# HiveGuard: A Network Security Monitoring Architecture for Zigbee Networks

**Dimitrios-Georgios Akestoridis and Patrick Tague**

*Carnegie Mellon University*

IEEE CNS 2021

# Introduction (pt. 1)

- Zigbee networks can be found in a wide range of smart environments with low-power IoT devices, but they remain **largely unmonitored**
- There are no robust open-source software tools to **continuously monitor** Zigbee traffic for potential security issues

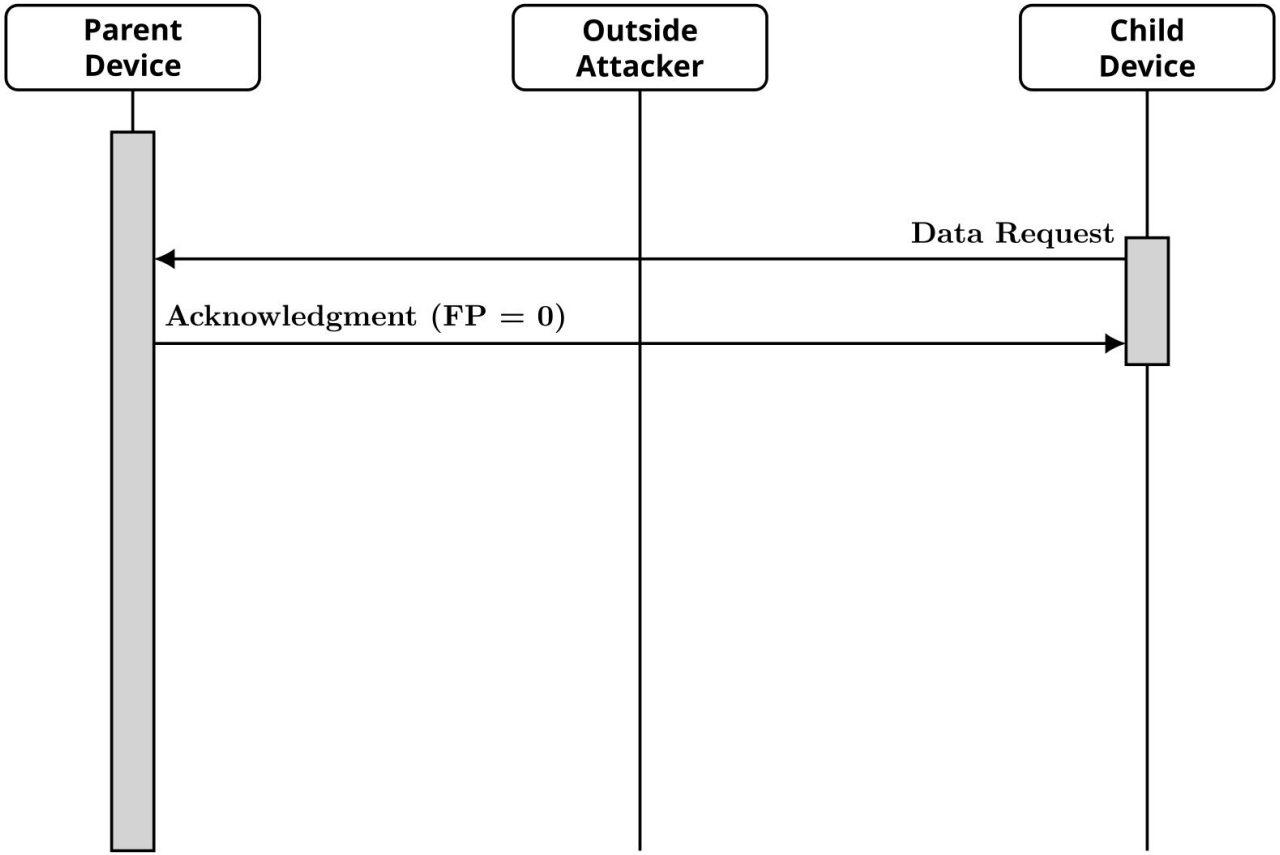
# Introduction (pt. 2)

