ITSC 301: Wireless Security

Module 8 – Non-802.11 Protocols

Table of Contents

Review Lecture & Lab

Review Module 7 Lecture/Lab

- Wireless architecture
- Wireless infrastructure
- Function of each device
- Application for each device
- Monitor wireless network traffic
- Evaluate wireless network traffic
- Module 7 Lab

Module 8: Non-802.11 Protocols

Small Group Discussion

- Outline ZigBee and IEEE 802.15.4 physical and MAC layer architectures

XBee Products

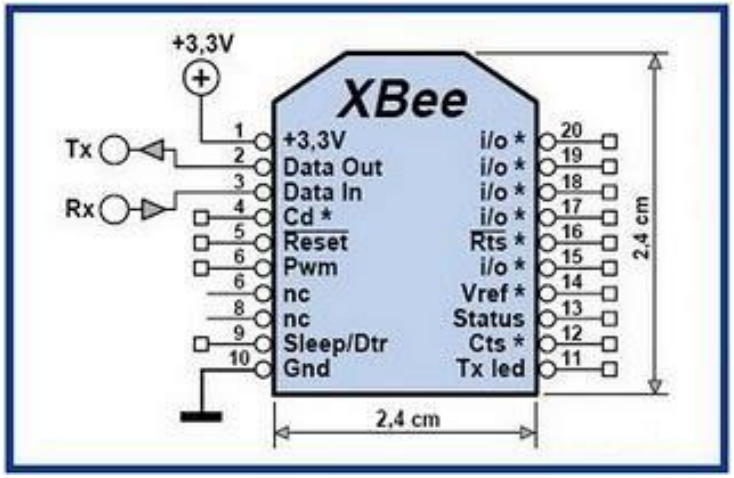


Figure 1: title
Source: Gravitech, 2014. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Figure 2: title
Source: Gravitech, 2012. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Zigbee Profiles

- Profiles defined to allow product interoperability between vendors
- Defines message types, security requirements, etc.
- Main areas of interest:
  - Health: patient monitoring
  - Smart energy: metering, SCADA, demand management
  - Building automation: security, HVAC, lighting
  - Industrial control: process control, energy management

Introduction to IEEE 802.15.4

- IEEE 802.15.4 is the basis for several low- to medium-speed networks
  - Zigbee
  - Zigbee pro
    - 6LowPAN
- Competes with Bluetooth Low Energy
- Allows P2P, mesh, one-to-many connections
- Allows for:
  - End points with limited functionality
  - Routers
  - Co-ordinators
  - Zigbee allows for Trust Center

IEEE 802.15.4 Physical Layer

- Typical frequencies:
  - 902 to 928 MHz
    - North and South America
    - Range divided into 10 channels
  - 868 to 868.6 MHz
    - Single channel
  - 2.4 to 2.4835 Ghz
    - International
    - Range divided into 16 channels

IEEE 802.15.4 Physical Layer

- In this module, focus is on the 2.4 to 2.4835 Ghz range
  - Normal transmission speeds of up to 250 Kbps
  - Direct sequence spread spectrum
  - Modulation is O-QPSK (offset-quadrature phase shift keying)
    - Allows for 2 bits per sample (four possible phases of the carrier) with an offset of -π/4 and a 90° phase shift per 2 bits

IEEE 802.15.4 Physical Layer

- Physical layer also handles:
  - Transceiver switching between three states:
    - Receive (RX)
    - Transmit (TX)
    - Sleep (ZZZ)
    - Typical maximum switching time: 48 bit periods
  - Energy detection:
    - Used for channel selection
    - No decoding, just energy measurements
    - Used for clear channel assessment (CCA)

IEEE 802.15.4 Physical Layer

- Physical layer also handles:
  - Clear Channel Assessment (CCA)
    - Three modes of assessment
    - Energy detection (see previous slide)
    - Carrier sense
    - Carrier sense with energy detection
  - Channel selection

