Detecting Attacks against Zigbee Networks with HiveGuard

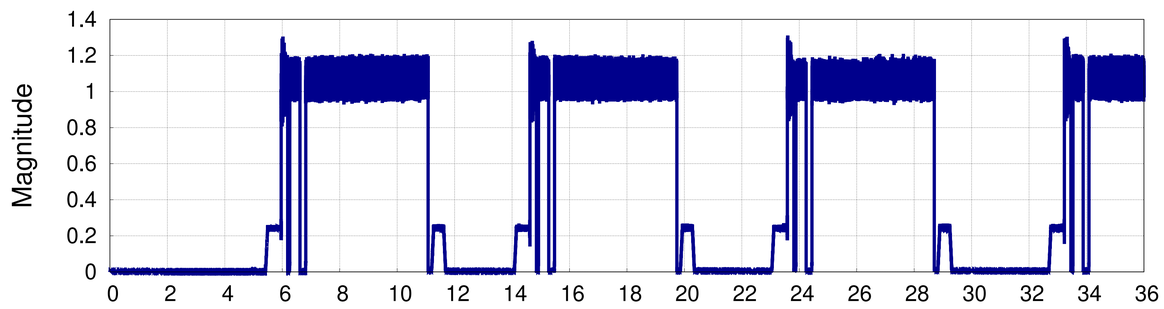
Dimitrios-Georgios Akestoridis
Carnegie Mellon University
akestoridis@cmu.edu

Patrick Tague
Carnegie Mellon University
tague@cmu.edu

1. Motivation

- There is a lack of robust open-source software tools that consumers can use to ***continuously monitor*** Zigbee traffic for potential security issues
- Malicious users can launch several types of attacks against Zigbee networks and ***go undetected***
- Network security monitoring systems can be used to detect attacks that exploit vulnerabilities that ***cannot be eliminated*** with firmware updates