- Without an appropriate network security monitoring system, several types of attacks against Zigbee networks can **go undetected**
- We designed **HiveGuard** to provide archiving, aggregation, inspection, visualization, and alert services for Zigbee traffic

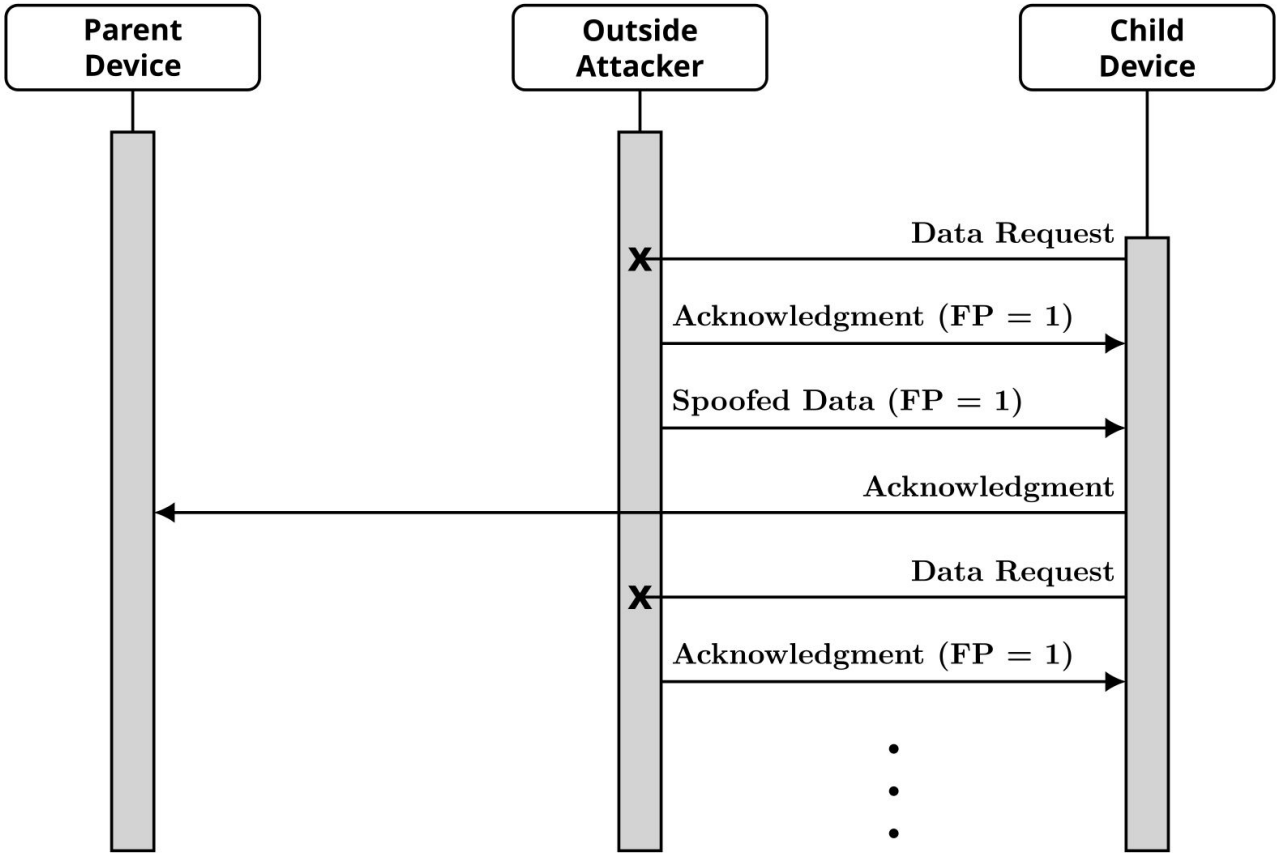
# Introduction (pt. 3)

- We developed detection rules for attacks against centralized Zigbee networks that can be launched by an **outside attacker**
- We developed an **energy depletion attack** against battery-powered Zigbee devices that improves upon the attack that Cao et al. presented (DOI: 10.1109/JIOT.2016.2516102)