Layer 2 Media Access Control

- Similar to MAC in IEEE 802.11
  - No CTS/RTS
  - Uses Carrier Sense Multiple Access/Contention Avoidance (CSMA/CA) – randomized back-offs
  - Two basic modes:
    - Beacon
    - Non-beacon (just “go for it”)
  - Beacon uses a “super frame” mechanism

MAC Beacons

- Beacon terminology:
  - Guaranteed Time Slot (GTS)
  - Contention Access Period (CAP)
  - Contention Free Period (CFP)
  - Quality of Service (QOS)
  - Personal Area Network (PAN)

Application Support Layer

- Handles link-level encryption depending on application requirements
- If network-level encryption is present it will be used.

Encryption Key Hierarchy

- Master key
  - Supplied with product
    - Steals sensor dump key from RAM after firmware reload
  - Supplied via Trust Center
    - Key transmitted in the clear or vendor/profile defaults
- Network key
  - Used by all link-level messages if used by profiles
- Link key
  - Used for inter-device communications

Key Issues

- Commissioning new devices or re-establishment of communications:
  - Link key may be transmitted in the clear
  - Many profiles rely on fallback keys known to all device-compatible manufacturers
  - Home automation default link key
    - 5A,69,67,42,65,65,41,6C,69,61,6E,63,65,30,39
- Key rotation is difficult, devices are usually asleep

Key Issues

- Sensor processors typically very slow
- Limited RAM and extreme power requirements limit complexity of key management
- Sensors typically do not have tamper protection

Security Modes

- Null
  - in the clear, no security
- AES-CTR
  - AES 128 with nonce
- AES-CBC-MAC uses message authentication code (MAC) to authenticate message
- AES-CCM encrypts message and uses MAC

Security Mode Issues

- AES-CTR
  - Radios need large numbers of ACL entries to prevent nonce reuse (frame count and key counter same)
  - ACL is key and nonce pair
  - Standard allows up to 256 ACL entries on a radio but most radios have two entries
  - If replay protection is enabled, a denial of service is possible by injecting a packet with maximum values in frame and key counters

Areas of Interest

- Modeling of existing open source stacks
  - Instrumented stack
  - Evolutionary attack – stress and state machine testing
  - Fuzzing
- Targeted attacks
  - Oil/gas remote sensors
  - Power meters
  - SCADA applications
  - Home security

Attack Surface

- Physical, MAC, routing and message attacks are possible
  - Discovery of key material
    - Spoofing, data gathering, selective forwarding
  - Routing attacks
    - Sybil, selective forwarding, tunneling
  - Denial of service
    - Sinkhole, selective forwarding, jamming
  - Replay attacks
    - Valves, servos, etc.
    - Access or temperature controls

