Zigbee Network Security

Dimitrios-Georgios Akestoridis

akestoridis@cmu.edu

2020 CyLab Partners Conference

CyLab Security and Privacy Institute

Carnegie Mellon University

Mobile,
Embedded, &
Wireless
Security

What is Zigbee?

- Zigbee is a **wireless communication protocol** that is designed to achieve:
  - Low power consumption
  - Self-forming mesh networking
  - Universal application-layer interactions
  - Low manufacturing cost

What is Zigbee?

- Zigbee is a **wireless communication protocol** that is designed to achieve:
  - Low power consumption
  - Self-forming mesh networking
  - Universal application-layer interactions
  - Low manufacturing cost
- Comparison with other protocols:

	Data Rate	**Battery Life**
Wi-Fi	High	Low
Bluetooth	Medium	Medium
Zigbee	Low	High

Examples of Zigbee Devices

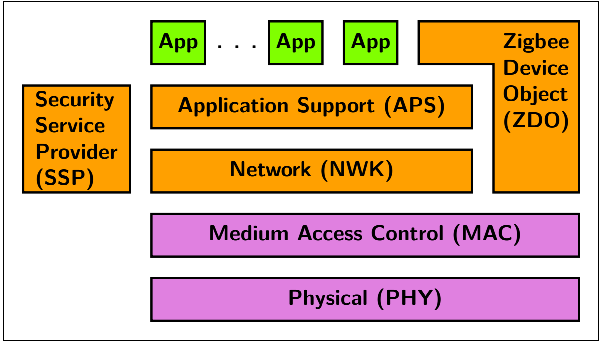
Schlage Connect Smart Deadbolt

SmartThings Outlet (IM6001-OTP01)

SmartThings Hub (IM6001-V3P01)

Security Concerns for Zigbee Networks

- The security of Zigbee networks can affect the **physical security** of smart home residents
- The Zigbee protocol provides security services for packets on its **NWK and APS layers**
- Currently, Zigbee networks do not utilize **MAC-layer security** services


App
. . .
App
App
Zigbee Device Object (ZDO)
Security Service Provider (SSP)
Application Support (APS)
Network (NWK)
Medium Access Control (MAC)
Physical (PHY)

Architecture of the Zigbee protocol stack

Key Contributions[1]

- We developed **Zigator** to analyze the security of Zigbee networks:
  - https://github.com/akestoridis/zigator

[1] D.-G. Akestoridis, M. Harishankar, M. Weber, and P. Tague, "Zigator: Analyzing the security of Zigbee-enabled smart homes," in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2020, pp. 77–88. DOI: 10.1145/3395351.3399363

Key Contributions[1]

- We developed **Zigator** to analyze the security of Zigbee networks:
  - https://github.com/akestoridis/zigator
- We built a **testbed** to study operational Zigbee networks in depth:
  - Packet Sniffing ⟹ Software-Defined Radio
  - Packet Injection ⟹ Software-Defined Radio and IEEE 802.15.4 USB Adapter
  - Packet Jamming ⟹ IEEE 802.15.4 USB Adapter
  - Packet Analysis ⟹ Zigator

[1] D.-G. Akestoridis, M. Harishankar, M. Weber, and P. Tague, "Zigator: Analyzing the security of Zigbee-enabled smart homes," in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2020, pp. 77–88. DOI: 10.1145/3395351.3399363

Key Contributions[1]

- We developed **Zigator** to analyze the security of Zigbee networks:
  - https://github.com/akestoridis/zigator
- We built a **testbed** to study operational Zigbee networks in depth:
  - Packet Sniffing ⟹ Software-Defined Radio
  - Packet Injection ⟹ Software-Defined Radio and IEEE 802.15.4 USB Adapter
  - Packet Jamming ⟹ IEEE 802.15.4 USB Adapter
  - Packet Analysis ⟹ Zigator
- We implemented and validated **selective jamming and spoofing attacks** that can lead to the exposure of the network key:
  - https://github.com/akestoridis/atusb-attacks

[1] D.-G. Akestoridis, M. Harishankar, M. Weber, and P. Tague, “Zigator: Analyzing the security of Zigbee-enabled smart homes,” in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2020, pp. 77–88. DOI: 10.1145/3395351.3399363

Summary of Findings and Developments

- We discovered that an attacker can disconnect Zigbee devices by causing a **PAN ID conflict** and selectively jamming **Network Update** commands

Summary of Findings and Developments

- We discovered that an attacker can disconnect Zigbee devices by causing a **PAN ID conflict** and selectively jamming **Network Update** commands
- We demonstrated how an attacker can then **keep Zigbee devices disconnected** in order to force the end user to factory reset them

Summary of Findings and Developments

- We discovered that an attacker can disconnect Zigbee devices by causing a **PAN ID conflict** and selectively jamming **Network Update** commands
- We demonstrated how an attacker can then **keep Zigbee devices disconnected** in order to force the end user to factory reset them
- We observed that some Zigbee Routers either did not initiate or significantly delayed the **rejoin process** after the jamming of Network Update commands

Summary of Findings and Developments

- We discovered that an attacker can disconnect Zigbee devices by causing a **PAN ID conflict** and selectively jamming **Network Update** commands
- We demonstrated how an attacker can then **keep Zigbee devices disconnected** in order to force the end user to factory reset them
- We observed that some Zigbee Routers either did not initiate or significantly delayed the **rejoin process** after the jamming of Network Update commands
- We responsibly disclosed our findings to the **Zigbee Alliance**:
  - Specification changes will prevent malicious PAN ID changes
  - A more aggressive algorithm will be required to avoid missing PAN ID changes
  - The firmware of SmartThings hubs was modified to ignore PAN ID conflicts[2]

[2] SmartThings Community. (2020), Hub firmware release notes - 0.31.4, [Online]. Available: https://community.smartthings.com/t/hub-firmware-release-notes-0-31-4/197941

Future Research Directions

- Extend our security analysis to the application layer of the Zigbee stack
- Study security enhancements for the Zigbee protocol
- Develop monitoring tools for Zigbee networks
- Zigator project webpage:
  - http://mews.sv.cmu.edu/research/zigator/

CyLab Security and Privacy Institute

Carnegie Mellon University

Mobile,
Embedded, &
Wireless
Security