2023 tech talks WEBINAR SERIES

# Welcome

## Enhancing Bluetooth® LE Advertising Range with Novel Bits

Arnold Kalvach & Mohammad Afaneh

BLUETOOTH SERIES

SILICON LABS

BLUETOOTH SERIES

# Presentation Will Begin Shortly

**BLUETOOTH SERIES SCHEDULE**

**NEW**

NOV 16TH | Enhancing Bluetooth LE Advertising Range with Novel Bits

**ON DEMAND**

OCT 26TH | Bluetooth App Development with CircuitPython

FEB 23RD | ML in Predictive Maintenance and Safety Applications

MAR 23RD | Unboxing: What's New With Bluetooth

APR 20TH | What's New with Bluetooth Mesh 1.1

MAY 18TH | Bluetooth Portfolio: What's Right for Your Application

JUN 15TH | The Latest in HADM With Bluetooth LE

**We will begin in:** 0:00

# BLUETOOTH SERIES

## BLUETOOTH SERIES SCHEDULE

### NEW

NOV 16TH | Enhancing Bluetooth LE Advertising Range with Novel Bits

### ON DEMAND

OCT 26TH | Bluetooth App Development with CircuitPython

FEB 23RD | ML in Predictive Maintenance and Safety Applications

MAR 23RD | Unboxing: What’s New With Bluetooth

APR 20TH | What’s New with Bluetooth Mesh 1.1

MAY 18TH | Bluetooth Portfolio: What’s Right for Your Application

JUN 15TH | The Latest in HADM With Bluetooth LE

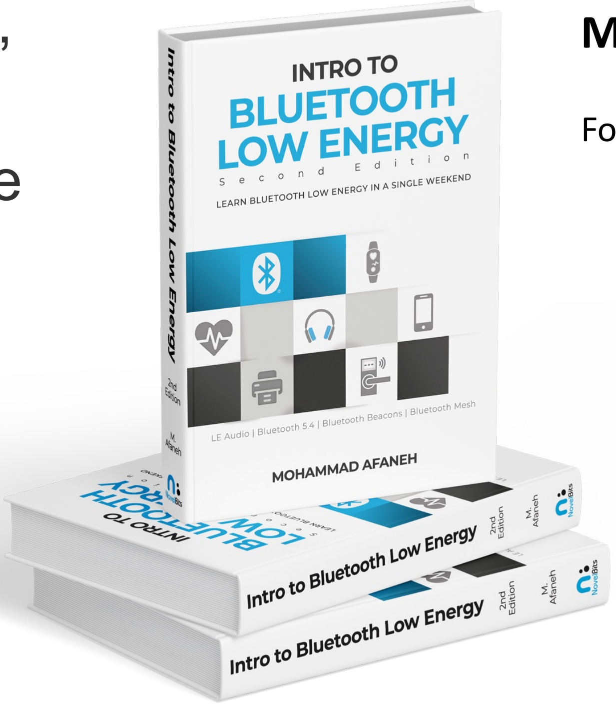
# About Me – *Arnold Kalvach*

- PhD in electrical engineering
- Embedded and firmware developer since 2011
- Supported 100s of Bluetooth LE developers during 6 years as an Application Engineer
- Bluetooth Product Manager at Silicon Labs since 2022

**Arnold Kalvach**
Bluetooth Product Manager
Silicon Labs

# About Me – *Mohammad Afaneh*

- Embedded developer since 2006
- Bluetooth LE embedded developer since 2014
- Founded Novel Bits in July 2015
- Focused on helping developers learn Bluetooth LE development via in-person training sessions, books, tutorials, video courses, and more
- Worked for and consulted for companies like the Bluetooth SIG, Motorola, Allegion, Stanley Security, Technicolor, and more
- Published three books on the topic of Bluetooth LE
- 2nd Edition of "Intro to Bluetooth Low Energy" published October 2023




**Mohammad Afaneh**
Bluetooth Developer
Founder @ Novel Bits, LLC
https://novelbits.io

NovelBits

SCAN ME

# Agenda

What's new with Bluetooth® 5.4

Scaling Bluetooth Networks with PAwR

Encrypted Broadcasting with EAD

Extend Your Range with Coded PHY

Summary and Q&A

# Bluetooth® 5.4

# Why Bluetooth 5.4?


- **Need for standardized large scale star networks**
  - Capability to host thousands of nodes
  - Encrypted data traffic
  - Ultra-low power consumption
  - Driven by electronic shelf label (ESL) market
- **Enhancements**
  - Optimizing access to secure data
  - Better control for LE Coded PHY for extended advertising

# Bluetooth 5.4 New Features

### Periodic Advertising with Responses (PAwR)

Provides energy efficient, large-scale, and bi-directional one-to-many communication topology

### Encrypted Advertising Data (EAD)

Feature to the secure broadcasting of data in advertising packets

### LE GATT Security Levels Characteristic

Devices can indicate the security mode and level required for all their GATT functionality to be available

### Advertising Coding Selection

The Host can specify which of two supported long range coding options are used with LE extended advertising

