Department of Computer Science

FLORIDA TECH
FLORIDA'S STEM UNIVERSITY™

CSE 4820: Wireless and Mobile Security

14. Zigbee Overview

Dr. Abdullah Aydeger
Location: Harris Inst #310
Email: aaydeger@fit.edu

Outline

- Zigbee
  - History
  - Layers
  - Security

Recall: Software Defined Radios

- The process of reverse engineering a radio signal to understand elements such as frequency, modulation, encoding, and protocol in order to intercept or replicate the signal
  - For ex. replace sound waves with radio waves
    - By using special 'radio soundcard', you can receive and transmit arbitrary signals
- Has redefined wireless hacking
  - Instead of being limited by black box radios, unfettered access to RF
    - Access to Radio modules/protocols that were obscured

Recall: How to try this in wild?

- Finding a target
  - For ex., key fob, garage opener, wireless mouse, and RC car
- Device reconnaissance;
  - Figure out what frequency it uses
- Finding and capturing signal
- Replaying/changing

Zigbee

- Set of standards for low-power wireless networking
  - Devices with up to 5 years battery life
- Low data-rate transfers, short-range, persistent-powered network coordinators/routers, and simple protocol stack
- Found in industrial and home applications
  - For ex., home theater remote controls to hospital patient monitoring systems

Zigbee as Wireless Standard

- Strong position to be the wireless tech for IoT
  - Already used in Google Nest Smart Thermostat, Philips Hue led light bulbs, Comcast Xfinity home security router to connect home light switches and other peripherals to public internet
- Why do we need Zigbee?
  - Compared to Wifi and BLE, Zigbee is much simpler protocol with a fully functional stack implemented in 120kb of NVRAM where some vendors claim to make reduced-functionality stacks as small as 40kb

Zigbee as Wireless Standard

- Wireless networks transmit at least 54mbps, BLE 1-3mbps, and Zigbee 20-250kbps
  - Not the right protocol for high-speed data transfers
- Wifi devices; relatively short battery life
  - Bluetooth relatively comparable to Zigbee
- Deployed mostly for the home automation;
  - Connectivity among home control systems such as electrical appliances, lighting controls, home security, etc.

Zigbee Overview

Solution	Description
Network Protocol	Zigbee PRO 2015 (or newer)
Network Topology	Self-Forming, Self-Healing MESH
Network Device Types	Coordinator (routing capable), Router, End Device, Zigbee Green Power Device
Net. Size (theoretical # of nodes)	Up to 65,000
Radio Technology	IEEE 802.15.4-2011
Frequency Band / Channels	2.4 GHz (ISM band) 16-channels (2 MHz wide)
Data Rate	250 Kbits/sec
Security Models	Centralized (with Install Codes support) Distributed
Encryption Support	AES-128 at Network Layer AES-128 available at Application Layer
Communication Range (Avg)	Up to 300+ meters (line of sight) Up to 75-100 meter indoor
Low Power Support	Sleeping End Devices Zigbee Green Power Devices (energy harvesting)
Legacy Profile Support	Zigbee 3 devices can join legacy Zigbee profile networks. Legacy devices may join Zigbee 3 networks (based on network's security policy)
Logical device support	Each physical device may support up to 240 end-points (logical devices)

