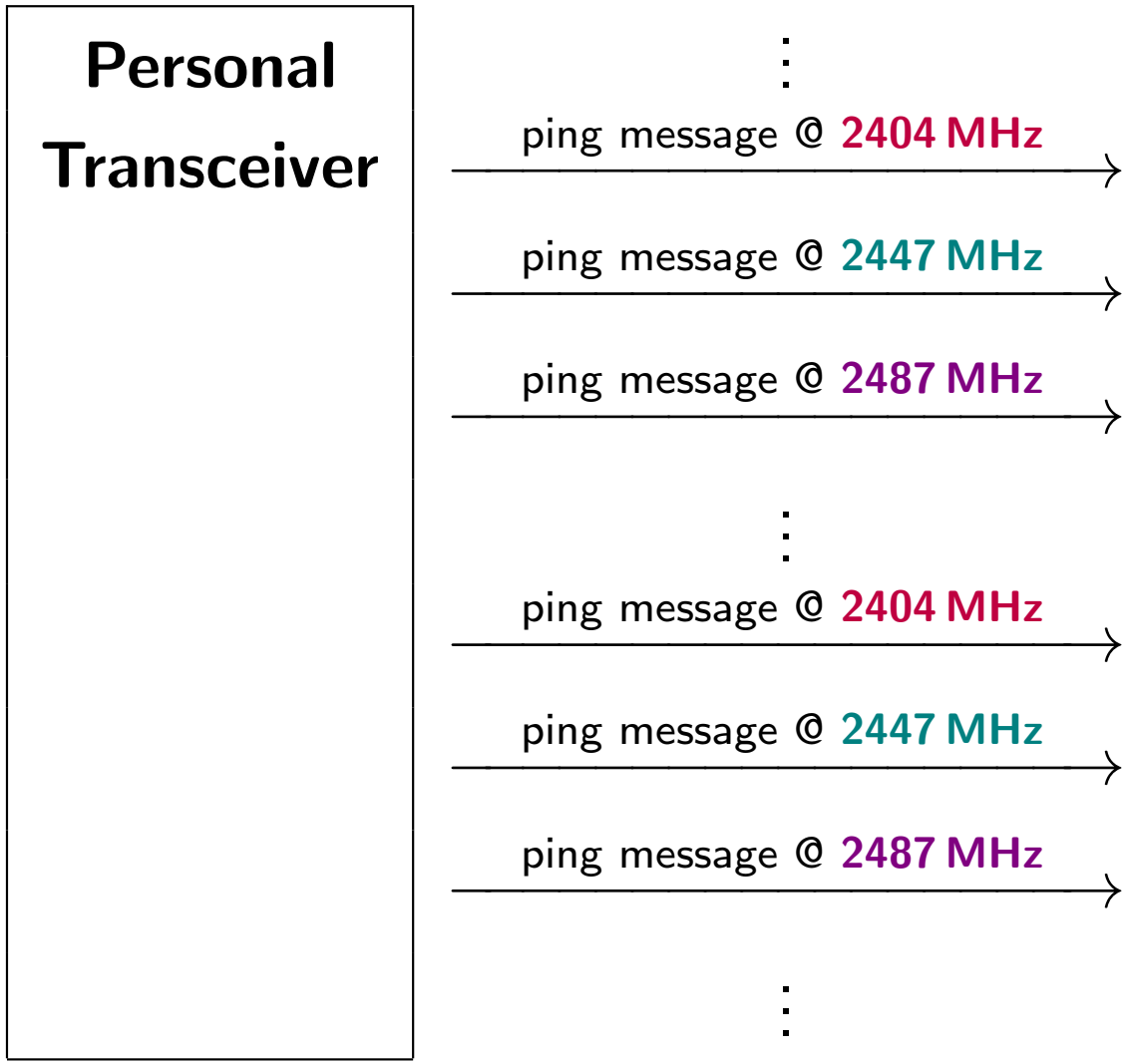


Packets sent by Skybrake DD5

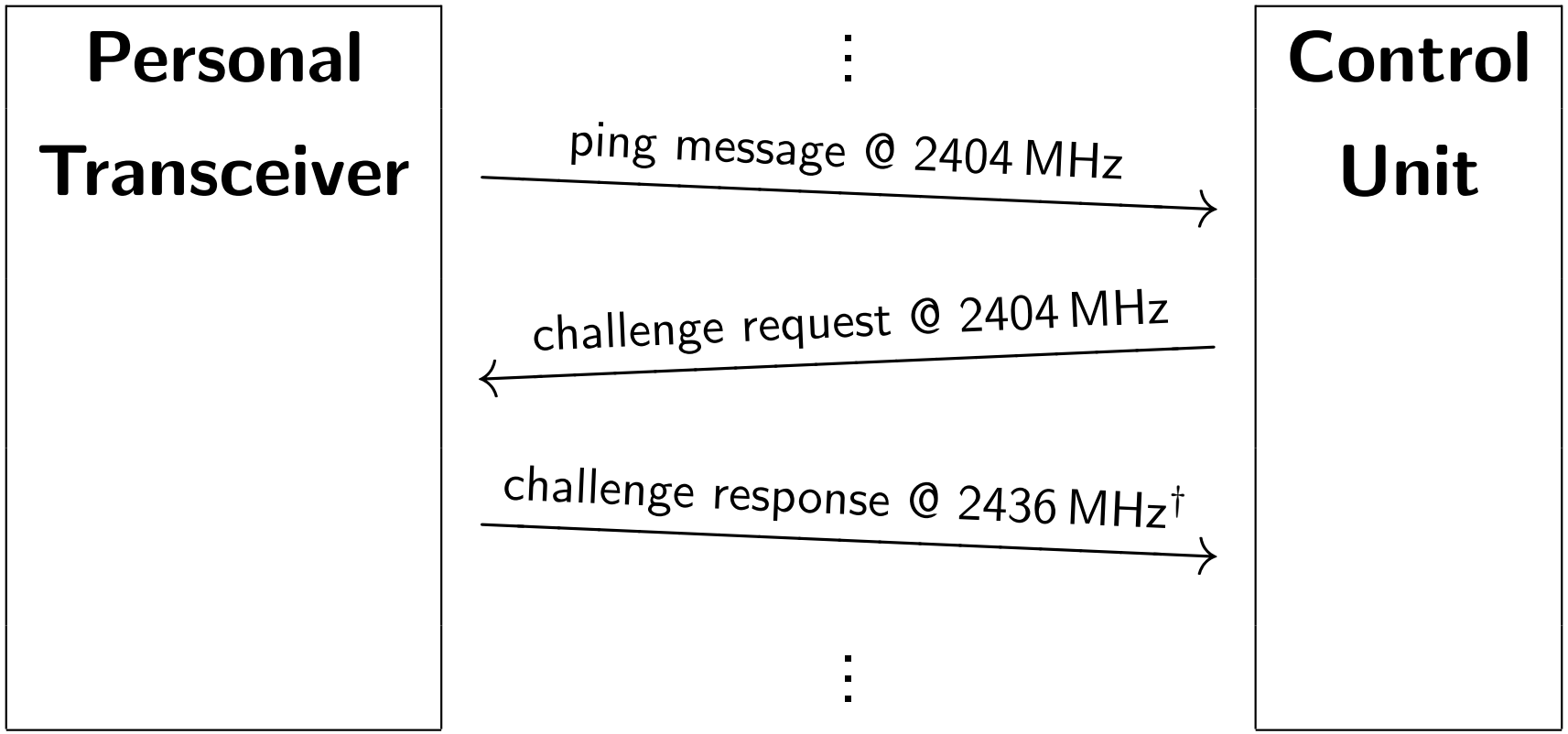
- 4 byte logical address, derived from unknown algorithm
- Always has a payload of 16 bytes