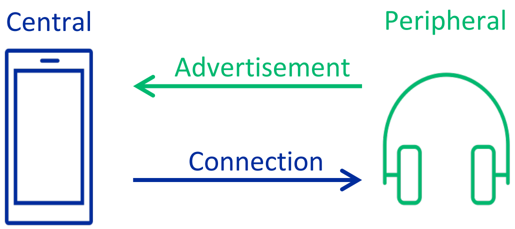
# Scaling Bluetooth Networks with PAwR

Arnold Kalvach

# Advertising Modes in Bluetooth 5.4

## Advertising for Connection

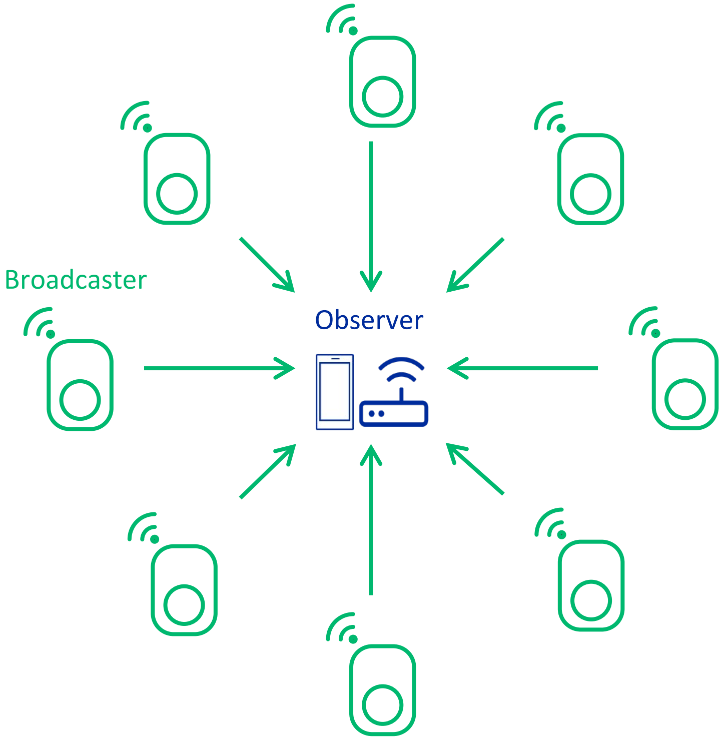
(irregular, unidirectional)




Max number of connections: **32**

## One-way “Beaconing”

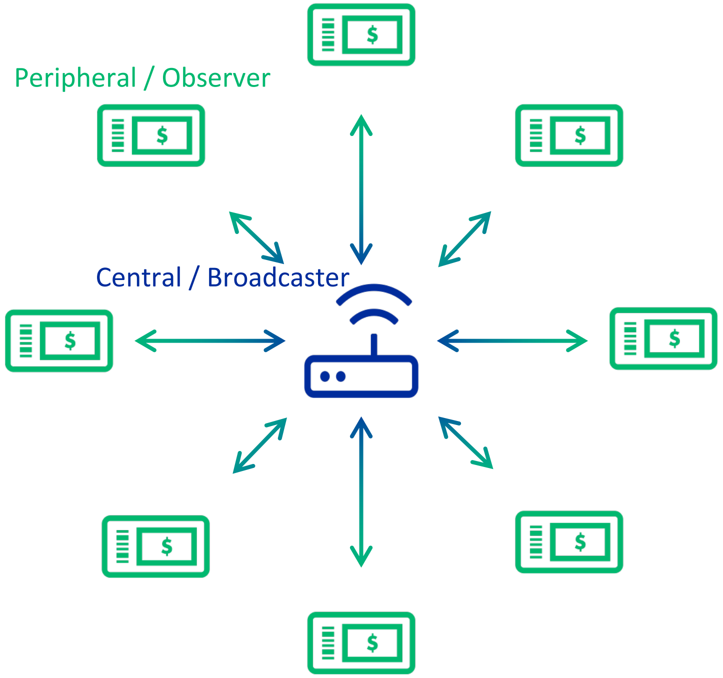
(regular, unidirectional)




Max number of beacons:
limited by channel capacity to a **few 1000s**
(unsynchronized nature causes collisions)

## Periodic Advertising with Responses

(regular, bidirectional)




Max number of Peripherals: **32,767**
New mode enabling “Synchronized” mode network.

