



# Evaluating the Security Vulnerabilities of ZigBee Motion Detectors in Wireless Sensor Networks

A Study on Jamming, Interception, and Behavioral Manipulation

SNE/OS3.nl - Research Presentation

Diogo Marques

diogo.marque@os3.nl

University of Amsterdam

Henk Netten

henk.netten@os3.nl

University of Amsterdam

Muhammad Mansour

muhammad.mansour@os3.nl

University of Amsterdam

# Introduction



The rise of IoT devices, especially those using the ZigBee protocol, has brought about greater convenience in automation but also heightened security risks.

Many sellers have been advertising their human presence sensors as effective tools for intruder detection, often selling these devices in bundles with alarms and security hubs for global markets.



# Research Questions

How can ZigBee-based motion detectors be utilized safely in high-security applications, such as break-in detection?

What are the vulnerabilities in the ZigBee-based IoT network?

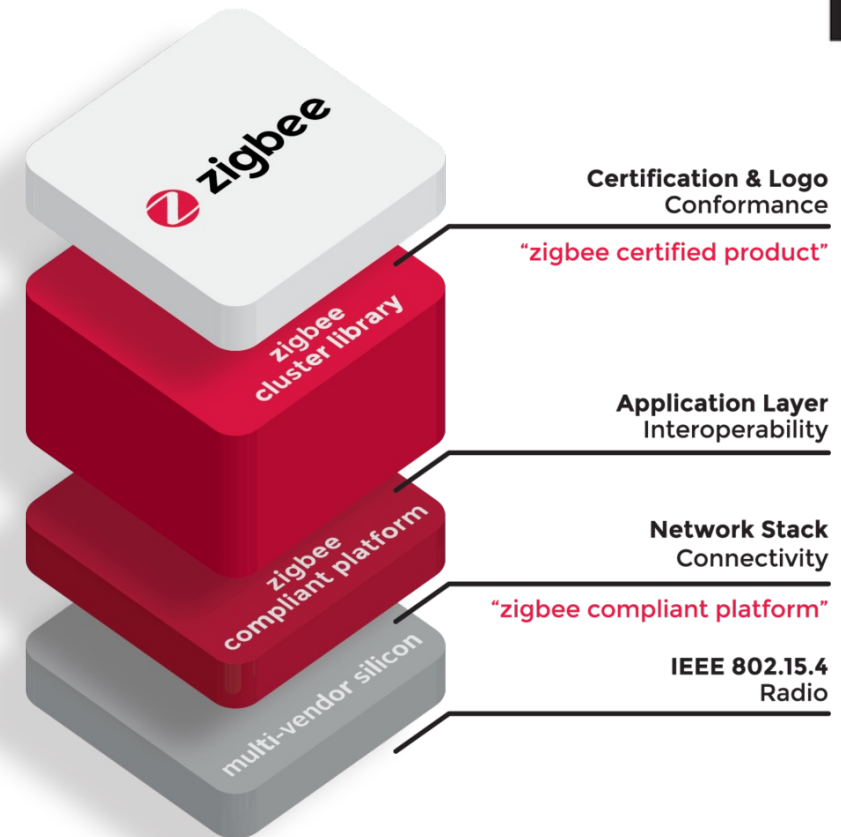
How can we defend against attacks that exploit these vulnerabilities?



# What is Zigbee?

A wireless communication protocol for low-power, low-data-rate applications.

Ideal for Internet of Things (IoT) devices, smart homes, and industrial automation.





# What are its features?

**Low Power Consumption:** Designed for long battery life in devices like sensors.

**Short Range:** Operates at distances of 10 to 100 meters.

**Low Data Rate:** Supports rates from 20 kbps to 250 kbps.

**Mesh Networking:** Enhances reliability and extends communication range.

**Robust Security:** Implements encryption and authentication for data protection.

**Encryption:** Uses AES-128 encryption to secure data transmission, preventing unauthorized access and ensuring data confidentiality.

**Authentication:** Employs mechanisms such as key establishment protocols to authenticate devices before joining the network, protecting against unauthorized device access.