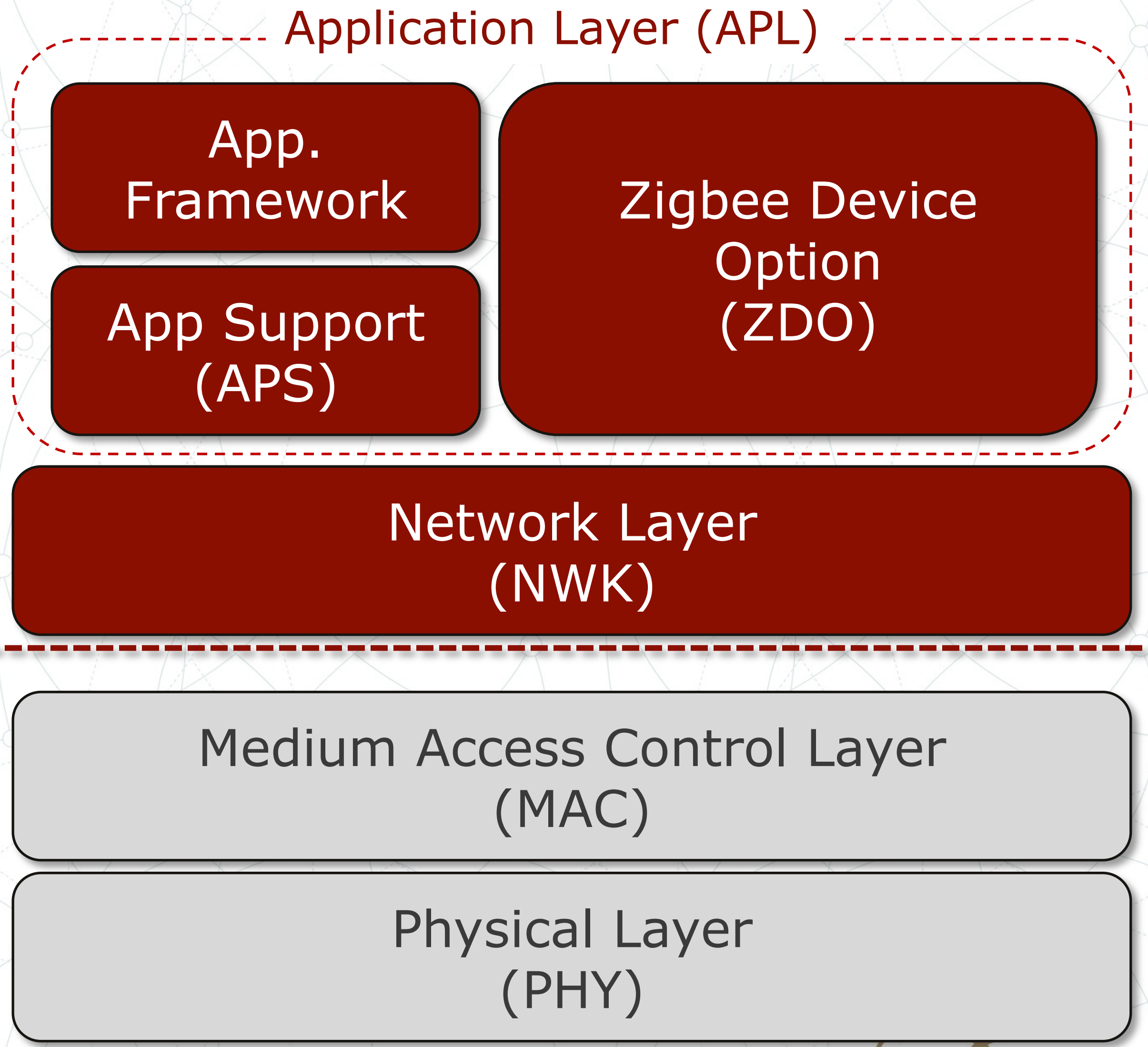
Zigbee History

- First Zigbee specification Zigbee-2004
  - Attractive to organizations in which rival wireless protocols were not a good fit
- Zigbee-2006; group addressing capabilities where one device sends message to multiple clients with a single frame
  - Simplifying the process of developing cross platform compatible apps over Zigbee

Zigbee History

- Zigbee Pro in 2007 defined enhanced security features and ability to send large messages through data fragmentation
- Zigbee in 2012; multihop mesh network range capability
  - Also, ‘Green Energy’ feature where devices can join and interact with Zigbee network without the need for an outside power source (harness energy from other ’green’ ways)

ZigBee Layers



🟥 Defined by Zigbee Alliance

⬜ Defined in IEEE 802.15.4 (Low-rate wireless personal area network)

https://csa-iot.org/all-solutions/zigbee/

Zigbee: Physical Layer

- Physical layer defined by IEEE 802.15.4 Specification
- To avoid interference, uses Direct Sequence Spread Spectrum or Parallel Sequence Spread Spectrum

Channel	Width	Freq	Data
0	600 KHz	868 MHz	100 Kb/s
1-10	2 MHz	915 MHz	250 Kb/s
11-26	5 MHz	2.4 GHz	250 Kb/s

- Operates on 915 MHz (North and South America), 866 MHz (Europe), or 2.4 GHz (worldwide)

Zigbee: MAC Layer

- Includes functionality needed to build extensive Zigbee networks
  - Including the design of device interconnect topologies, device roles, packet framing, and network association/disassociation
- Each device has set of capabilities defined by operational roles:
  - Trust Center, Coordinator, Router, and End Device