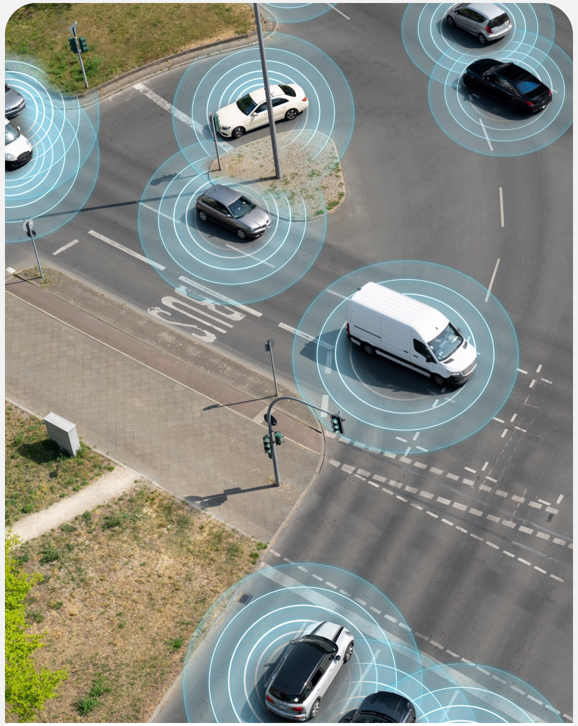
# Applications beyond ESL

ASSET MANAGEMENT

Status updates from a huge number of items, location finding

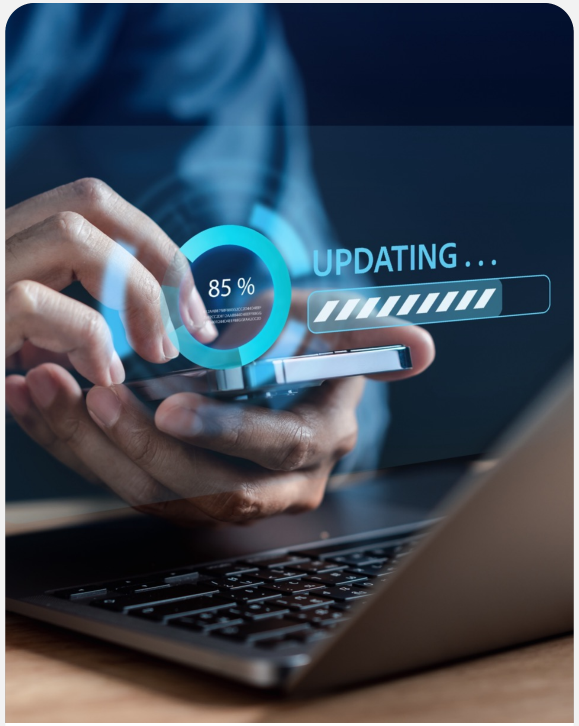
SMART CITIES

Access Points to connect to more than 32 Bluetooth devices nearby



AUTOMOTIVE

Non safety critical electronics to communicate with the central computer



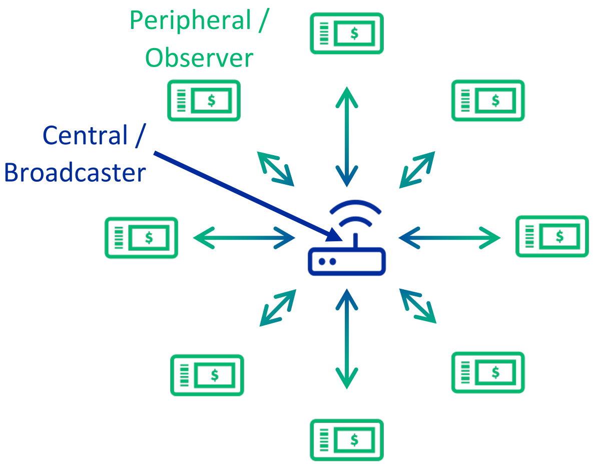

FIRMWARE UPDATES

Updating multiple devices at once (with ACK)

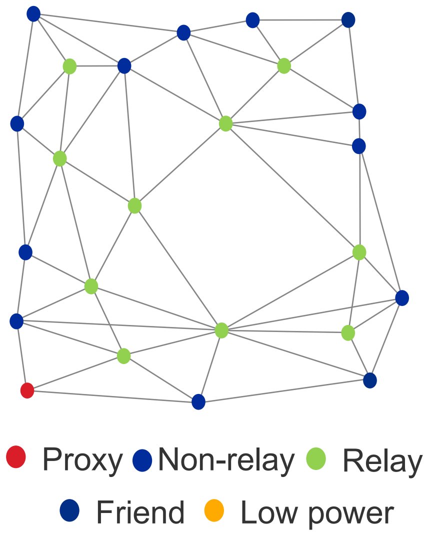
# PAwR vs Bluetooth Mesh

## Periodic Advertising with Responses




10,000s of nodes
Centralized
Synchronized
Low power nodes
Non-standard application
Long range with Coded PHY
Low throughput (except when broadcasting)

## Bluetooth Mesh



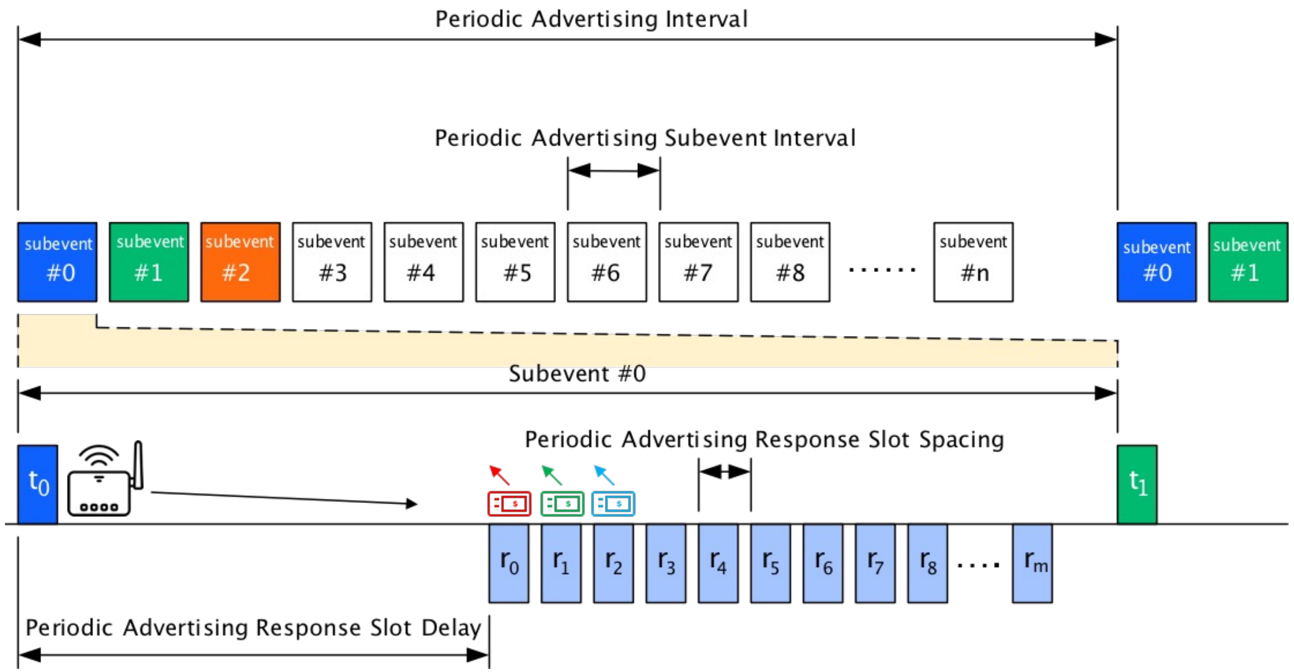

1000s of nodes
Decentralized
Unsynchronized
High power nodes (mostly)
Standardized application
Long range by relaying
Low throughput (except when broadcasting)