**Integrity Checks:** Includes message integrity checks to ensure data has not been tampered with during transmission.

**Interoperability:** Based on IEEE 802.15.4 standard for compatibility with various devices.

# Environment - Hardware

Wireless router

Silvercrest Controller

Sonoff Zigbee Human Presence Sensor

Sonoff Zigbee Wireless Switch

HackRF One

Smartphone

Linux laptop





# GnuRadio Companion

# Wireshark

# JamRF

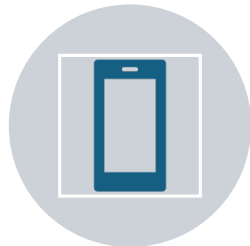
10,12	All
-------	-----



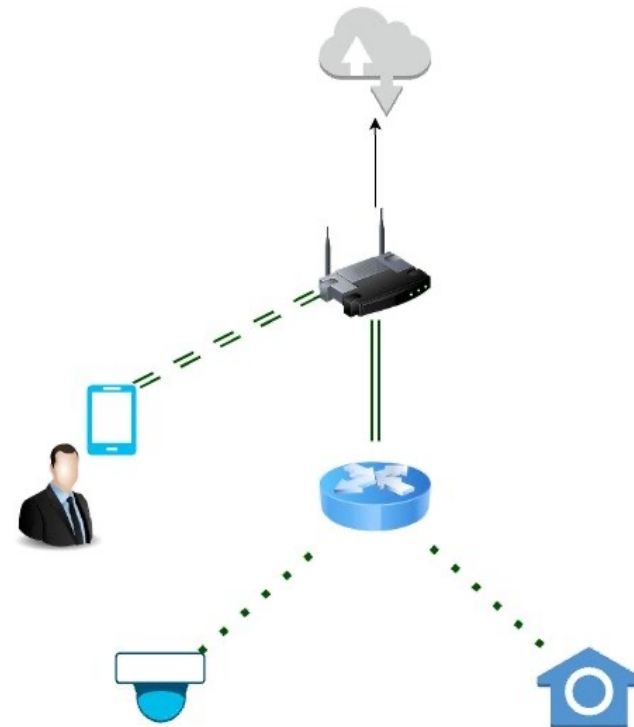
## Environment - Zigbee



We connected the zigbee controller to the internet router.



Using the smartphone application Tuya we paired the zigbee controller and both sensors.



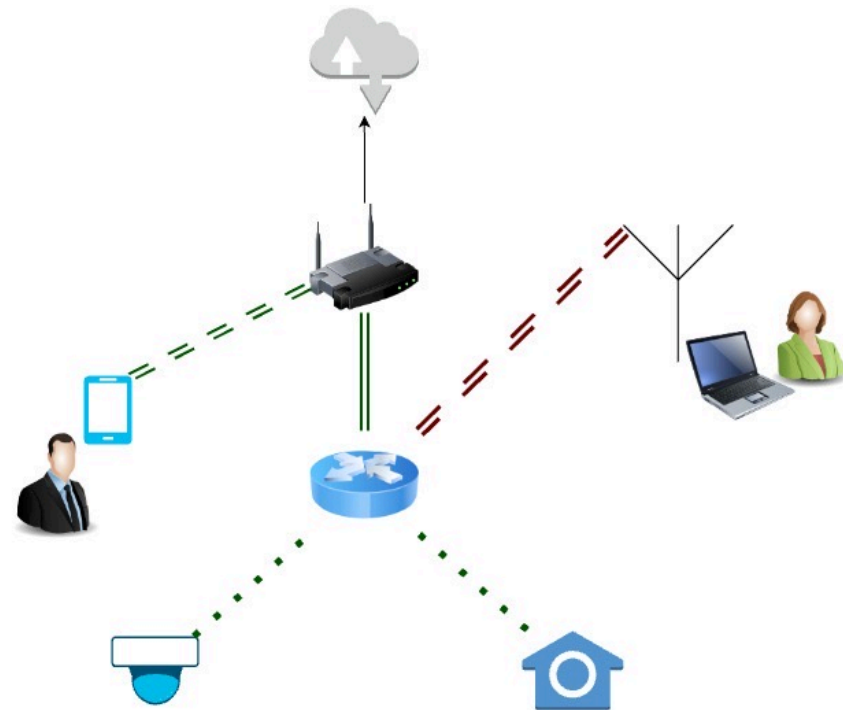




# Intruder

Scans the 2.4GHz network to retrieve information using HackRF and Gnuradio (RFTap).

Wireshark can the decrypt the packets with the Global Key but gives us limited information.







# Wireshark

Required to read the HackRF output.

Using the Zigbee Global Key is possible to decrypt some of the messages.

A second key is required to have the full information.