Zigbee: MAC Layer

- **ZigBee Trust Center (TC):**
  - Fully functional Zigbee device (FFD) responsible for the authentication of devices that join Zigbee network
  - When a device attempts to join, nearest router notifies the TC that a device has joined
    - TC instructs router to authenticate or terminate new node’s connection

Zigbee: MAC Layer

- **ZigBee Coordinator (ZC):**
  - Fully controls the Personal Area Network (PAN)
  - Performs replay messages on behalf of other devices
  - Allow other Zigbee devices to join them and participate in the network
  - Selects network channel to reduce interference
  - Issues 16-bit device addresses

Zigbee: MAC Layer

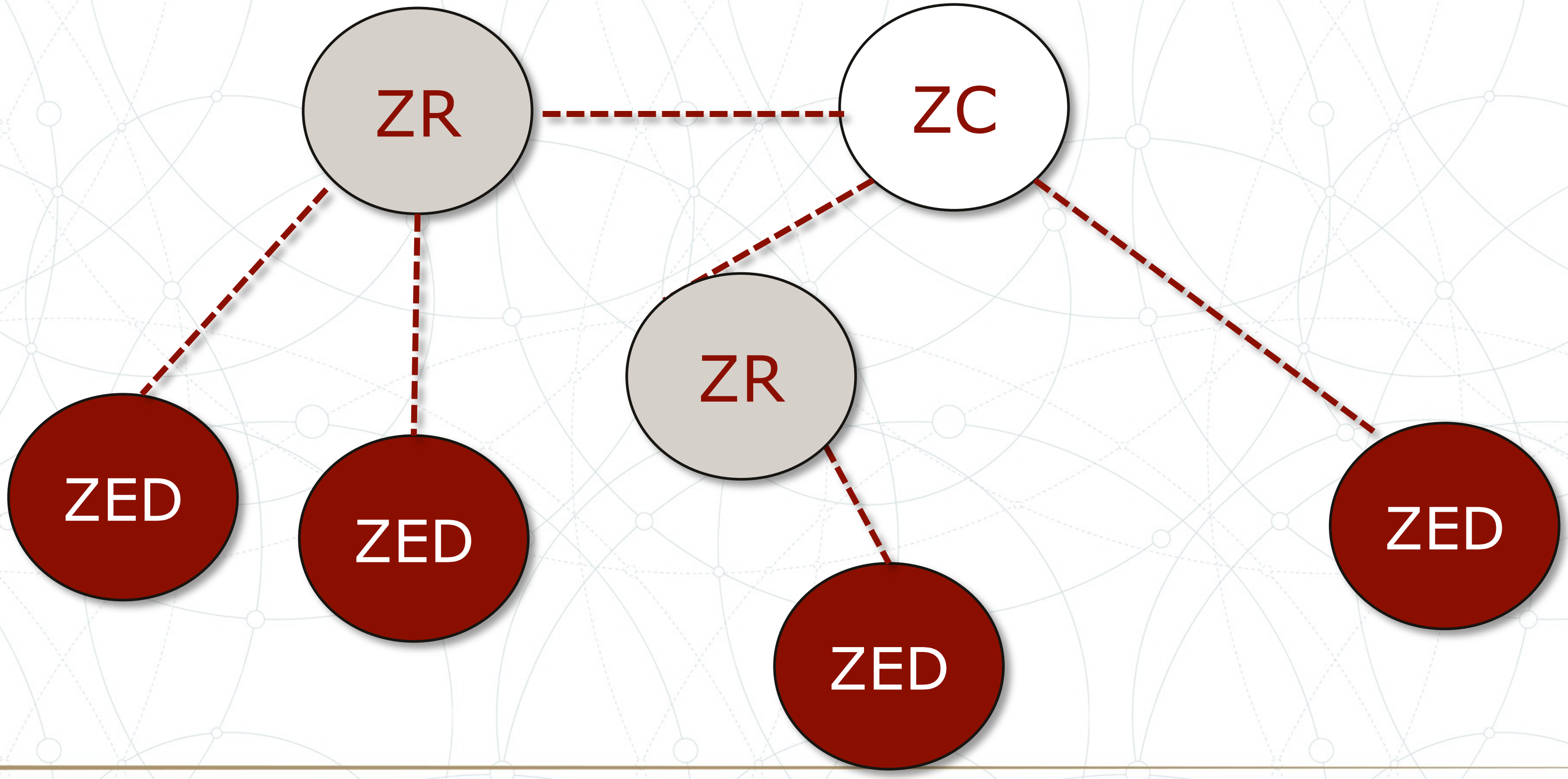
- **ZigBee Router (ZR):**
  - Similar to ZC but defers network management to ZC;
  - Allows devices to join network
  - Performs replay messages on behalf of other devices