# Periodic Advertisement with Responses (PAwR) Explained

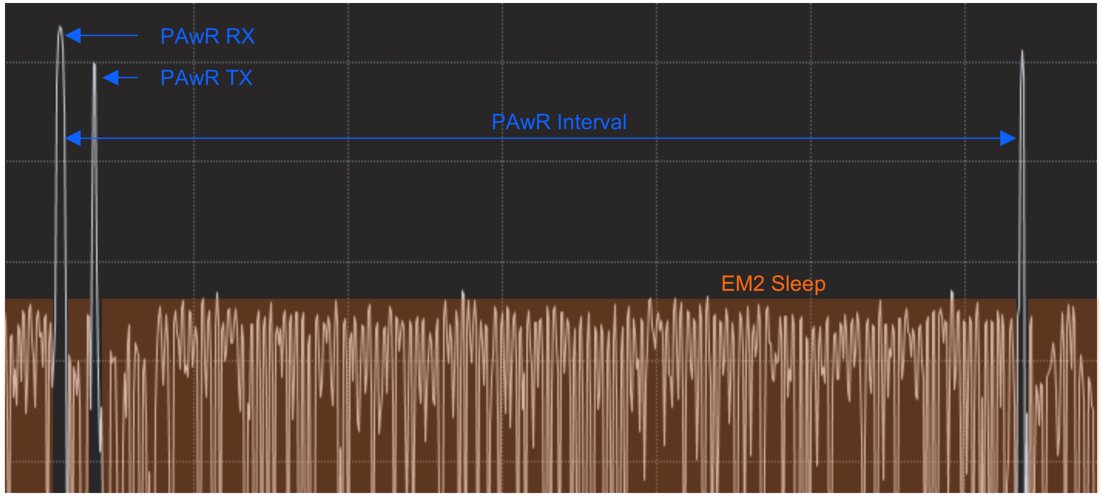
- **PAwR train setup**
  - Sets timing parameters
  - Configure number of Subevents and Response Slots

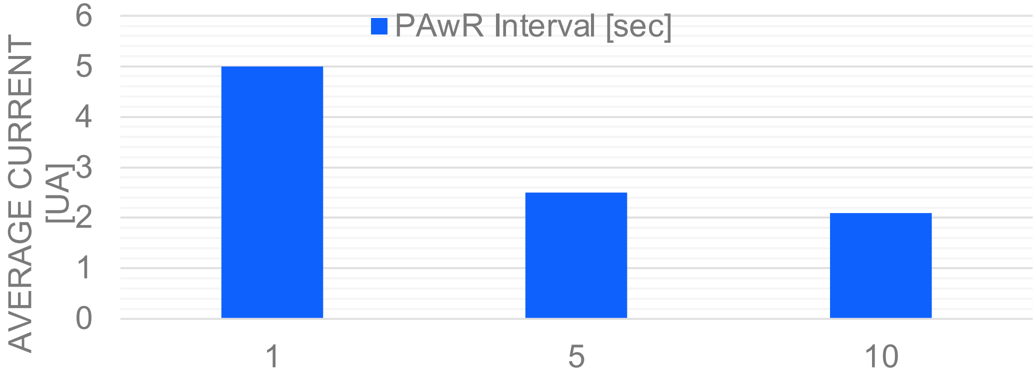
- **Subevents**
  - Each Peripheral belongs to one Subevent
  - Maximum 128 Subevents
  - Maximum 255 Peripherals in one Subevent (group)
  - Total max 32,640 Peripherals in the network

- **Inside a Subevent**
  - All Peripherals in one Subevent receive the Central Device transmission (downlink)
    - Keeps up the synchronization to the PAwR train
    - Transmits downlink payload data
  - A given number of Peripherals can respond in dynamically allocated response slots (uplink)



# Example of PAwR Current Consumption




- **Peripheral device use case**
  - Receives Central Device downlink transmission at given Subevent time slot
  - Responses uplink at given Response Slot
  - Remains in sleep mode rest of time
- **Measurement condition**
  - MG22 Radio Board
  - Vinput 3.0V, DC/DC in use
  - SoC Current only
  - TX 0dBm
  - LFXO accuracy 50ppm

# Encrypted Broadcasting with EAD

Arnold Kalvach

# Bluetooth Security

- **Bluetooth Connections**
  - Encryption with ECDH
  - Authentication with passkey / OOB data
  - Re-authentication with stored LTK (pairing/bonding)

- **Bluetooth Mesh Network**
  - Network key, IV secures the whole network
  - Application key secures a group of devices
  - Device key for device-to-device security

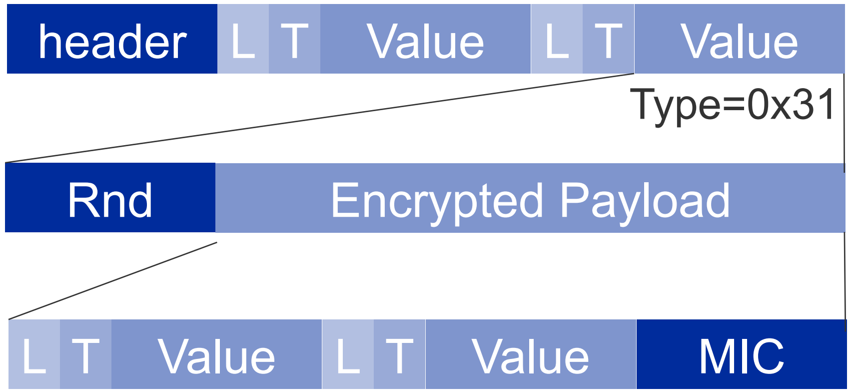
- **Broadcasting (Advertisements)**
  - Only application layer security

**Encrypted Advertisement Benefits**

- Enables full privacy along with Private Addresses
  - device cannot be tracked based on their address nor based on their advertisement data
- Enables encrypted data exchange over PAwR and other broadcasting mechanisms (beacons, periodic advertisements)
  - Closed network of advertisers
- Enables super low power secure communication
  - For ex., an energy harvesting lamp switch shall only send out a single advertisement, and it can still securely control the lamp