Superframe Structure

- Outline ZigBee and IEEE 802.15.4 physical and MAC layer architecture

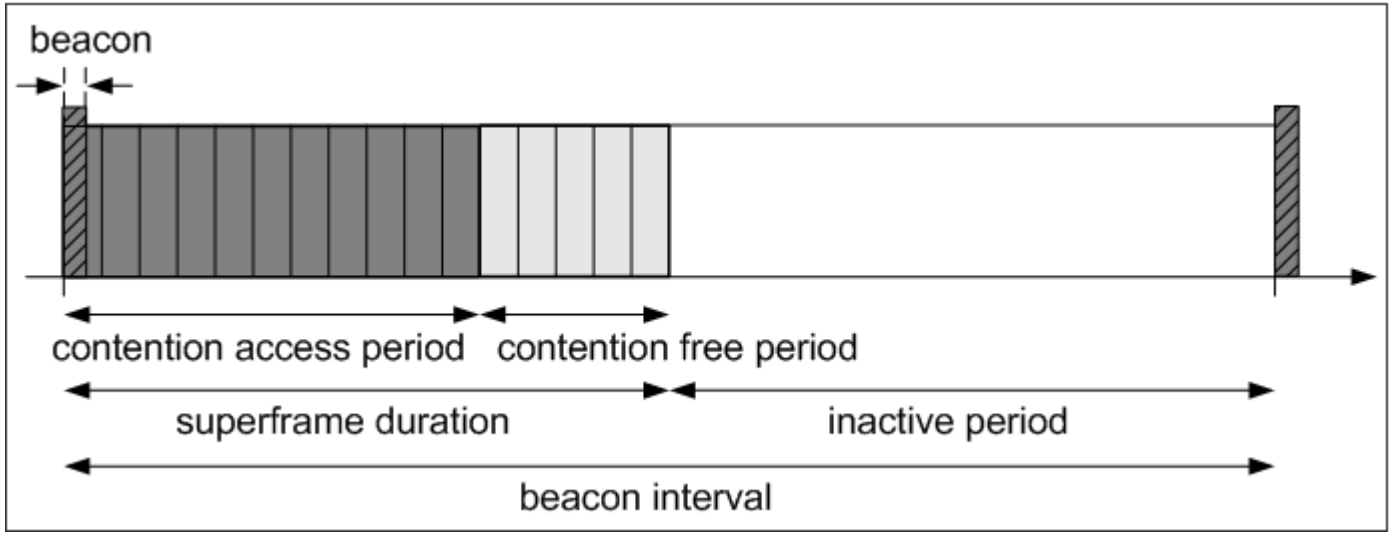


Figure 3: Superframe Structure

Source: PRISM Model Checker, (n.d.). Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

IEEE 802.15.4 Parameters

Physical Layer Parameters

Attribute	Value
CCA duration	8 symbol periods
PHY acknowledgement frame length	11 octets
PHY beacon frame length	23--100 octets
PHY data frame length	15--133 octets
aBaseSlotDuration	60 symbol periods
aMaxBE	5
aMaxFrameRetries	3
aMaxSIFSFrameSize	18 octets
aMinCAPLength	440 symbol periods
aMinLIFSPeriod	40 symbol periods
aMinSIFSPeriod	12 symbol periods
aTurnaroundTime	12 symbol periods
aUnitBackoffPeriod	20 symbol periods
macAckWaitDuration	120 or 54 symbol periods
(channels 0 to 10 and 11 to 26, respectively)	
macBeaconOrder	0-15 (default 15)
macMaxCSMABackoffs	0-5 (default 4)
macMinBE	0-3 (default 3)
macSuperframeOrder	0-15 (default 15)