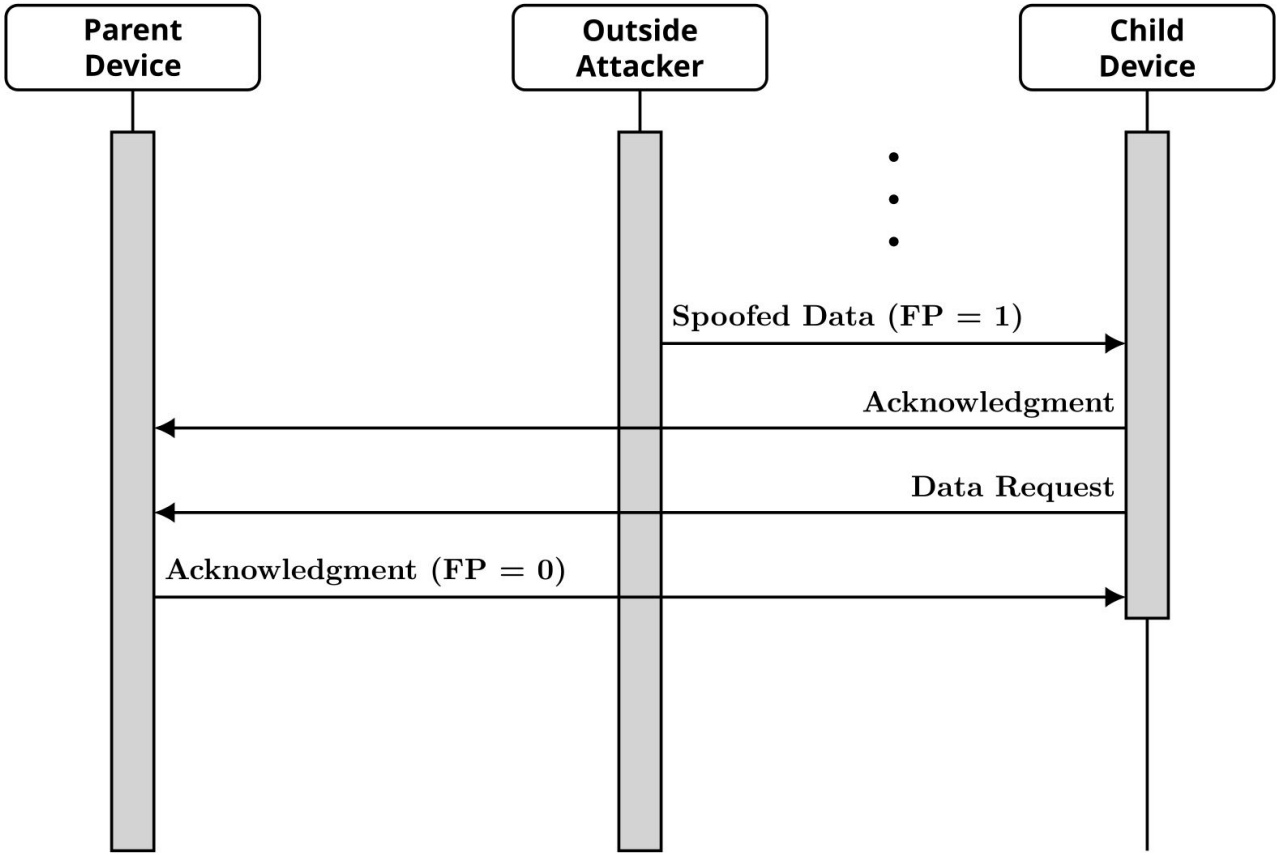
# Overview of Our Attack (pt. 1)