# Encrypted Advertising Data (EAD)

- **Standardized Encryption for Broadcasting**
  - Can be applied in any type of advertisement
  - Re-uses cryptographic methods used in connection encryption
- **Advertisement Payload Format**
  - Length – Type – Value triplets
  - Type = 0x31 means EAD




- **Encryption method**
  - Payload encrypted with ***CCM method*** (same as on connections) using ***Rnd field, Session key*** and ***IV***
- **Key Exchange**
  - Session key and IV must be exchanged
  - May be exchanged
    - Over encrypted connection using Encrypted Data Key Material characteristic
    - Out-of-band
    - Using ECDH over PAwR (non-standard)
    - Via other non-standard methods

# Software Support

**Transmitter:**

sl_bt_ead_session_init()

- Initializes session with a given Key and IV

sl_bt_ead_randomizer_set()

- Sets random data field

sl_bt_ead_randomizer_update()

- Updates random data field

sl_bt_ead_encrypt()

- Encrypts advertisement data

sl_bt_ead_pack_ad_data()

- Formats advertisement data

**Receiver:**

sl_bt_ead_session_init()

- Initializes session with a given Key and IV

sl_bt_ead_unpack_ad_data()

- Parses advertisement data

sl_bt_ead_decrypt()

- Decrypts advertisement data

sl_bt_ead_unpack_decrypt()

- Parses and decrypts advertisement data

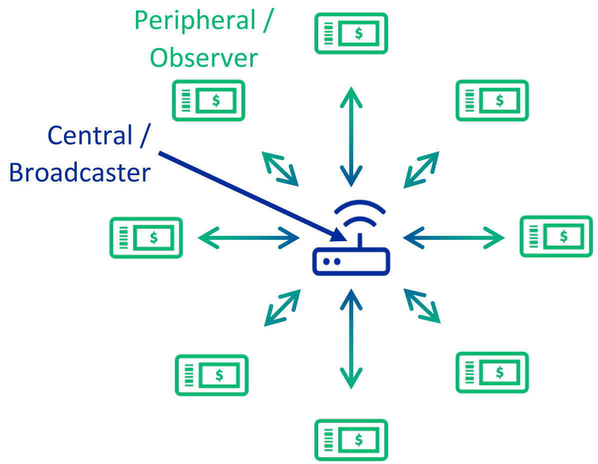
# Extend Your Range with Coded PHY

Mohammad Afaneh

# PAwR vs Bluetooth Mesh

## Periodic Advertising with Responses




10,000s of nodes

Centralized

Synchronized

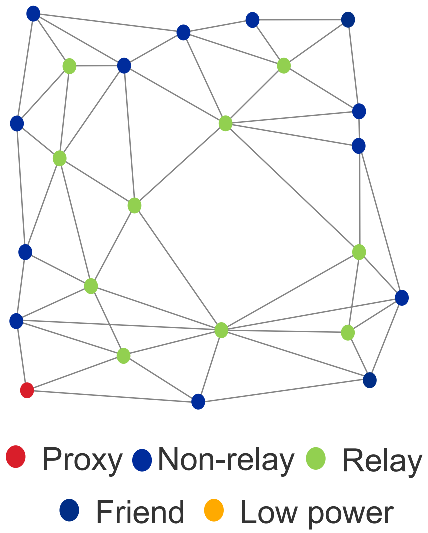
**Low power nodes**

Non-standard application

**Long range with Coded PHY**

Low throughput (except when broadcasting)

## Bluetooth Mesh




1000s of nodes

Decentralized

Unsynchronized

High power nodes (mostly)

Standardized application

Long range by relaying

Low throughput (except when broadcasting)

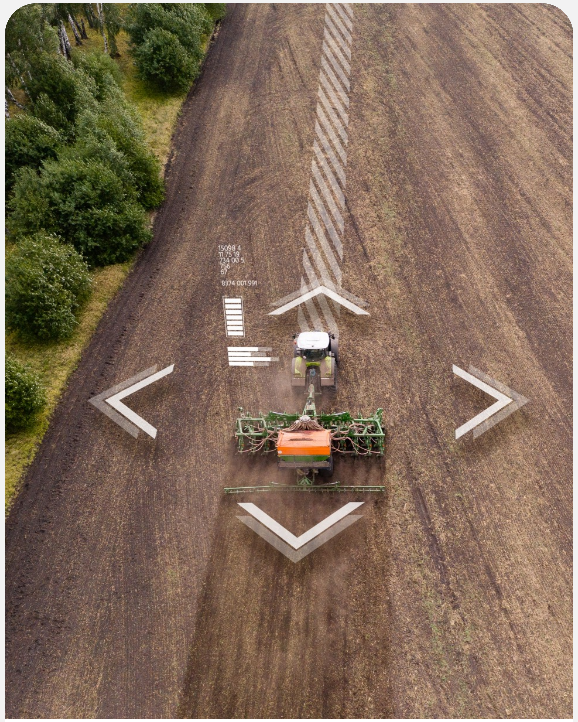
# Coded PHY + PAwR Example Applications

SMART RETAIL

Large-scale, long-range ESL and inventory management systems

INDUSTRIAL

Monitoring sensors and controlling actuators spread across extensive facilities



AGRICULTURE

Monitoring and control of agricultural equipment and sensors spread across large farmlands

EVENT MANAGEMENT

Crowd monitoring, emergency response coordination, and asset tracking across concerts or sporting events

# What is Coded PHY?

- **Introduced in Bluetooth Core Spec v5.0**
  - New LE PHY (optional)
  - Achieves up to 4x range of LE 1M PHY
  - Without the need to increase the TX Power
- **How?**
  - By utilizing Forward Error Correction (FEC)
  - Introduces data redundancy in transmitted data
  - Allows error correction in addition to error detection
- **Two Coding Schemes**
  - The coding scheme defines the # of symbols/data bit
    - S=2, uses 2 symbols to represent each data bit
    - S=8, uses 8 symbols to represent each data bit
  - The data throughput depends on the coding scheme used:
    - S=2 leads to 500 kbps data rate
    - S=8 leads to 125 kbps data rate