Zigbee: MAC Layer

- **ZigBee End Device (ZED):**
  - Participates in network but cannot relay ZigBee frames for other devices;
  - Directly connected to ZR or ZC, cannot connect to another ZED

Example Zigbee Network

- One ZC for the network, additional ZRs



ZR ZigBee Router

ZC ZigBee Coordinator

ZED ZigBee End Device

Example Zigbee Network

- Can be deployed in a star or mesh topology
- ZRs are essential to build and bridge traffic to and from downstream nodes (ZEDs or other ZRs), whereas ZC manages network operation
- Period of inactivity (aka sleep mode) where ZEDs can shut down all transceiver functions for a period of time (microsecs to hours)
  - Can wake up/transmit anytime and go back sleep afterwards
    - Mechanism to allow long battery life
  - ZRs and ZC are generally deployed with persistent power source since they need to be ready to receive anytime

IEEE 802.15.4 MAC Frame Format

Frame Control	Seq. No.	Dest. Pan ID	Dest. Addr	Source Pan ID	Source Addr	Aux Sec Hdr	Payload	FCS

- Specified in IEEE 802.15.4 Spec
- Frame Control tells what type of frame (beacon, command, data, ack…)
- Sequence Numbers enables in-order delivery
- Dest/Src Pan ID/Addr handles delivery of frame
- Auxiliary Security Header optionally implements security
- FCS is CRC 16-bit checksum of the mac layer frame

Zigbee MAC Frame Types

- Beacon Frames – used for network discovery; scan the network for ZC or ZR
- Command Frames – same as 802.11 management (association/disassociation)
- Data Frames – same as 802.11 data; exchange data b/w devices
- Acknowledgement Frames – acknowledge frames that were received

ZigBee Network Layer (NWK)

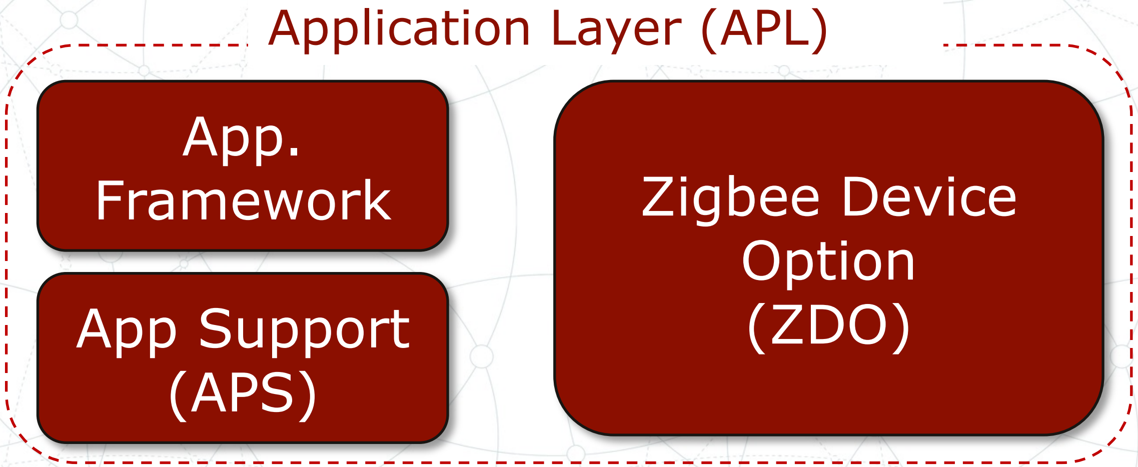
- ZigBee Network Layer (NWK) defined by ZigBee Alliance
    - Responsible for network formation, address allocation, and routing
- Network formation; FFD establishes itself as network coordinator
- Through device discovery, the coordinator must;
    - Select suitable channel to avoid interference
    - Choose random Pan ID that doesn’t conflict with nearby Pans
    - Select and issue 16-bit device addresses for devices

ZigBee Application Layer (APL)

- Specifying operation and interface for application objects that define Zigbee device's functionality
- Application objects are developed by Zigbee Alliance as standard functionality profiles, or
  - By manufacturers for proprietary device functionality using the APL as mechanism to communicate with lower layers of Zigbee stack