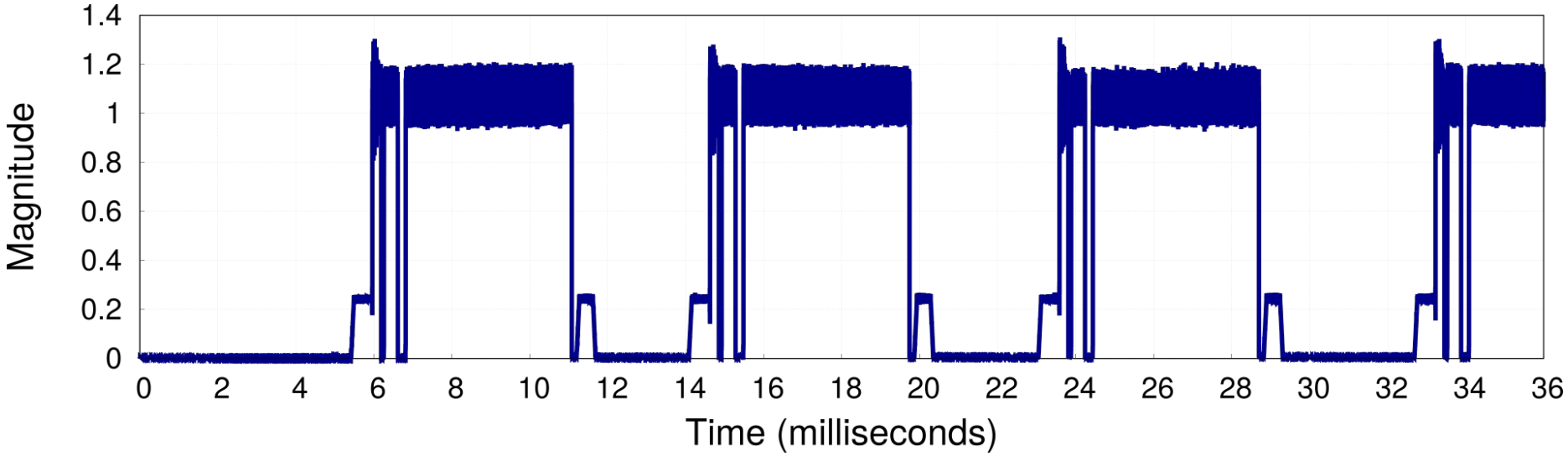
# Overview of Our Attack (pt. 2)