## Relevant Zigbee Packages

- Transport Key
- Association Request
- Association Response
- Device Announcement
- Status Zone Change

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

zbee\_aps.cmd.id == 0x05

No.	Time	Source	Destination	Protocol	Length	Info
354	192.388338	0x0000	0xa52a	ZigBee	102	Transport Key
356	192.381856	0x0000	0xa52a	ZigBee	102	Transport Key
360	192.576386	0xa52a	0xd884	ZigBee	73	Transport Key
369	192.608501	0xa52a	0xd884	ZigBee	73	Transport Key
370	192.611971	0xa52a	0xd884	ZigBee	73	Transport Key
371	192.613781	0xa52a	0xd884	ZigBee	73	Transport Key
373	192.621464	0xa52a	0xd884	ZigBee	73	Transport Key
384	192.683471	0xa52a	0xd884	ZigBee	73	Transport Key
775	195.889758	0x0000	0xd884	ZigBee	94	Transport Key
1066	264.926440	0x0000	0xa52a	ZigBee	102	Transport Key
1068	264.929884	0x0000	0xa52a	ZigBee	102	Transport Key
1072	265.100359	0xa52a	0xa033	ZigBee	73	Transport Key
1097	265.254837	0xa52a	0xa033	ZigBee	73	Transport Key
1486	267.941696	0x0000	0xa033	ZigBee	94	Transport Key
1491	267.943586	0x0000	0xa033	ZigBee	94	Transport Key
1501	268.110437	0x0000	0xa033	ZigBee	90	Transport Key

▶ Frame 1066: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0

▶ IEEE 802.15.4 Data, Src: 0x0000, Dst: 0xa52a

▶ ZigBee Network Layer Data, Dst: 0xa52a, Src: 0x0000

▶ ZigBee Application Support Layer Command

▶ ZigBee Application Support Layer Command

▶ Frame Control Field: Command (0x21)

Counter: 209

▶ ZigBee Security Header

▶ Security Control Field: 0x30, Key Id: Key-Transport Key, Extended Nonce

Frame Counter: 57350

Extended Source: SiliconLabor\_ff:fe:a6:33:87 (84:71:27:ff:fe:a6:33:87)

Message Integrity Code: 1d9c02cd

[Key: 5a6967426565416c6c69616e63653039]

[Key Label: ]

▶ Command Frame: Transport Key

Command Identifier: Transport Key (0x05)

Key Type: Standard Network Key (0x01)

Key: 3f5f40d8b1fb7cbddda29980df714b

Sequence Number: 0

Extended Destination: SiliconLabor\_ff:fe:2b:45:09 (94:de:b8:ff:fe:2b:45:09)

Extended Source: SiliconLabor\_ff:fe:a6:33:87 (84:71:27:ff:fe:a6:33:87)

0000 01 05 0e 09 45 2b fe ff b8 de 94 21 d1 30 06 e0 ..E+... ..

0010 00 00 87 33 a6 fe ff 27 71 84 ae 3e f8 6f b7 54 ...3... q...

0020 65 d6 ab 40 10 f3 6d df d8 fb f9 82 9a 95 78 db e...@...m... ..

0030 27 8d 2d e3 46 7b 51 b2 95 70 fa 63 8a 1d 0c 02 '...F(Q...p...

0040 cd

es)Decrypted ZigBee Payload (65 bytes)Decrypted ZigBee Payload (35 bytes)

Counter (zbee\_aps.counter), 1 bytePackets: 10332 - Displayed: 16 (0.2%)Profile: Default