ZigBee Application Layer

- ZDO: provides core functionality
  - Setting roles (ZC, ZR, ZED)
  - Encryption
  - Network management (association)
- APS: provides functionality to application profiles (such as reliable data delivery)
- Application Profiles: Define actual functionality of devices
  - ZigBee Link Lighting (ZLL)
  - ZigBee Home Automation (AHA)



Zigbee Security

- AES encryption, device and data authentication using a network key
- Two operational modes:
  - Standard; TC authorizes deices through the use of ACL (Access control list), each devices uses a single shared key
  - High Security; TC keeps track of all encryption and authentication keys used on the network, enforcing policies for network authentication and key updates
    - If TC fails, no device will be permitted to join the network

Zigbee Security Design Rules

- Each layer originates a frame is responsible for securing it
  - If APL requires data to be secure, APL will protect the data (can be both at NWK as well)
- If protection from unauthorized access is required, NWK security will be used on all frames following association and key derivation

Zigbee Security Design Rules

- An open trust model is used within a single device where key reuse is permitted between layers (NWK and APL)
- End-to-end security is accommodated
  - Only source and destination can understand (not the TC)
- Same security level must be used by all devices in the network and by all layers of device

Zigbee Encryption

- Uses 128-bit AES
  - Assumed to be strong security
  - Could be leveraging AES in an insecure manner
    - How?
- Three types of keys to manage security;
  - Master key, network key, and link key

Zigbee Keys

- Master key; optional except the Zigbee Pro stack
  - Used in conjunction with Zigbee symmetric key-key establishment (SKKE) process to derive other keys
- Network key; protect broadcast and group traffic, as well as authenticating to the network
  - Common key among all nodes
  - Can be distributed to a device in plaintext when it joins the network
- Link key: protect unicast traffic between two devices

Zigbee Encryption Keys

- Global Link Key: used by all nodes on the network
- Unique Link Key: used to encrypt communication between a pair of nodes
    - Preconfigured Link Key: used between trust center and a node;
        - Derived prior to joining
    - Trust Center Link Key: used between trust center and a node; distributed to node
    - Application Link Key: used between pair of nodes; distributed to node

Zigbee: Key Provisioning

- Significant challenge; process of provisioning, rotating, and revoking keys on devices
- Zigbee Pro; Administrator can use the SKKE method to derive the network and link keys on devices
  - Requires devices to have master key provisioned on the TC and device joining the network

Zigbee: Key Provisioning

- Key transport; network and link keys are sent in plaintext over the wireless network to the device when it joins
  - Can Easily be intercepted
- Pre-installation; administrator preconfigures all devices with the desired encryption keys at the manufacturing process
  - How to accommodate key revocation and rotation methods?
  - Manual changes to each device to change keys