# Overview of Our Attack (pt. 3)

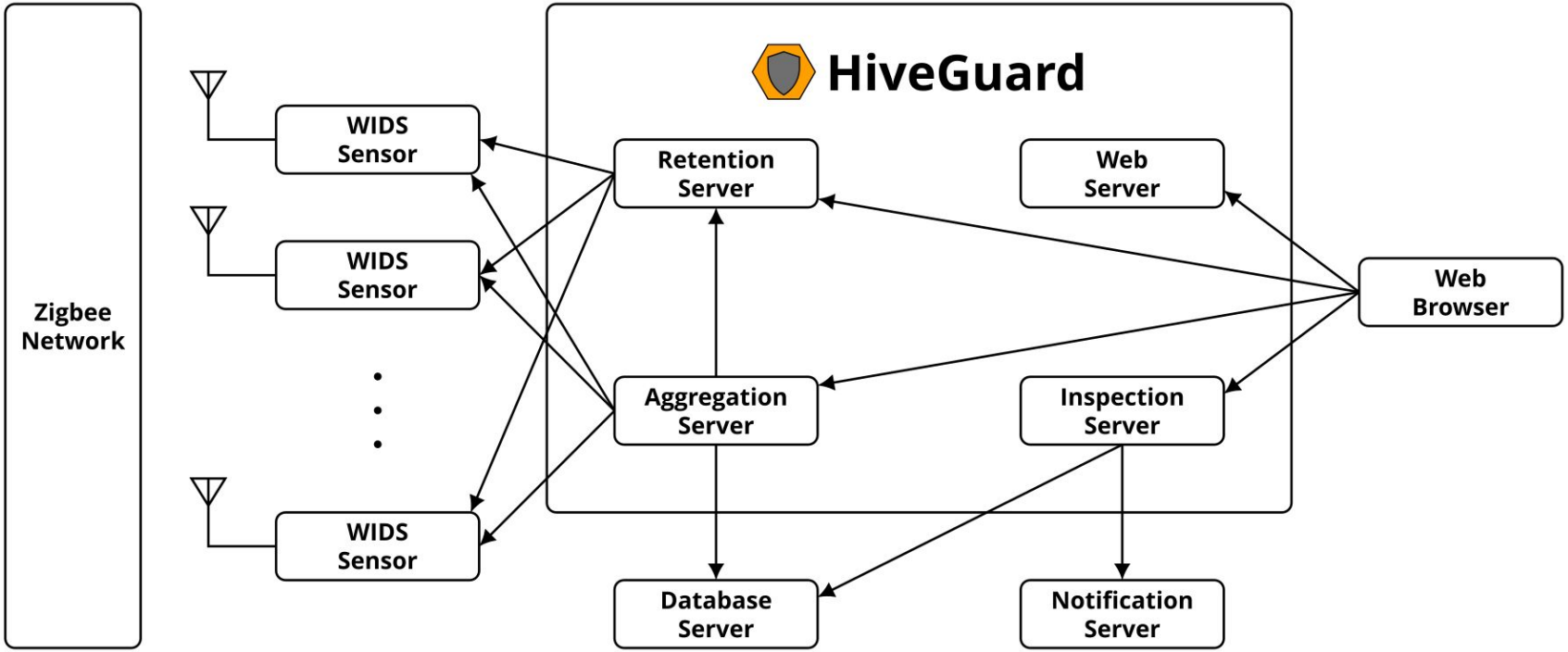


# Proof-of-Concept Implementation




- It will be available as the **attack with ID 13**
- https://github.com/akestoridis/atusb-attacks

# Overview of HiveGuard



# Prototype Implementation (pt. 1)

- Our HiveGuard prototype implementation has been organized into **three repositories**
- https://github.com/akestoridis/hiveguard
- https://github.com/akestoridis/hiveguard-backend
- https://github.com/akestoridis/hiveguard-frontend

# Prototype Implementation (pt. 2)

- We wrote our WIDS sensor software on top of **Zigator** and we extended **Scapy** to dissect certain Zigbee packets
- https://github.com/akestoridis/zigator/commit/8565e6fd26cc3c2ac457c4a467c184297eb51e94
- https://github.com/secdev/scapy/commit/6ad83c513648fc1b4199a4b2d7b74b8a8c2ae0ce

# Experimental Results (pt. 1)

- We conducted **four experiments** in order to test HiveGuard against our energy depletion attack
- We used two Raspberry Pis, each of which was equipped with an ATUSB, as our **WIDS sensors**
- Our **dataset** of captured Zigbee packets will be available at https://crawdad.org/

# Experimental Results (pt. 2)

HiveGuard Inspection Archive About

## Header Fields Page

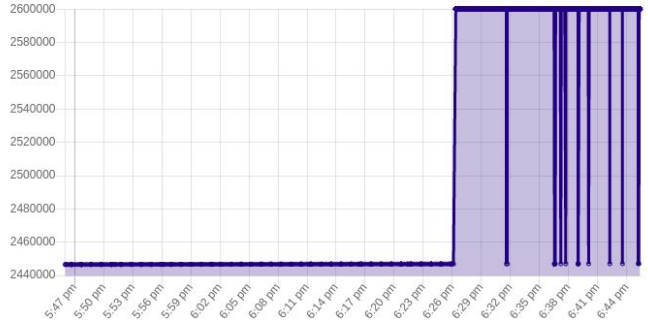
WIDS Sensor ID: rpi02 Time Interval: 1 hour

Source PAN ID: 0x2482 Source Address: 0x0000

Header Field Name: NWK Auxiliary Frame Counter

Header Field Value over Time

Last Updated: 6:45:48 PM




HiveGuard Inspection Archive About

## Header Fields Page

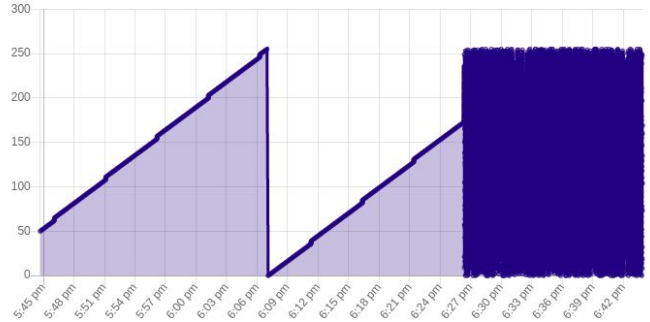
WIDS Sensor ID: rpi02 Time Interval: 1 hour