# Wireshark – Transport Key

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
255	462.070276	0x0000		ZigBee HA	50	ZCL: Default Response, Seq: 23
256	462.070293			IEEE 802.15.4	5	Ack
257	462.092323	0xa52a	0x0000	ZigBee HA	51	ZCL: Write Attributes Response, Seq: 24
258	462.092333			IEEE 802.15.4	5	Ack
259	462.135069	0x0000	0xa52a	ZigBee HA	50	ZCL: Default Response, Seq: 24
260	462.135103			IEEE 802.15.4	5	Ack
261	464.520282	0xa52a	Broadcast	ZigBee	50	Link Status
262	473.667346	0x0000	Broadcast	ZigBee	50	Link Status
263	474.969214	0xa52a	Broadcast	ZigBee	47	Leave
264	475.460046	0xa52a	Broadcast	ZigBee	47	Leave
265	475.920003	0xa52a	Broadcast	ZigBee	47	Leave
266	479.431116	0x0000	Broadcast	ZigBee	51	Many-to-One Route Request, Dst: 0xffff, Src: 0x0000
267	479.816600	0x0000	Broadcast	ZigBee	51	Many-to-One Route Request, Dst: 0xffff, Src: 0x0000
268	480.118006	0x0000	Broadcast	ZigBee	51	Many-to-One Route Request, Dst: 0xffff, Src: 0x0000
269	480.508085	0x0000	Broadcast	ZigBee	51	Many-to-One Route Request, Dst: 0xffff, Src: 0x0000
270	482.079190		Broadcast	IEEE 802.15.4	10	Beacon Request
271	482.149772	0x0000		ZigBee	28	Beacon, Src: 0x0000, EPID: 15:be:df:5b:19:89:c1:d4
272	482.352385	0c:ef:f6:ff:fe:5c:4...	0x0000	IEEE 802.15.4	21	Association Request, FFD
273	482.352715			IEEE 802.15.4	5	Ack
274	482.547623	0c:ef:f6:ff:fe:5c:4...	0x0000	IEEE 802.15.4	18	Data Request
275	482.547651			IEEE 802.15.4	5	Ack
276	482.549035	84:71:27:ff:fe:a6:3...	0c:ef:f6:ff:fe:5c:4...	IEEE 802.15.4	27	Association Response, PAN: 0x1f0d Addr: 0xa52a
277	482.549083			IEEE 802.15.4	5	Ack
278	482.571371	0x0000	0xa52a	ZigBee	73	Transport Key
279	482.571391			IEEE 802.15.4	5	Ack
280	482.576340	0xa52a	Broadcast	ZigBee ZDP	65	Device Announcement, Nwk Addr: 0xa52a, Ext Addr: SiliconLabor_ff:fe:5c:44:01
281	482.577648	0xa52a	Broadcast	ZigBee	50	Link Status
282	482.639307	0xa52a	Broadcast	ZigBee ZDP	65	Device Announcement, Nwk Addr: 0xa52a, Ext Addr: SiliconLabor_ff:fe:5c:44:01
283	482.642625	0x0000	0xa52a	ZigBee HA	60	ZCL: Read Attributes, Seq: 25
284	482.642769			IEEE 802.15.4	5	Ack
285	482.646514			IEEE 802.15.4	5	Ack
286	482.648384			IEEE 802.15.4	5	Ack

Frame 272: 21 bytes on wire (168 bits), 21 bytes captured (168 bits) on interface 0

IEEE 802.15.4 Command, Src: SiliconLabor\_ff:fe:5c:44:01, Dst: 0x0000

Frame Control Field: 0xc823, Frame Type: Command, Acknowledge Request, Destination Addressing Mode: Short/16-bit, Frame Version: IEEE Std 802.15.4-2003, Source Addressing Mode: Long/64-bit

Sequence Number: 86

Destination PAN: 0x1f0d

Destination: 0x0000

Source PAN: 0xffff

Extended Source: SiliconLabor\_ff:fe:5c:44:01 (0c:ef:f6:ff:fe:5c:44:01)

Command Identifier: Association Request (0x01)

Association Request

- ...0 = Alternate PAN Coordinator: False
- ...1 = Device Type: FFD
- ...1 = Power Source: AC/Mains Power
- ...1 = Receive On When Idle: True
- ...0 = Security Capability: False
- ...1 = Allocate Address: True

FCS: 0xba46 (Correct)

23 c8 56 0d 1f 00 00 ff ff 01 44 5c fe ff f6 ef # V ..... D  
0c 01 8e 46 ba ... F