Ping Broadcast



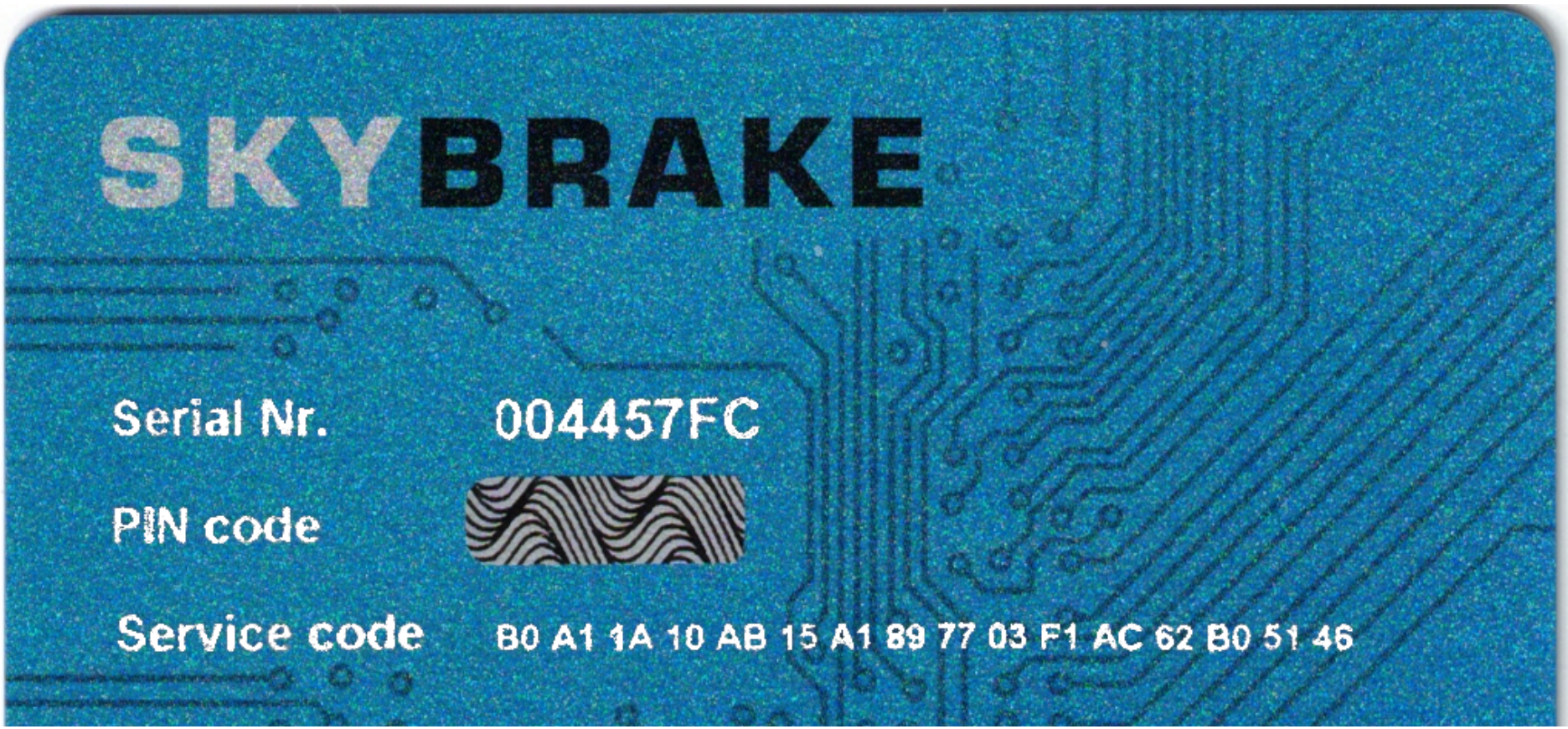
Authentication Flow



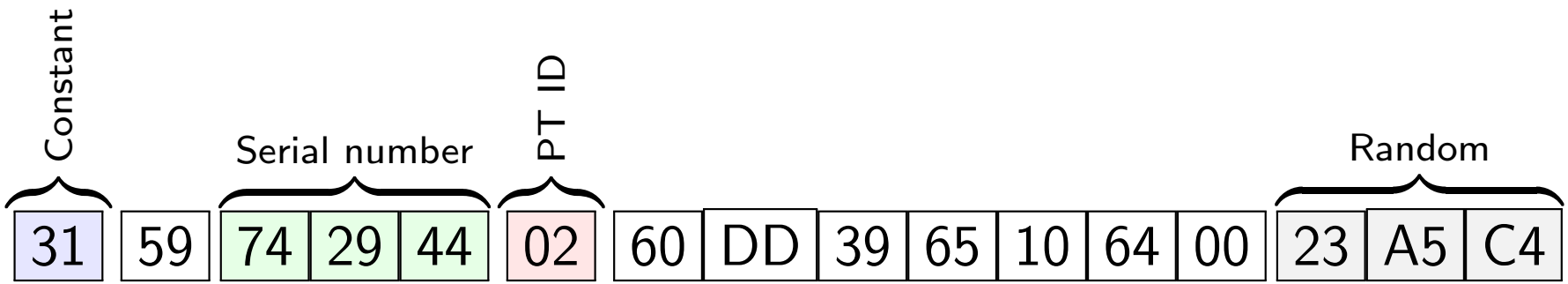
† Channels for challenge response seemingly random

Encryption

- Messages all have length of 16 bytes
- Messages are encrypted using AES-128
- Service code (from service card) used as AES-128 key