Zigbee Authentication

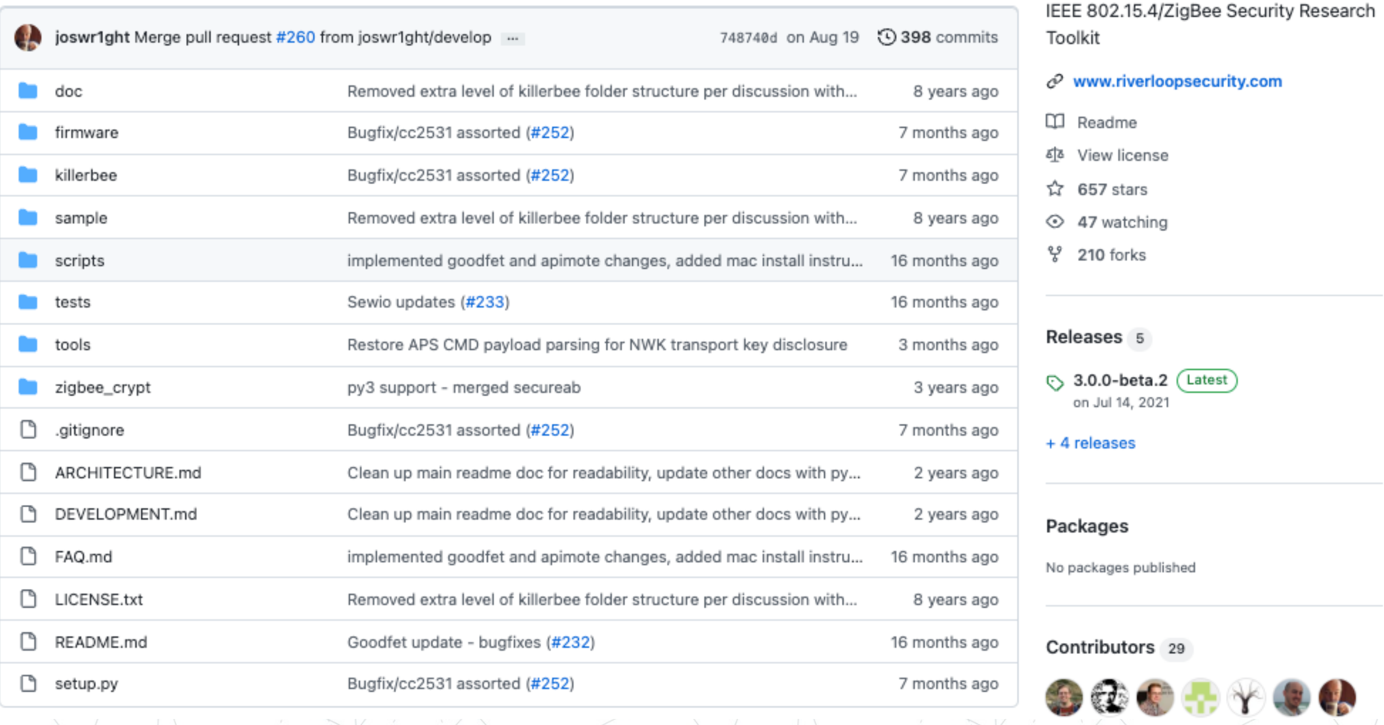
- MAC address validation through ACL;
  - A list of authorized devices is maintained on each node
  - Challenging to keep the list up-to-date (memory req.)
- Standard mode; TC grants access by issuing a network key
  - Sent in plaintext
- High security mode; SKKE method to derive the network key
  - 4-way handshake

Zigbee Authentication’s Vulnerability

- No mutual authentication is used in standard Zigbee (except high security mode with SKKE)
  - Authenticating node accepts the identity of TC for the delivery of network key without any validity check to verify the identity of the network
  - Easy to impersonate a legitimate network by using the same PAN ID as target, potentially on a different channel

Zigbee Attacks

- KillerBee:
  - Python-based framework for manipulating and penetration testing Zigbee and IEEE 802.15.4 networks
  - Written and tested on Linux, free and open-source
  - Includes support for Scapy
  - Includes a variety of tools including zbwireshark, zbdump, and zbreplay



joswr1ght Merge pull request #260 from joswr1ght/develop ··· 748740d on Aug 19 398 commits

doc	Removed extra level of killerbee folder structure per discussion with...	8 years ago
firmware	Bugfix/cc2531 assorted (#252)	7 months ago
killerbee	Bugfix/cc2531 assorted (#252)	7 months ago
sample	Removed extra level of killerbee folder structure per discussion with...	8 years ago
scripts	implemented goodfet and apimote changes, added mac install instru...	16 months ago
tests	Sewio updates (#233)	16 months ago
tools	Restore APS CMD payload parsing for NWK transport key disclosure	3 months ago
zigbee_crypt	py3 support - merged secureab	3 years ago
.gitignore	Bugfix/cc2531 assorted (#252)	7 months ago
ARCHITECTURE.md	Clean up main readme doc for readability, update other docs with py...	2 years ago
DEVELOPMENT.md	Clean up main readme doc for readability, update other docs with py...	2 years ago
FAQ.md	implemented goodfet and apimote changes, added mac install instru...	16 months ago
LICENSE.txt	Removed extra level of killerbee folder structure per discussion with...	8 years ago
README.md	Goodfet update - bugfixes (#232)	16 months ago
setup.py	Bugfix/cc2531 assorted (#252)	7 months ago

IEEE 802.15.4/ZigBee Security Research Toolkit

www.riverloopsecurity.com

Readme

View license

657 stars

47 watching

210 forks

Releases 5

3.0.0-beta.2 Latest
on Jul 14, 2021

+ 4 releases

Packages

No packages published

Contributors 29

https://github.com/riverloopsec/killerbee

FLORIDA TECH

FLORIDA'S STEM UNIVERSITY™

Thank you.
Questions?

Dr. Abdullah Aydeger