Source PAN ID: 0x2482 Source Address: 0xe0b3

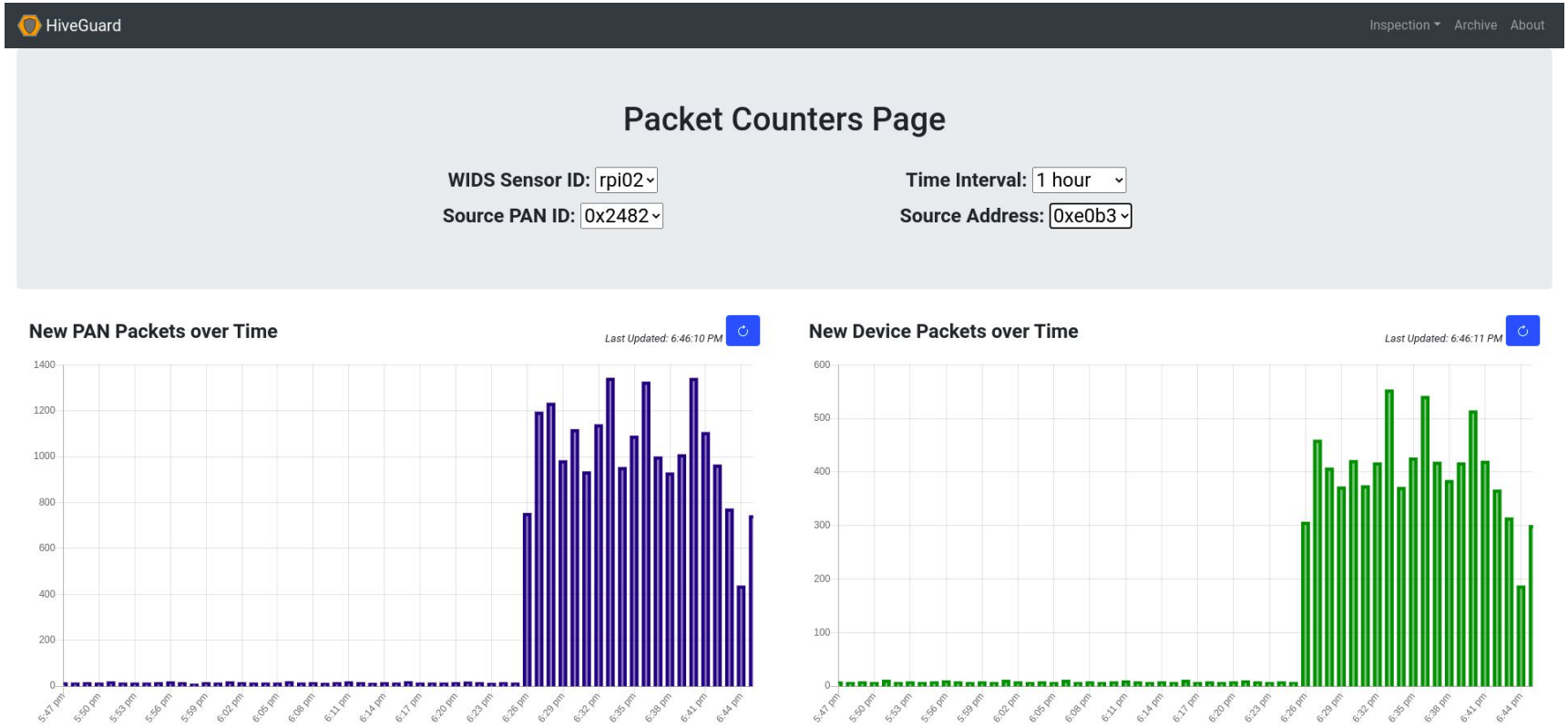
Header Field Name: MAC Sequence Number

Header Field Value over Time

Last Updated: 6:44:35 PM



# Experimental Results (pt. 3)



# Experimental Results (pt. 4)

| No. | Time | Delta time | MAC Src | MAC Dst | MAC SN | Length | Info |
|---|---|---|---|---|---|---|---|
| 136 | 308.369641 | 6.733838 | 0x0000 | 0xffff | 10 | 47 | Link Status |
| 137 | 308.699795 | 0.330154 | 0xe0b3 | 0x0000 | 171 | 12 | Data Request |
| 138 | 308.701158 | 0.001363 | | | 171 | 5 | Ack |
| 139 | 315.764929 | 7.063771 | 0xe0b3 | 0x0000 | 172 | 12 | Data Request |
| 140 | 315.765009 | 0.000080 | | | 172 | 5 | Ack |
| 141 | 322.832626 | 7.067617 | 0xe0b3 | 0x0000 | 173 | 12 | Unknown Command, Bad FCS |
| 142 | 322.840584 | 0.007958 | 0x0000 | 0xe0b3 | 255 | 127 | Data, Dst: 0xe0b3, Src: 0x0000 |
| 143 | 322.840606 | 0.000022 | | | 255 | 5 | Ack |
| 144 | 322.842006 | 0.001400 | 0xe0b3 | 0x0000 | 174 | 12 | Unknown Command, Bad FCS |
| 145 | 322.847454 | 0.005448 | 0x0000 | 0xe0b3 | 255 | 127 | Data, Dst: 0xe0b3, Src: 0x0000 |
| 146 | 322.847471 | 0.000017 | | | 255 | 5 | Ack |
| 147 | 322.852682 | 0.005211 | 0xe0b3 | 0x0000 | 175 | 12 | Unknown Command, Bad FCS |
| 148 | 322.859255 | 0.006573 | 0x0000 | 0xe0b3 | 255 | 127 | Data, Dst: 0xe0b3, Src: 0x0000 |
| 149 | 322.859341 | 0.000086 | | | 255 | 5 | Ack |
| 150 | 322.863217 | 0.003876 | 0xe0b3 | 0x0000 | 176 | 12 | Unknown Command, Bad FCS |