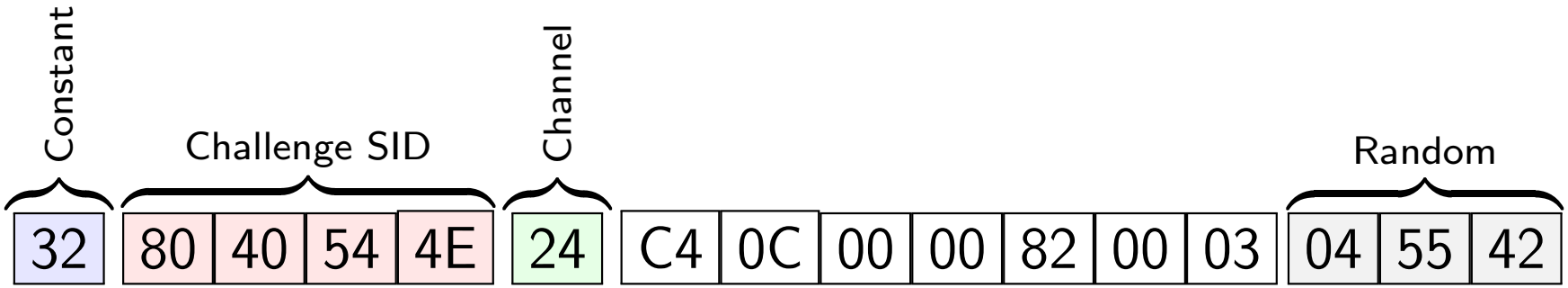


Ping message



Challenge Request

Challenge Request



Challenge Response

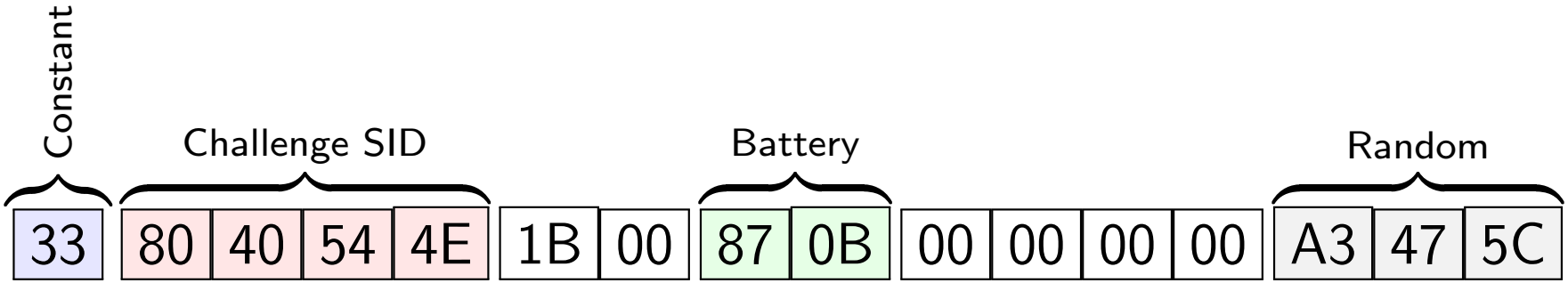


Table of Contents

1 Introduction

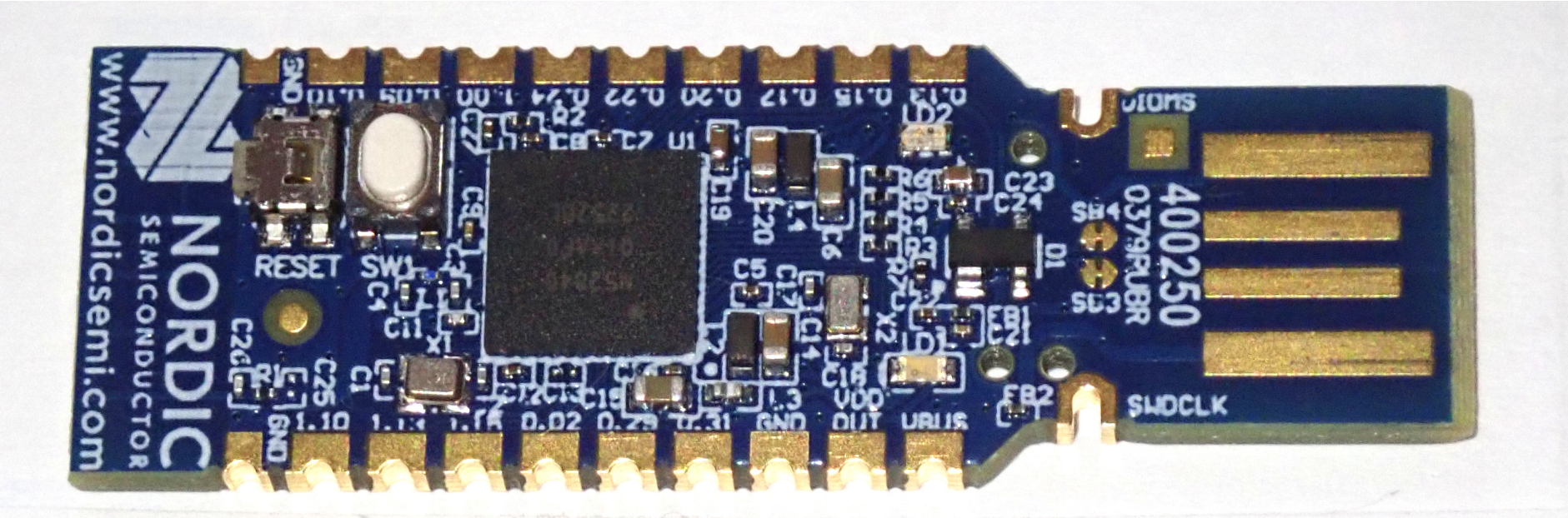
2 Black-box Analysis

3 Attack Vectors

4 Conclusion

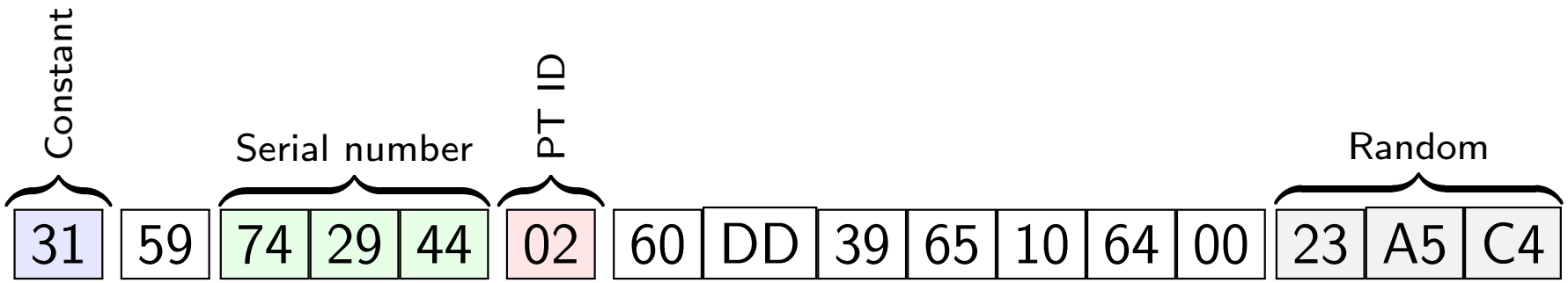
How to send messages?