after\_detecting\_multiple\_times.pcap Packets: 3180 Profile: Default

# Wireshark – Association Request

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
255	462.070276	0x0000		ZigBee HA	50	ZCL: Default Response, Seq: 23
256	462.070293			IEEE 802.15.4	5	Ack
257	462.092323	0xa52a	0x0000	ZigBee HA	51	ZCL: Write Attributes Response, Seq: 24
258	462.092333			IEEE 802.15.4	5	Ack
259	462.135069	0x0000	0xa52a	ZigBee HA	50	ZCL: Default Response, Seq: 24
260	462.135103			IEEE 802.15.4	5	Ack
261	464.520282	0xa52a	Broadcast	ZigBee	50	Link Status
262	473.667346	0x0000	Broadcast	ZigBee	50	Link Status
263	474.969214	0xa52a	Broadcast	ZigBee	47	Leave
264	475.460046	0xa52a	Broadcast	ZigBee	47	Leave
265	475.920003	0xa52a	Broadcast	ZigBee	47	Leave
266	479.431116	0x0000	Broadcast	ZigBee	51	Many-to-One Route Request, Dst: 0xffff, Src: 0x0000
267	479.816600	0x0000	Broadcast	ZigBee	51	Many-to-One Route Request, Dst: 0xffff, Src: 0x0000
268	480.118006	0x0000	Broadcast	ZigBee	51	Many-to-One Route Request, Dst: 0xffff, Src: 0x0000
269	480.508085	0x0000	Broadcast	ZigBee	51	Many-to-One Route Request, Dst: 0xffff, Src: 0x0000
270	482.079190		Broadcast	IEEE 802.15.4	10	Beacon Request
271	482.149772	0x0000		ZigBee	28	Beacon, Src: 0x0000, EPID: 15:be:df:5b:19:89:c1:d4
272	482.352385	0c:ef:f6:ff:fe:5c:4...	0x0000	IEEE 802.15.4	21	Association Request, FFD
273	482.352715			IEEE 802.15.4	5	Ack
274	482.547623	0c:ef:f6:ff:fe:5c:4...	0x0000	IEEE 802.15.4	18	Data Request
275	482.547651			IEEE 802.15.4	5	Ack
276	482.549035	84:71:27:ff:fe:a6:3...	0c:ef:f6:ff:fe:5c:4...	IEEE 802.15.4	27	Association Response, PAN: 0x1f0d Addr: 0xa52a
277	482.549083			IEEE 802.15.4	5	Ack
278	482.571371	0x0000	0xa52a	ZigBee	73	Transport Key
279	482.571391			IEEE 802.15.4	5	Ack
280	482.576340	0xa52a	Broadcast	ZigBee ZDP	65	Device Announcement, Nwk Addr: 0xa52a, Ext Addr: SiliconLabor_ff:fe:5c:44:01
281	482.577648	0xa52a	Broadcast	ZigBee	50	Link Status
282	482.639307	0xa52a	Broadcast	ZigBee ZDP	65	Device Announcement, Nwk Addr: 0xa52a, Ext Addr: SiliconLabor_ff:fe:5c:44:01
283	482.642625	0x0000	0xa52a	ZigBee HA	60	ZCL: Read Attributes, Seq: 25
284	482.642769			IEEE 802.15.4	5	Ack
285	482.646514			IEEE 802.15.4	5	Ack
286	482.648384			IEEE 802.15.4	5	Ack

Frame 276: 27 bytes on wire (216 bits), 27 bytes captured (216 bits)

- IEEE 802.15.4 Command, Src: SiliconLabor\_ff:fe:a6:33:87, Dst: SiliconLabor\_ff:fe:5c:44:01
  - Frame Control Field: 0xcc63, Frame Type: Command, Acknowledge Request, PAN ID Compression, Destination Addressing Mode: Long/64-bit, Frame Version: IEEE Std 802.15.4-2003, Source Addressing Sequence Number: 102
    - Destination PAN: 0x1f0d
    - Destination: SiliconLabor\_ff:fe:5c:44:01 (0c:ef:f6:ff:fe:5c:44:01)
    - Extended Source: SiliconLabor\_ff:fe:a6:33:87 (84:71:27:ff:fe:a6:33:87)
    - Command Identifier: Association Response (0x02)
  - Association Response
    - Short Address: 0xa52a
    - Association Status: 0x00 (Association Successful)
    - FCS: 0xed7e (Correct)

0000 63 cc 66 0d 1f 01 44 5c fe ff f6 ef 0c 87 33 a6 c f ... D ...  
0010 fe ff 27 71 84 02 2a a5 00 7e ed ... t q ...

after\_detecting\_multiple\_times.pcap Packets: 3180 Profile: Default

# Wireshark – Association Response

Wireshark interface showing a packet capture of a ZigBee cluster library frame. The packet list shows a sequence of frames, with the selected frame (No. 527) being a ZigBee Cluster Library Frame (Type: Zone Status Change Notification, Seq: 2).

