Evaluating the Security Vulnerabilities of ZigBee Motion Detectors in Wireless Sensor Networks: A Study on Jamming, Interception, and Behavioral Manipulation

Diogo Marque, Henk Netten, Muhammad Mansour

October 7, 2024

1 Introduction

The rapid proliferation of Internet of Things (IoT) devices in modern homes and industries has brought significant improvements in automation, convenience, and efficiency. ZigBee-based sensors and controllers have emerged as popular choices among these devices due to their low power consumption, scalability, and support for wireless mesh networking. However, the increasing integration of these devices into critical systems, such as home security networks, raises important concerns regarding their security and resilience against attacks.

ZigBee, a widely adopted wireless communication protocol, facilitates connectivity between a variety of smart devices, including motion detectors, lights, thermostats, and security cameras. While its encryption mechanisms—such as AES-128—offer a basic layer of security, vulnerabilities in its implementation and communication protocols have been highlighted in recent research. This brings into question whether ZigBee-based devices, such as motion detectors, can be relied upon in high-security environments or can be compromised by attackers, undermining the entire system's integrity.

This study seeks to evaluate the security and robustness of ZigBee motion detectors, specifically investigating their potential vulnerabilities in security applications. By examining the communication between the motion detector and the hub, the research aims to assess whether these devices can be effectively compromised through methods such as signal jamming, packet interception, and message manipulation. The study will also explore whether the motion detector's intended function—as an automated relay for triggering actions—can be adapted for more secure use in comprehensive security systems.

2 Research Question

Our research question is: How can ZigBee-based motion detectors be safely used for high-security applications, such as break-in detection? We specifically look at jamming, interception, and message manipulation attacks. We split our main research question into two sub-questions:

1. What are the vulnerabilities in the ZigBee-based IoT network?
2. How do we defend against attacks that use these vulnerabilities?

3 Requirements

To conduct the research effectively, specific hardware and tools are required to create and evaluate a ZigBee-based environment. The following items are essential:

• **Philips Hue Motion Sensor**: This sensor is the subject of the experiment, acting as the motion detection device within the ZigBee network. The study will evaluate whether it can be used in security applications (such as break-in detection) rather than just triggering automation systems. The sensor will generate data that will be captured and analyzed during the tests.

• **SDR device (e.g., HackRF One)**: The SDR device is crucial for intercepting and decoding the communication between the motion sensor and the ZigBee hub. A versatile tool for this purpose is the **HackRF One**, which can capture and analyze ZigBee packets and other wireless communication protocols. The HackRF One allows for a more flexible approach, supporting a wider range of frequencies and enabling more advanced techniques such as **signal jamming**, **manipulation**, or interception during the experiment. Its capabilities will help us understand how data is transmitted, offering insights into potential vulnerabilities and allowing us to transmit doctored traffic which is necessary in a variety of possible attacks.

• **Philips Hue Bridge**: Acting as the ZigBee controller (hub), the bridge manages communication between the motion sensor and other devices in the ZigBee network. It plays a critical role in testing real-world communication scenarios between the controller and the motion sensor to assess the effectiveness and security of the ZigBee protocol in this setting.

These components will be used in a lab environment to simulate real-world ZigBee communication, allowing for the observation and manipulation of data flow between devices. Tools like **Wireshark** (for network traffic analysis) and **ZBOSS Sniffer** or **Killerbee** (to capture ZigBee communication) will assist in decrypting and analyzing the packets exchanged within the network.

This setup will enable the testing of security vulnerabilities, such as **jamming attacks**, **data interception**, and the potential manipulation of transmitted information, which are common challenges in ZigBee networks.

4 Related Work

1. **Research on the Security of ZigBee Wireless Sensor Network**: Research by Tang (2022) analyzes various aspects of ZigBee network technology, including its security structure and encryption algorithms. It demonstrates the implementation of symmetric keys and the security architecture of the protocol stack. Additionally, it investigates the security of the ZigBee on different layers. It provides a deeper insight into the structural and security aspects of ZigBee networks. [1]

2. **ZigBee Security Vulnerabilities: Exploration and Evaluation**: This work discusses common vulnerabilities such as jamming attacks and replay attacks in ZigBee networks. It explores how attackers can exploit ZigBee's relatively weak encryption and key management protocols, which are crucial considerations when evaluating whether ZigBee motion detectors are secure enough for break-in detection.[2]

3. **MIT's Security Analysis of ZigBee Protocol**: This paper provides a comprehensive analysis of ZigBee's security, covering encryption mechanisms, key management, and various attack vectors, including jamming and eavesdropping. It gives valuable context for understanding how an attacker might intercept or manipulate the data sent between a ZigBee motion detector and a controller. [3]

4. **Advanced Analysis of ZigBee-based IoT System Security**: Another relevant study offers practical insights into attacks like man-in-the-middle, jamming, and replay attacks, showing how easily ZigBee networks can be compromised without proper countermeasures. The findings align with your aim to evaluate the motion sensor's reliability in a security system. [4]

5. **ZigBee Jamming**: This journal describes a low-tech way of disabling a ZigBee sensor through jamming. They used SDR to perform multiple types of jamming attacks. It also goes into why wireless devices are generally not suitable for physical security applications. [5]

5 Approach & Methods

The objective of this project is to evaluate the security of a ZigBee-based network comprising a motion detector, a ZigBee hub, and an application layer such as a mobile phone. Due to the increasing deployment of ZigBee networks in various IoT applications, ensuring their security is essential. This project aims to identify potential vulnerabilities and assess the robustness of the network against various attacks.