Nordic Semiconductor nRF52840 USB Dongle



Replay attacks

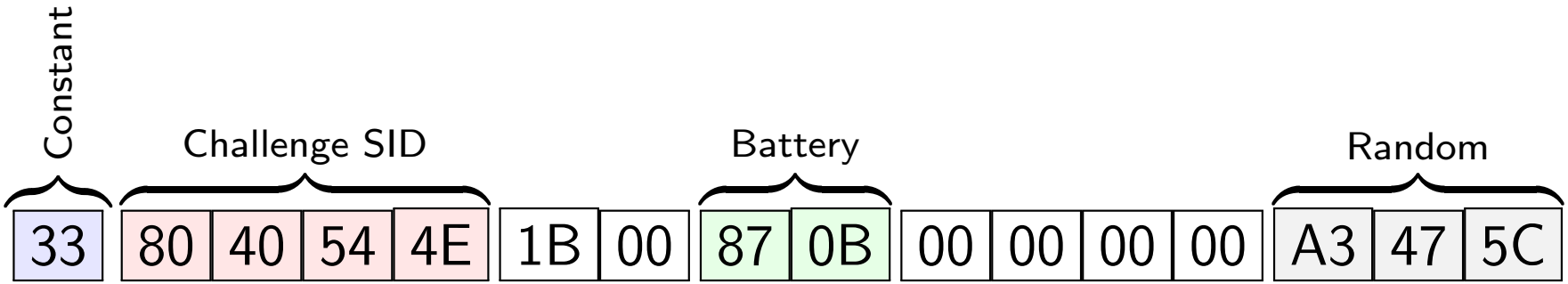
Ping message



- No checks for freshness, vulnerable to replay attacks
- Does not give any benefit for an attacker
  - Does not authenticate the attacker and disable the immobilization
  - Allows attacker to receive a challenge request message