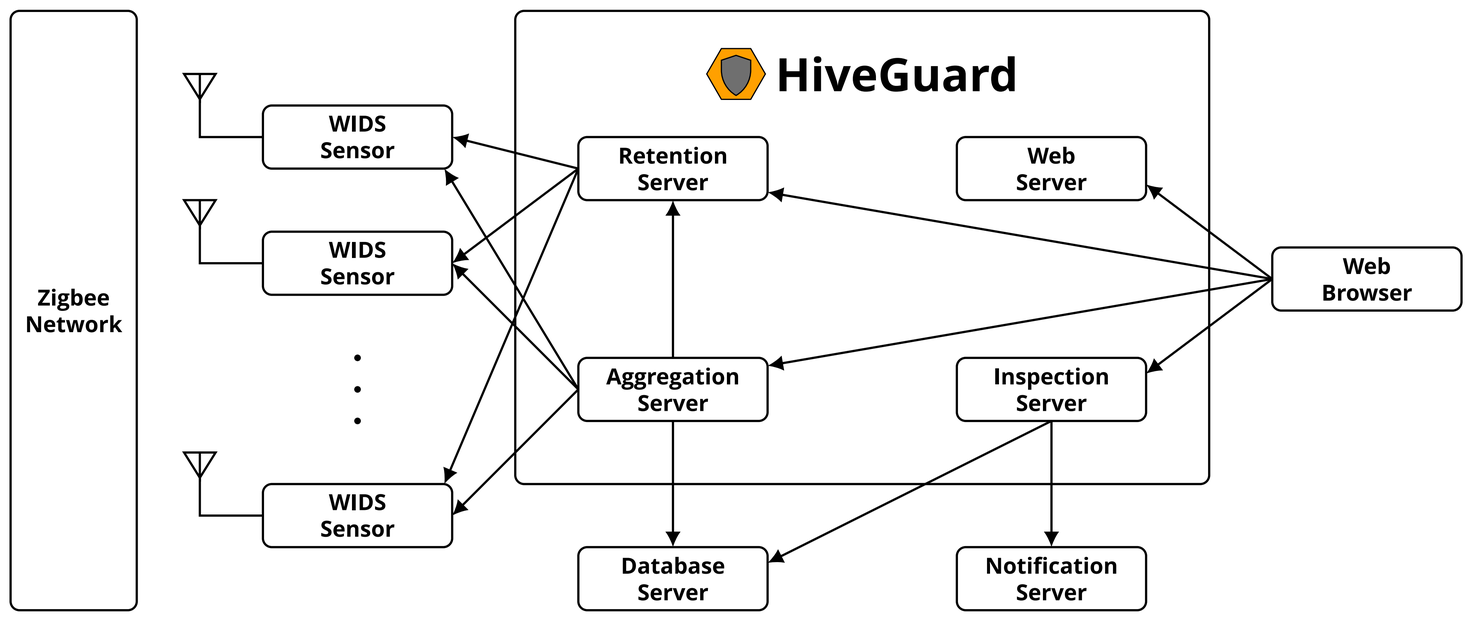
2. Energy Depletion Attack



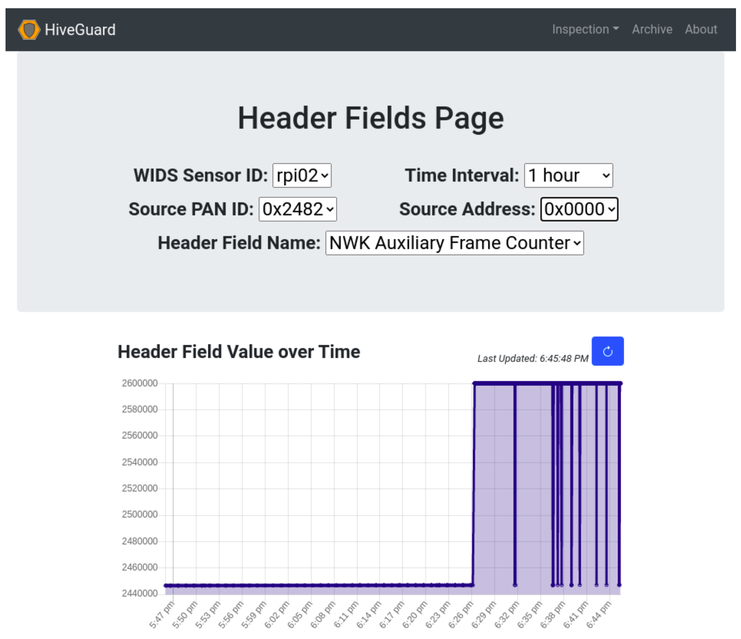
- We developed an energy depletion attack that exploits the way that Zigbee devices are currently handling ***Data Requests*** by selectively jamming them and injecting spoofed packets [1]

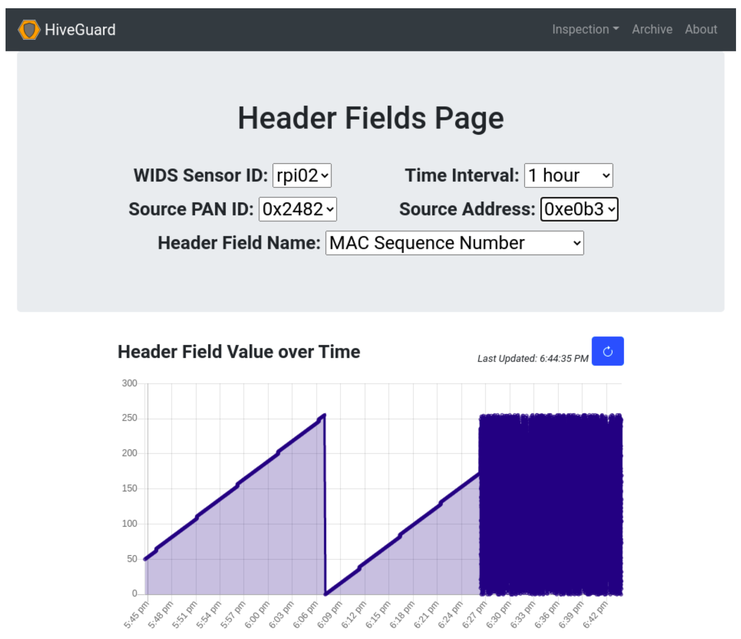
3. System Architecture

- We designed a distributed system, called ***HiveGuard***, that provides archiving, aggregation, inspection, visualization, and alert services [1]
- We enhanced Zigator [2] in order to deploy stand-alone ***WIDS sensors***
- Our ***prototype implementation*** of HiveGuard is publicly available [3]



4. Experimental Results





- We conducted ***four experiments*** in order to test our prototype's monitoring capabilities against our energy depletion attack
- HiveGuard successfully generated an ***alert*** for each attack that we launched during our experiments

We showed that it is possible for an outside attacker to completely deplete the energy of four commercial Zigbee devices, each powered by a 3-volt CR2450 lithium battery, in ***less than 16 hours***

Acknowledgments

This research was supported in part by CyLab. The views and conclusions contained here are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either express or implied, of CyLab or Carnegie Mellon University.

2021 CyLab Partners Conference, Virtual Event, October 2021

References

[1] D.-G. Akestoridis and P. Tague, "HiveGuard: A network security monitoring architecture for Zigbee networks," to appear in Proc. IEEE CNS'21.
[2] D.-G. Akestoridis. Zigator: Security analysis tool for Zigbee networks. [Online]. Available: https://github.com/akestoridis/zigator
[3] ——. HiveGuard: A distributed system for monitoring the security of Zigbee networks. [Online]. Available: https://github.com/akestoridis/hiveguard