| 151 | 322.871094 | 0.007877 | 0x0000 | 0xe0b3 | 255 | 127 | Data, Dst: 0xe0b3, Src: 0x0000 |
| 152 | 322.871218 | 0.000124 | | | 255 | 5 | Ack |
| 153 | 322.876364 | 0.005146 | 0xe0b3 | 0x0000 | 177 | 12 | Unknown Command, Bad FCS |
| 154 | 322.876467 | 0.000103 | | | 177 | 5 | Ack |
| 155 | 322.883090 | 0.006623 | 0x0000 | 0xe0b3 | 255 | 127 | Data, Dst: 0xe0b3, Src: 0x0000 |
| 156 | 322.883216 | 0.000126 | | | 255 | 5 | Ack |
| 157 | 322.888365 | 0.005149 | 0xe0b3 | 0x0000 | 178 | 12 | Unknown Command, Bad FCS |
| 158 | 322.896215 | 0.007850 | 0x0000 | 0xe0b3 | 255 | 127 | Data, Dst: 0xe0b3, Src: 0x0000 |
| 159 | 322.896342 | 0.000127 | | | 255 | 5 | Ack |

# Experimental Results (pt. 5)

- We depleted the energy of four commercial Zigbee devices, each powered by a 3-volt CR2450 lithium battery, in **less than 16 hours**
- HiveGuard successfully generated an **alert** for each launched attack during our experiments

# Conclusion (pt. 1)

- We built a distributed system, called **HiveGuard**, to monitor the security of Zigbee networks
- We developed an **energy depletion attack** against battery-powered Zigbee devices to test our prototype's monitoring capabilities

# Conclusion (pt. 2)

- Our experiments show that it is possible for an **outside attacker** to completely deplete the energy of four commercial Zigbee devices in a **relatively short amount of time**
- We are publicly releasing our **source code** and our **captured packets** to enable others to use them for their own projects