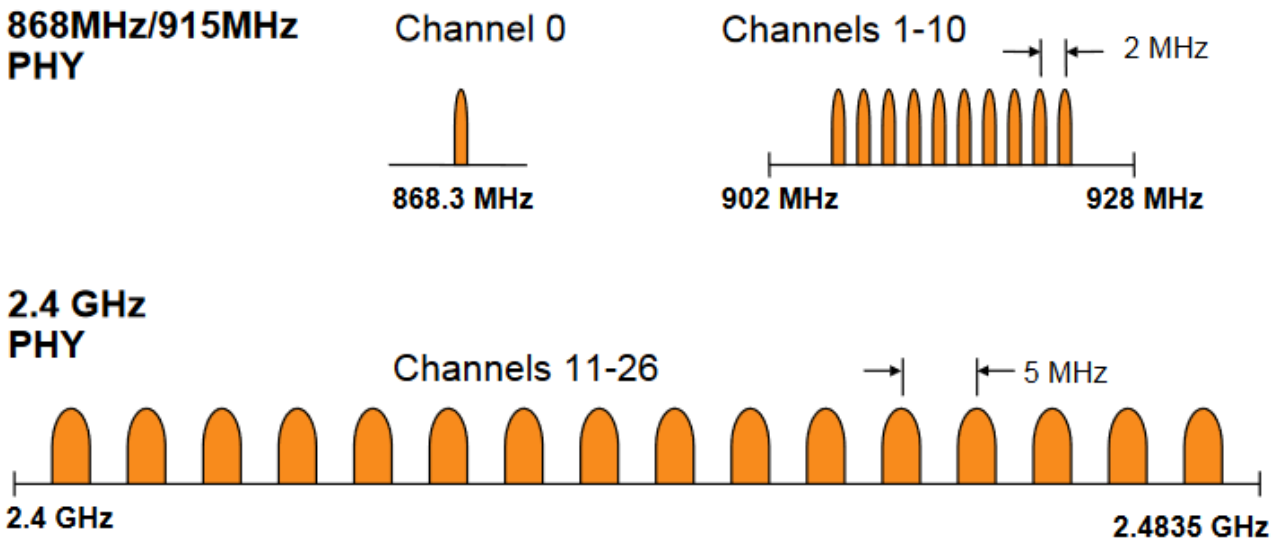
Figure 4: Physical Layer Parameters

Source: PRISM Model Checker, (n.d.). Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Channel Assignment in 802.15.4

802.15.4 Physical Layer

Operating Frequency Bands



Jamming

- Super frame structure is subject to selective or broad-based jamming
- If sensor uses GTS, then the signal can be selectively overridden

Packet Snooping and Injection

- Many networks unencrypted or use only a single vendor-specific key
- Some profiles use sequence numbers to help mitigate injection/replay issues

Small Group Discussion

- Discuss weaknesses in ZigBee key provisioning and management mechanisms.

Possible Solutions

- Near Field Key Delivery
  - Impractical for large, temporary networks
  - Can be monitored and overridden
- Better hardware protection for CPU and RAM
- Fixed network configurations with unique device keys
  - Complex, requires large number of ACL entries
  - Joining network still an issue

Tools

- KillerBee
  - Uses RZUSB sticks with custom firmware
    - Packet sniffing: Wireshark compatible
    - Packet injection: replay attacks, sybil, hello, selective forwarding
- High gain antennas
  - Yagi 18 to 25 db gain
  - Jamming, routing attacks
  - Data collection
- Software defined radio
  - HackRF