Comparison of LE PHYs

| PHY / Parameter | 1M PHY | 2M PHY | Coded PHY S=2 | Coded PHY S=8 |
|---|---|---|---|---|
| Symbol Rate | 1 Ms/s | 2 Ms/s | 1 Ms/s | 1 Ms/s |
| Data Rate | 1 Mbps | 2 Mbps | 500 kpbs | 125 kbps |
| Max App Data Rate | 700 kbps | 1400 kbps | 400 kbps | 100 kbps |
| Error Detection | CRC | CRC | CRC | CRC |
| Error Correction | None | None | FEC | FEC |
| Range Multiplier | 1 | 0.8 | 2 | 4 |
| Requirement | Mandatory | Optional | Optional | Optional |
| Rx Sensitivity (dBm) | ≤ -70 | ≤ -70 | ≤ -75 | ≤ -82 |

# Advantages and Disadvantages of Coded PHY

- **Long Range Communication** +
  - Up to 4x the range of 1M PHY
  - Does not require higher TX power
  - Ranges of over 1km line-of-sight!

- **Limited Smartphone Support** −
  - Most LE applications rely on smartphones
  - Coded PHY support is very limited in smartphones
  - Smartphones need to support Coded PHY for both extended advertising and connections for full utilization of its capabilities

- **Great for SoC-based Systems** +
  - Wide support for Coded PHY in Bluetooth SoCs
  - Supported by all Silicon Labs Bluetooth SoCs
  - Great for systems that utilize embedded systems on both ends

- **Not Just for Long Range** +

  Coded PHY can also help in the following scenarios:
  - Noisy RF environments
  - Increased reliability in the presence of physical obstacles

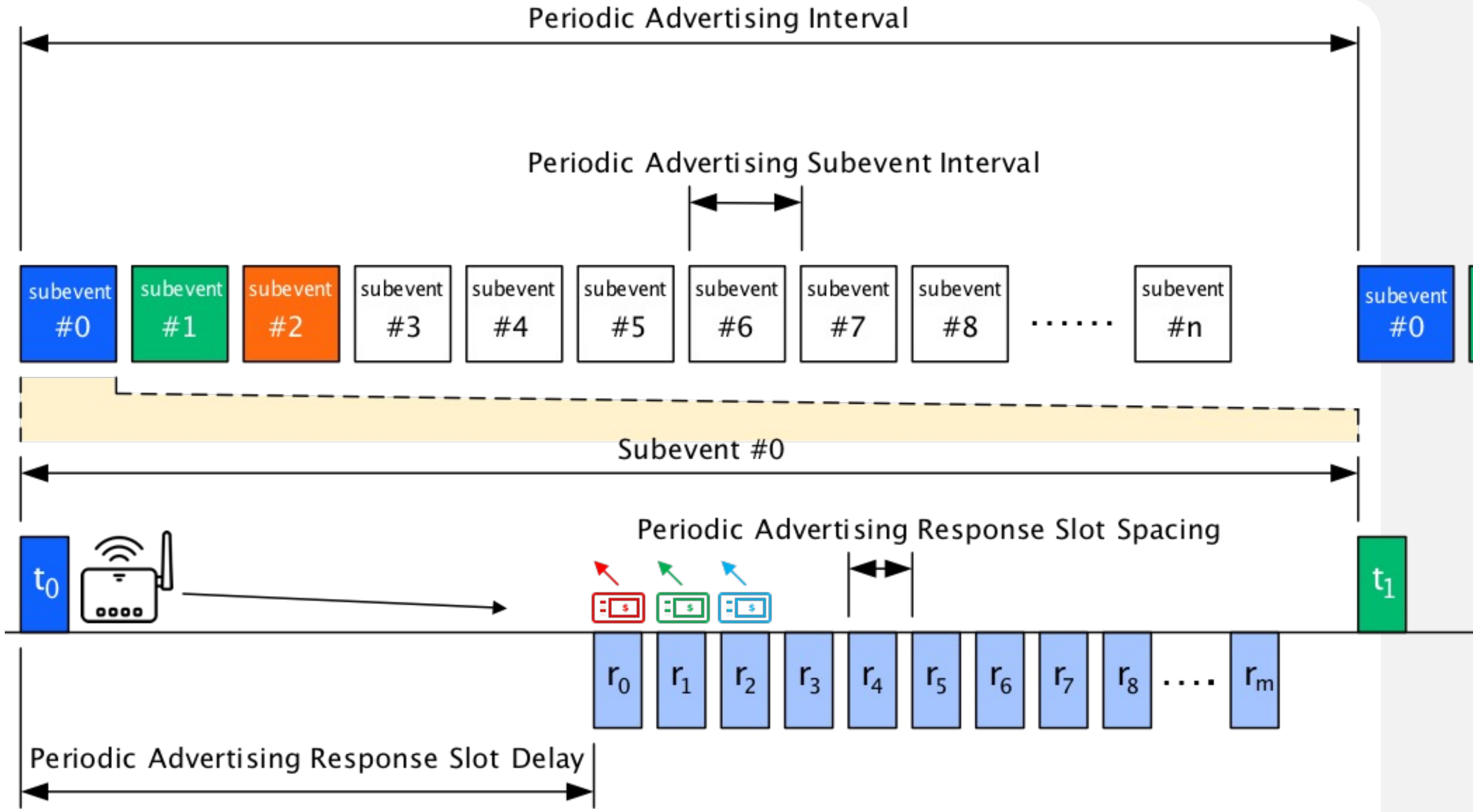
- **Lower Data Throughput** −

  Coded PHY will reduce the data throughput:
  - S=2, reduced to 500 kbps
  - S=8, reduced to 125 kbps