Methodology

Network Setup and Configuration

- **Initial Configuration**: Ensure that all devices are properly configured and communicating effectively within the network.

Packet Capture

- **ZigBee Sniffer**: Utilize a ZigBee sniffer to intercept and capture packets transmitted between the motion detector and the ZigBee hub.
- **Data Collection**: Collect a comprehensive dataset of the captured packets over a defined period.

Traffic Analysis

- **Wireshark**: Employ Wireshark to analyze the captured packets. This involves:
  - **Protocol Dissection**: Examine the structure and content of ZigBee packets.
  - **Traffic Patterns**: Identify normal traffic patterns and any anomalies.
  - **Data Extraction**: Extract relevant data fields for further analysis.

Security Assessment

- **Vulnerability Analysis**: Identify potential vulnerabilities in the ZigBee communication protocol and network configuration.
- **Attack Simulation**: Conduct various attack simulations to test the network's resilience. These may include:
  - **Eavesdropping**: Attempt to intercept and decode sensitive information.
  - **Replay Attacks**: Replay captured packets to observe the network's response.
  - **Denial of Service (DoS)**: Simulate DoS attacks to evaluate the network's robustness under stress.
  - **Man-in-the-Middle (MitM)**: Perform MitM attacks to intercept and alter communication between devices.

Evaluation and Mitigation

- **Impact Assessment**: Assess the impact of each simulated attack on the network's functionality and security.
- **Mitigation Strategies**: Propose mitigation strategies to handle identified vulnerabilities. This may include:
  - **Encryption**: Enhance the encryption used for data transmission.
  - **Authentication**: stronger authentication protocols to prevent unauthorized access.
  - **Network Configuration**: Optimize network configuration to minimize system loopholes.

Expected Outcomes

The project is expected to provide a comprehensive evaluation of the ZigBee network's security, highlighting potential vulnerabilities and the effectiveness of various attack vectors. The findings should aid the development of robust security measures to protect ZigBee-based IoT networks.

6 Ethical issues

We will be sniffing ZigBee traffic. ZigBee transmission distances range from 10 to 100 meters.[6] If there are any ZigBee devices in the area we might pick up some traffic from them. However, we would immediately disregard and delete any data from this as we would be able to tell that it did not come from our device. Other than sniffing some local traffic we would not directly impact others with our experiments.

The findings of our research may have ethical issues. Our research may find it possible to effectively disable devices like the Hue motion sensor. These devices are used in security systems to detect break-ins. Disabling the devices would aid bad actors in breaking into these security systems with a reduced chance of detection.

We may also find it is possible to trigger the sensor with a false positive. This would allow an attacker to reduce a user's trust in the device or make the device effectively unusable.

However, we estimate that if these vulnerabilities do exist, the probability that some bad actors already know of them is sufficiently high that our research would not significantly increase that probability. Furthermore, with these findings, we could notify the manufacturer of the security vulnerability. This would allow the manufacturer to either fix the vulnerability or at least notify the users, thereby preventing bad actors from abusing it.

References

[1] J. Tang, "Research on the security of zigbee wireless sensor network," in *Proceedings of the International Conference on Intelligent Systems, Communications, and Computer Networks (ISCCN 2022)*, vol. 12332, SPIE. Chengdu, China: SPIE, 2022, p. 123321P, yunnan Police College (China). [Online]. Available: https://www-spiedigitallibrary-org.proxy.uba.uva.nl/conference-proceedings-of-spie/12332/2653014/Research-on-the-security-of-ZigBee-wireless-sensor-network/10.1117/12.2653014.full#_=_

[2] S. Khanji, F. Iqbal, and P. Hung, "Zigbee security vulnerabilities: Exploration and evaluating," in *2019 10th international conference on information and communication systems (ICICS)*. IEEE, 2019, pp. 52–57. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8809115

[3] X. Fan, F. Susan, W. J. Long, and S. Li, "Security analysis of zigbee," 2017. [Online]. Available: https://api.semanticscholar.org/CorpusID:37828092

[4] M. Kumar, V. Yadav, and S. P. Yadav, "Advance comprehensive analysis for zigbee network-based iot system security," *Discover Computing*, vol. 27, no. 1, p. 22, Jul 2024. [Online]. Available: https://doi.org/10.1007/s10791-024-09456-3

[5] J. T. Jackson, "Zigbee jamming," in *Journal of Physical Security*. Right Brain Sekurity, 2022, vol. Volume 15, pp. 1–13. [Online]. Available: https://rbsekurity.com/the-journal-of-physical-security.html

[6] (2011, Mar) Zigbee faq. [Online]. Available: https://web.archive.org/web/20130627172453/http://www.zigbee.org/Specifications/ZigBee/FAQ.aspx