# DISCOVERING AND PATCHING SECURITY VULNERABILITIES IN A ZIGBEE WIRELESS SENSOR NETWORK IMPLEMENTATION

**Anthony Lopez**, Bharathan Balaji, Yuvraj Agarwal, Alex Orailoglu
CSE Department , University of California, San Diego

## Introduction

- *ZigBee* is a *protocol* for wireless sensor networks.
- Its an *emerging specification* for *new generation* networks and technology.
- It is useful because it requires devices that use *low power* and *low data rates*.
- There are many applications that ZigBee can be used for.


ZigBee Energy Meter


UCSD CSE ZigBee Network Implementation

- In this case, the application is for the smart building.
- To prevent threats from attackers, this project is to find and patch the vulnerabilities.
- The challenges for this project include the number of sensors, different channels, layers of networking, and many types of attacks.

## ZigBee Specification

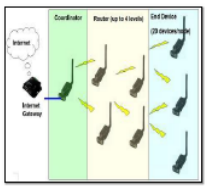


Figure 1: ZigBee Devices/Topology

### General

- ZigBee used for *low-power* and *low-data rate* networks.
- *Many applications* that ZigBee is used for: Medical purposes, home automation, and smart buildings.
- Allowing user to define application and their own network structure allows flexibility.

### Technical

- The *Zstack* is based off of the *IEE 802.15.4* stack: MAC and PHYS layers.
- MAC and PHYS layers define the hardware components of a ZigBee device.
- Layers above the MAC layer defined by the *ZigBee Alliance*.
- Upper layers define the software, network topology, and mode of security.

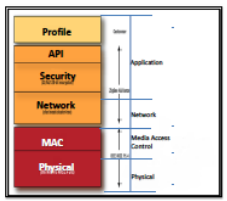


Figure 2: Z-Stack and Layers.

## ZigBee Security

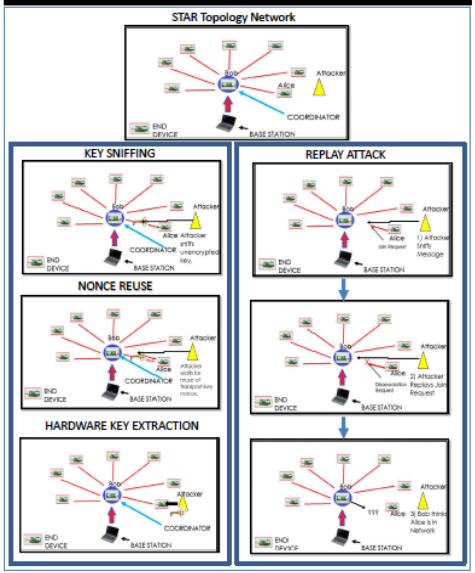
| KEYS | MODES | |
|---|---|---|
| | SS: | HS: |
| NK: | YES | YES |
| MK: | NO | YES(O) |
| LK: | YES(O) | YES(O) |

Figure 3: ZigBee Keys and Security Modes. E. Yüksel, et al. ZigBee-2007 Security Essentials. (NordSec 2008), pages 65-82.

NK: Network Key; MK: Master Key; LK: Link key; SS: Standard Security; HS: High Security

- Two types of security in ZigBee 2007 version: *Standard* and *High*.
- UCSD CSE Building *uses Standard Security* (SS) because it has a lower data rate and requires lower power than High Security (HS).
- No security breaches on network have been successful yet so no reason to update to HS.
- Standard sends the *first network key* to a commissioned node in *plaintext*.
- Standard security vulnerable to *insider* attacks and *some outsider* attacks.

## Data: Possible Attacks




## Equipment


Figure 4: TI Packet Sniffer

- The *packet sniffer* provides the ability to monitor the network in terms of its traffic.
- Catches messages Over-The-Air and presents them with information specific to the layers.
- Allows better view of images compared to other sniffers like Wireshark.

- KillerBee framework provides the means of mimicking attacks like an attacker would on ZigBee network.
- The framework provides code for attacks such as zbreplay which mimics the replay attack and zbsniff which mimics the key sniffing attack.
- In addition, it provides an attack called zbassocflood which mimics a denial of service.


Figure 5: KillerBee Tools

KillerBee, Framework and tools for exploiting ZigBee and IEEE 802.15.4 networks, URL http://killerbee.googlecode.com

## Network Evaluation

- The vulnerabilities that this project will focus on involve mostly the point at which devices join the network. Power downs, disconnected devices, and newly joining devices are all different cases that involve joining devices.
- Attacks such as *key sniffing*, *replay*, *nonce reuse*, and *hardware key extraction,* and *denial-of-service* can be implemented with KillerBee.
- Currently, sniffing messages is successful but obtaining the network key when a device *rejoins* is not. Further research is required for when a device *first joins* a network or *rejoins* after entire network powers down/disconnects.
- *Replay attack is unsuccessful* due to *frame counter* protection.
- Future goals include:
  - Continue to implement the *KillerBee framework* to try its attacks to obtain the Network Key of a network.
  - Figure out which attacks are successful and why.
  - Determine if switching to High Security is necessary or improving current security mechanisms can be done. To patch the vulnerability.

UCSDCSE Computer Science and Engineering

synergy systems, networking and energy efficiency