Non 802.11: Bluetooth

Small Group Discussion

- Bluetooth technology introduction, assessing the Bluetooth protocol stack

Bluetooth Network Architecture

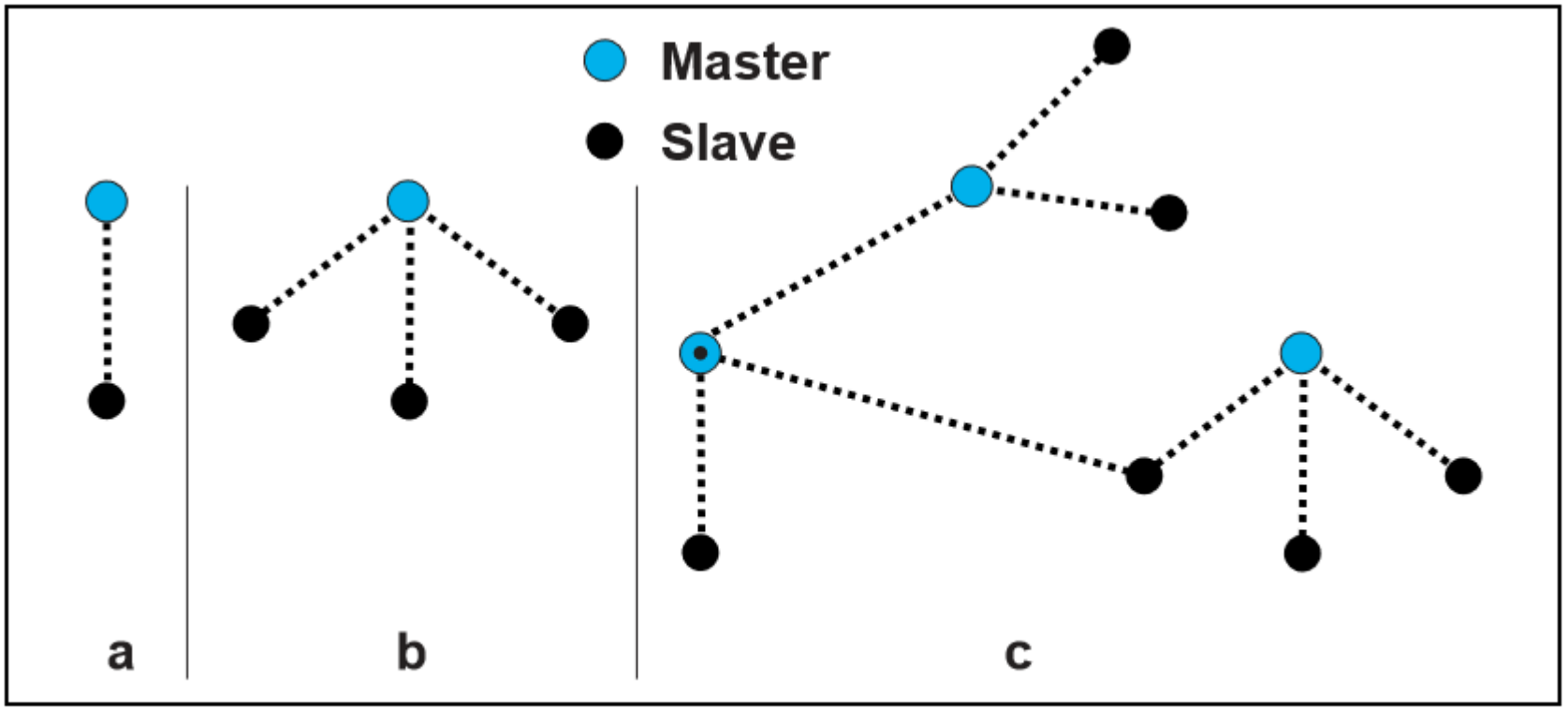


Figure 1.1: Piconets with a single slave operation (a), a multi-slave operation (b) and a scatternet operation (c)

Figure 4: Piconets with a Single Slave Operation (a), Multi-Slave Operation (b) and Scatternet Operation (c)
Source: Bluetooth Specification, (2016). Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Bluetooth Transmitter Characteristics

- Physical layer architecture of Bluetooth wireless protocols

Power Class	Maximum Output Power (Pmax)	Nominal Output Power	Minimum Output Power1	Power Control
1	100 mW (20 dBm)	N/A	1 mW (0 dBm)	Pmin<+4 dBm to Pmax Optional: Pmin2 to Pmax
2	2.5 mW (4 dBm)	1 mW (0 dBm)	0.25 mW (-6 dBm)	Optional: Pmin2 to Pmax
3	1 mW (0 dBm)	N/A	N/A	Optional: Pmin2 to Pmax

1. Minimum output power at maximum power setting.

2. The lower power limit Pmin<-30dBm is suggested but is not mandatory, and may be chosen according to application needs.

Ref: BLUETOOTH SPECIFICATION Version 5.0 | Vol 2, Part A page 326

Bluetooth Wireless Specs

- Uses frequency hopping, spread spectrum technique on 2.00-2.4835 GHz f=2402+k MHz, k=0,…,78
- Channels are 1 MHz apart, allowing for 79 channels in North America
- Channel bit rate is 1 Mb/s or greater
- Organizes data into packets and sends one packet per hop
- Packet length can be from 1 to 5 slots (1 slot = 625 microseconds)

Bluetooth Wireless Specs

- Intended to carry both audio and data transmission
- Audio is coded at 64 kb/s and can carry three streams in each direction
- Data applications can use 432 kb/s in each direction or 721 kb/s in one direction and 57.6 kb/s in the other
- Simple Bluetooth networks are called *piconets* and have between 2 and 8 nodes