- **Higher Power Consumption** −
  - Due to the increased radio-on time
  - Especially compared to 1M or 2M PHY

# Coded PHY and PAwR – Design Parameters

- **Important Parameters**
  - **Periodic Adv Interval**: 7.5 ms to 81.91875 sec
  - **Number of Subevents (n)**: 1 to 128
  - **Subevent Interval**: 7.5 ms to 318.75 ms
  - **Number of responses (m)**: 0 to 255
  - **Response Slot Delay**: 1.25 ms to 317.5 ms
  - **Response Slot Spacing**: 0.25 ms to 31.875 ms



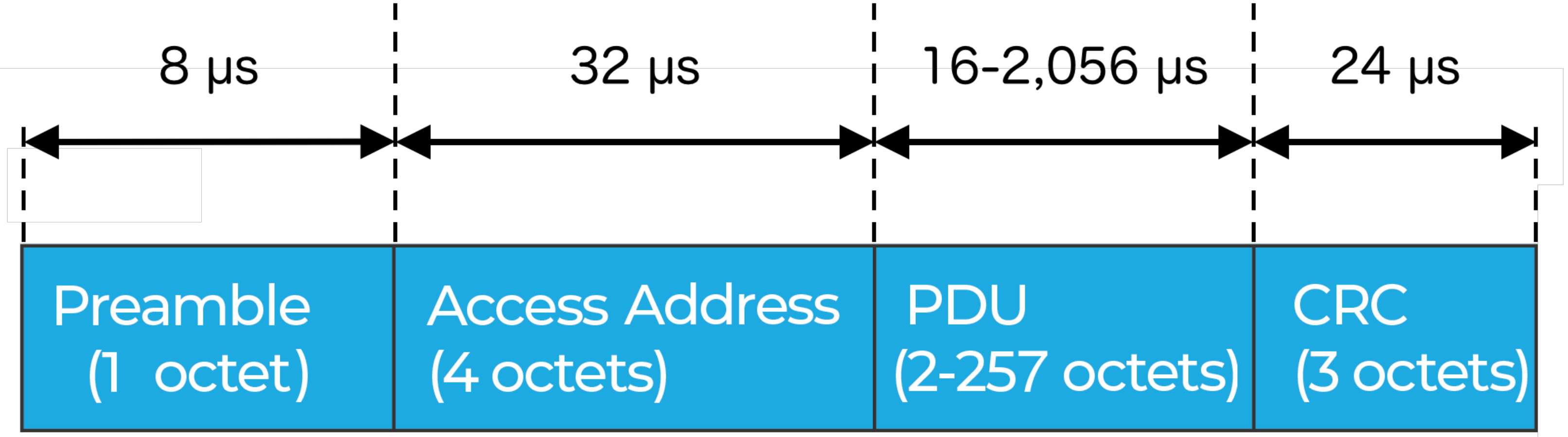

$$Periodic\ Advertising\ Interval > \#\ of\ SubEvents\ *\ Subevent\ Interval$$

$$SubeventInterval > Response\ Slot\ Delay + (\#\ of\ response\ slots\ *\ Response\ Slot\ Spacing)$$

$$Response\ Slot\ Delay > Amount\ of\ time\ needed\ to\ transmit\ a\ transmit\ packet$$

$$Response\ Slot\ Spacing > Amount\ of\ time\ needed\ to\ transmit\ a\ response\ packet$$

# Uncoded 1M PHY Advertising Packet Format and Duration

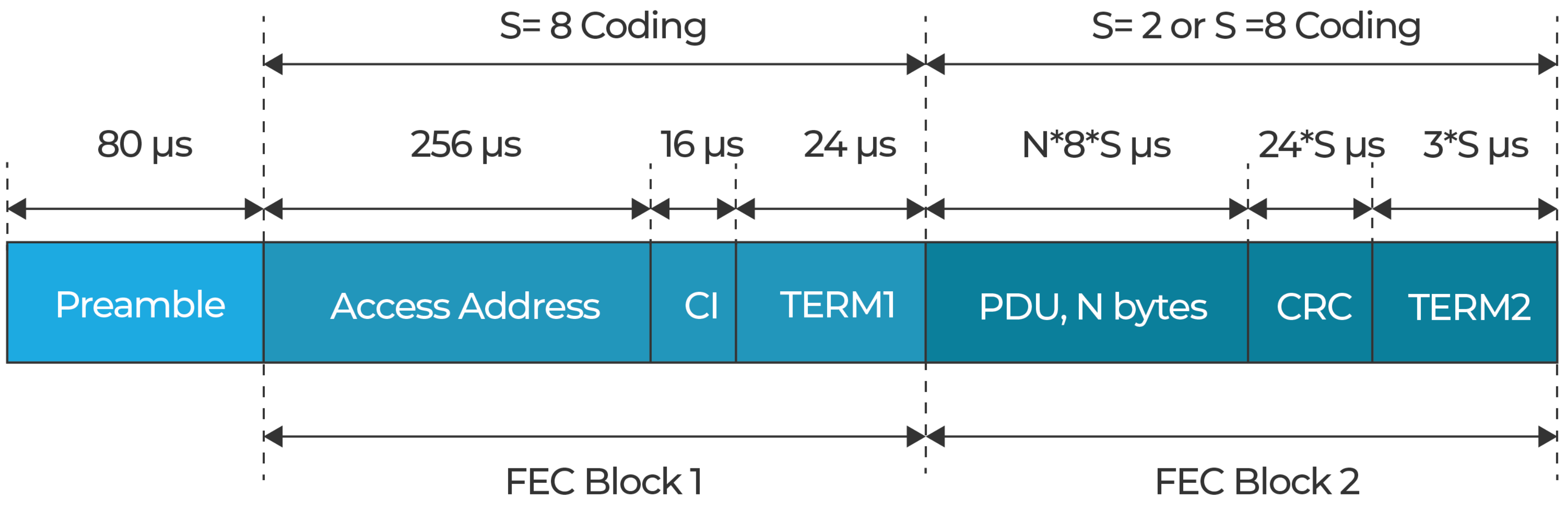



LE 1M (Uncoded) PHY Advertising Packet Format and Transmit Timing

Data rate = 1 Mega symbols / second = 1 Mbps

***Total Packet Time Required > 80 µs***

# Coded PHY Advertising Packet Format and Duration




LE Coded PHY Advertising Packet Format and Transmit Timing
Data rate = 1 Mega symbols / second