The packet details pane shows the following structure:

- Frame 527: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
- IEEE 802.15.4 Data, Src: 0xa52a, Dst: 0x0000
- ZigBee Network Layer Data, Dst: 0x0000, Src: 0xa52a
- ZigBee Application Support Layer Data, Dst Endpt: 1, Src Endpt: 1
  - Frame Control Field: Data (0x00)
    - Destination Endpoint: 1
    - Cluster: Intruder Alarm System Zone (0x0500)
    - Profile: Home Automation (0x0104)
    - Source Endpoint: 1
    - Counter: 135
  - ZigBee Cluster Library Frame
    - Frame Control Field: Cluster-specific (0x09)
      - Sequence Number: 2
      - Command: Zone Status Change Notification (0x00)
    - ZoneStatus: 0x0001, Alarm 1
      - ...1 = Alarm 1: Opened or alarmed
      - ...0 = Alarm 2: Closed or not alarmed
      - ...0 = Tamper: Not tampered
      - ...0 = Battery: Battery OK
      - ...0 = Supervision Reports: Does not report
      - ...0 = Restore Reports: Does not report restore
      - ...0 = Trouble: OK
      - ...0 = AC (mains): AC/Mains OK
    - Extended Status: 0x00
    - Zone ID: 0xff
    - Delay (in quarterseconds): 0

The packet bytes pane shows the raw data (hex and ASCII) for the selected frame.

Cluster (zbee\_aps.cluster), 2 bytes

Packets: 3180 · Displayed: 41 (1.3%)

Profile: Default

# Wireshark – Status Zone Change



# Experiments - Overview

Intercepting communications between the controller and the sensor.

Introduce a new/intruder device on the network.

Jamming the human presence sensor.

Jamming the communications between the sensor and the hub.





# Results - Overview

We verified during the experiments the human presence detection capabilities were not affected with HackRF when jamming signal.

- Aluminum foil covering its surface did the job.

Disable the Zigbee network communications.

- The app shown no notifications when the sensor has detected an intruder.
- After the intruder left the area and the service was back online no incidents were reported.



# Results - Intercepting

We got the key by listening in on the handshake.

Triggering the handshake is difficult. We tried to pair another device with the coordinator to force it to make a new handshake. This required access to the mobile phone app.

Furthermore, registering a new mobile phone app required pressing a button on the coordinator.



# Results - Jamming

Communication - With jamRF and RFJamming-FMRadio-SDR works 2.4GHz band (between coordinator and zigbee device)

The switch and human presence sensor both stopped communicating with the hub.

Jamming 5.8GHz to interfere with the sensor's detection was not successful.

Detection - We used gaussian noise and impulse noise in gnuradio.

The sensor still detected human presence, and the status changed on the app.

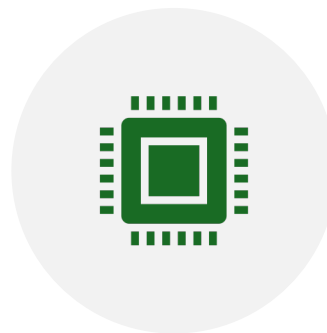
We tried to see if only the first detection would work but sadly future detections also worked. (The continuous noise wave doesn't make a status for the sensor.)

If this did work, an attacker could place a jamming device and come back later to do crimes.

# Conclusions



THE SENSOR IS PROVEN EFFICIENT WHEN  
DETECTING INTRUDERS.



WE COULDN'T TEST HIS COMMUNICATIONS  
DURING THE JAMMING BECAUSE WE HAD  
HARDWARE LIMITATIONS SO WE CAN'T CONFIRM  
THE SENSOR SENT THE CHANGE STATUS PACKAGE  
TO THE CONTROLLER.



WHEN JAMMING THE 2.4GHZ COMMUNICATION  
HUB IT WAS POSSIBLE TO NOT NOTIFY THE OWNER  
THAT AN INTRUDER WAS IN THEIR PROPERTY AND  
BECAUSE THERE IS NO INTERNAL MEMORY NO  
NOTIFICATION WAS SAVED IN HISTORY ON THE APP.



# Thank you!

## Questions?

Diogo Marques

[diogo.marque@os3.nl](mailto:diogo.marque@os3.nl)

University of Amsterdam

Henk Netten

[henk.netten@os3.nl](mailto:henk.netten@os3.nl)

University of Amsterdam

Muhammad Mansour

[muhammad.mansour@os3.nl](mailto:muhammad.mansour@os3.nl)

University of Amsterdam