Bluetooth Packet Format

- Two Modes:
  - Mandatory mode called Basic Rate: gross air data rate is 1 Mb/s
  - Optional mode called Enhanced Data Rate: has a primary modulation mode that provides a gross air data rate of 2 Mb/s and a secondary modulation mode that provides a gross air data rate of 3 Mb/s

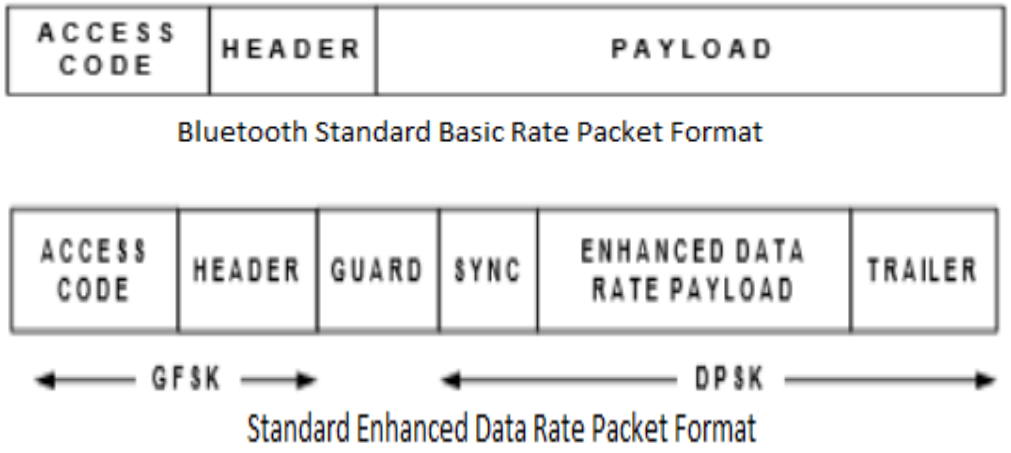


Figure 5: Bluetooth Packet Format

Source: Bluetooth Specification, (2016). Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Small Group Discussion

- Evaluate Bluetooth profiles and application features, Bluetooth security options, leveraging Bluetooth link authentication and encryption

Wireless Applications

- Specs developed by a consortium of Ericsson, IBM, Intel, Nokia and Toshiba
- Open standard for short range transmission
- (10 cm – 10 m) with RF amplifiers possibly 100 m, pico network (PAN)
- Idea was to make wireless devices small and inexpensive enough to be built into several types of equipment
  - Cellular and PCS phones, Notebooks, Personal Digital Assistants (PDA), printers, modems, speakers

Wireless Applications

- All nodes have identical capability, however initiating node acts as master for timing and control
- One device can operate on two piconets as a bridge
- Multiple piconets are called a *scatternet*

  http://www.bluetooth.com/Pages/How-It-Works.aspx

Wireless Applications

- Without Bluetooth, have to connect a computer to PSC phone for wireless using cable
- With Bluetooth transceivers, only necessary to have them in reasonable proximity
- Bluetooth standards resembles IEEE 802-11 Wireless Ethernet Standard

References

Bluetooth SIG, Inc. (2016). Specification of the Bluetooth System. Version 5.0. Retrieved Jul. 4, 2018 from https://www.bluetooth.com/specifications/bluetooth-core-specification

Gravitech. (n.d.). XBee ZB ZigBee Mesh Module 2.4GHz 2mW with Wire Antenna. Retrieved Jul. 3, 2018 from http://www.gravitech.us/xbzbmo22mwwa.html

PRISM Model Checker. (n.d.). IEEE 802.15.4 CSMA-CA Protocol (ZigBee). Retrieved Jul. 4, 2018 from http://www.prismmodelchecker.org/casestudies/zigbee.php

For more information, contact:
Director, Centre for Instructional Technology and Development
Southern Alberta Institute of Technology
1301 16 Ave. N.W., Calgary, AB T2M 0L4