Replay attacks

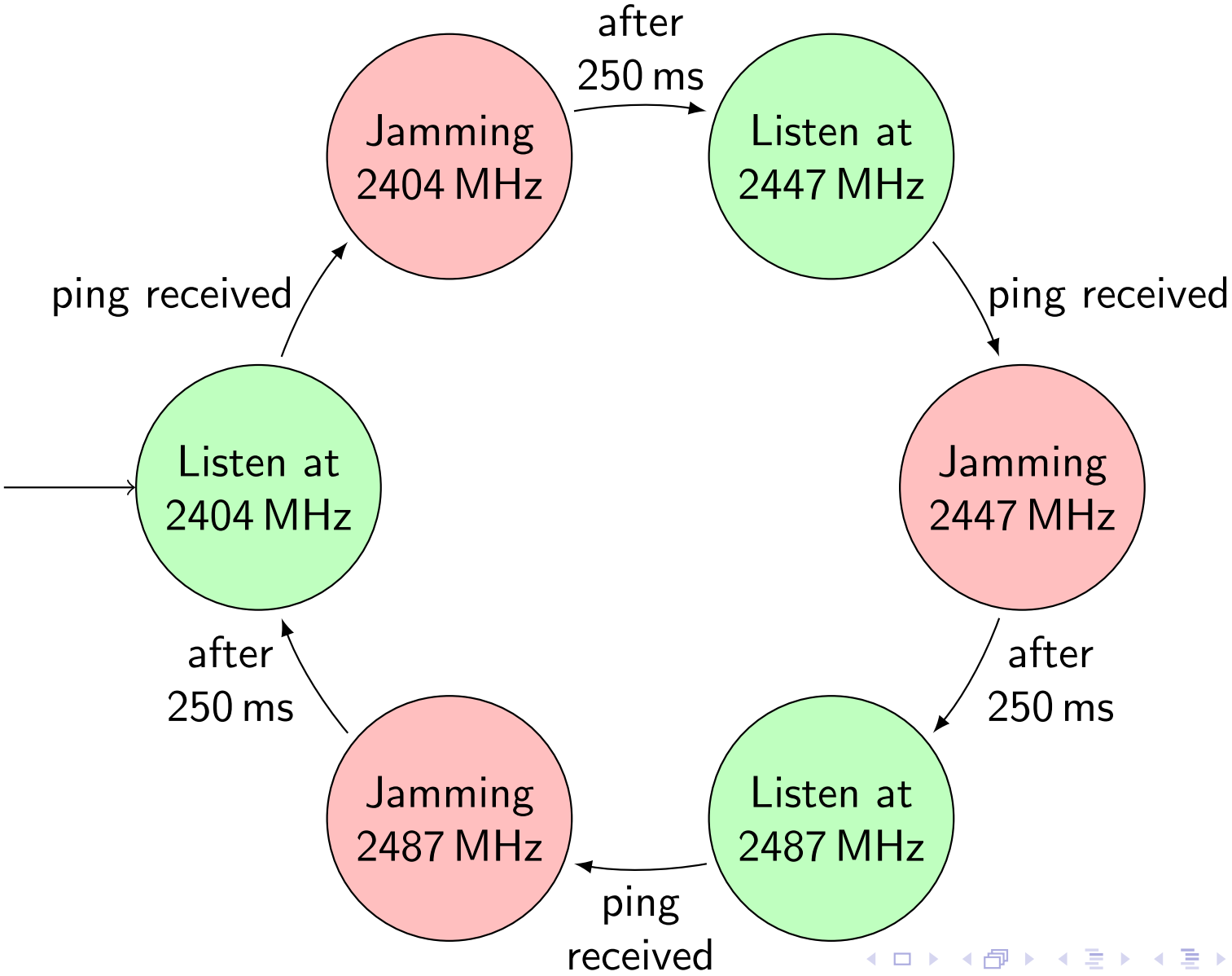
Challenge response



- Cannot be replayed by an adversary
  - Freshness is checked through Challenge SID
  - Adversary needs to determine correct radio channel[†]

[†] Adversary can just broadcast to all channels

Narrow-band Jamming



Emulating Personal Transceiver

Adversary can successful pass authentication knowing

- Service code from service card
- Logical address used by immobilizer†
- Serial number of immobilizer†

† Can be sniffed from target personal transceiver using SDR

Table of Contents

1 Introduction

2 Black-box Analysis

3 Attack Vectors

4 Conclusion

Conclusion

- General working principle of car immobilizer is known
- Secure against replaying attacks due to randomize challenge
- Security of car immobilizer depends on secrecy of the service code
  - Service code needs to be truly random
  - Service code needs to be secret
  - End user needs to keep the service code secret
- Vulnerable to narrow-band jamming attacks due to deterministic handshake channel selection algorithm

Future work

- Is it secure?
  - Maybe, performed black-box analysis is limited
- Full security analysis requires program code from microcontrollers to answer open questions
  - Additional commands/messages supported by the car immobilizer?
  - Algorithm used to derive the logical address?
  - Algorithm used to derive the radio channels for ping messages?
  - Source of randomness (PRNG) used by immobilizer?