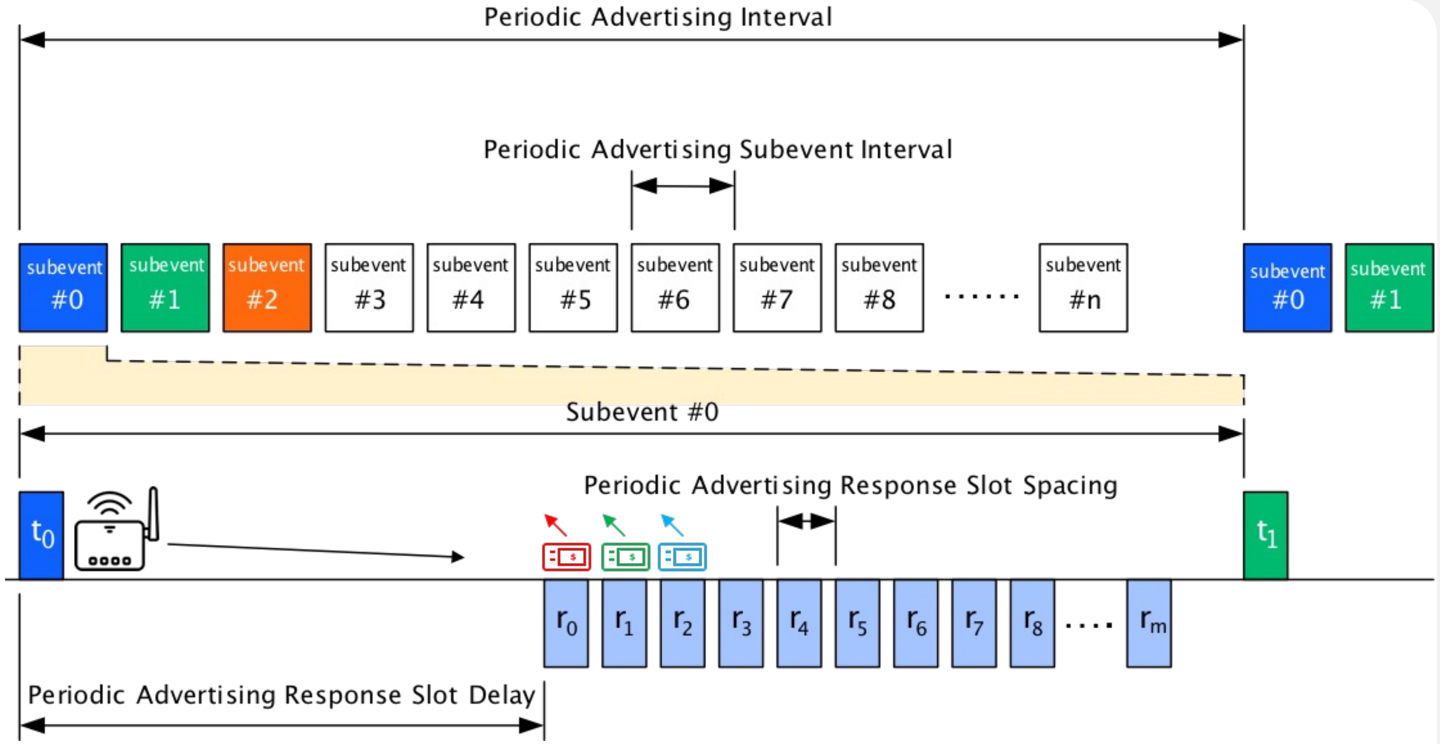
S = 2 → data rate = 500 kbps
S = 8 → data rate = 125 kbps

$\mathit{Total\ Packet\ Time\ Required} > 462\ \mu s$, for S=2
$\mathit{Total\ Packet\ Time\ Required} > 720\ \mu s$, for S=8

# Coded PHY and PAwR – Design Parameters

## Important Considerations

- Coded PHY takes much longer to transmit the same data compared to 1M PHY
- This applies to both:
  - Transmit packets ($t_0$, $t_1$, …, $t_n$)
  - Response packets ($r_0$, $r_1$, …, $r_m$)




$$\textit{Periodic Advertising Interval} > \textit{\# of SubEvents} * \textit{Subevent Interval}$$

$$\textit{SubeventInterval} > \textit{Response Slot Delay} + (\textit{\# of response slots} * \textit{Response Slot Spacing})$$

$$\textit{Response Slot Delay} > \textit{Amount of time needed to transmit a transmit packet}$$

$$\textit{Response Slot Spacing} > \textit{Amount of time needed to transmit a response packet}$$


Nov 14, 2023 at 5:07:57 PM
#4
#3
#2
#1
3.0

# Coded PHY and PAwR – Recap

- Coded PHY can be beneficial for:
  - Long-range applications
  - More robust communication
  - Or both
- PAwR provides a solution for:
  - Large-scale systems
  - Synchronized applications
  - Centralized systems (star topology)
  - Low power applications
- Utilizing Periodic Advertising with Responses (PAwR) with Coded PHY requires careful consideration in the design of the timing parameters

# Q&A

BLUETOOTH SERIES

SILICON LABS

2023 tech talks
WEBINAR SERIES

# Thank You

BLUETOOTH SERIES

Watch ON DEMAND