Bluetooth® Seminar Series

Tools, Techniques, and Trends

Best Practices for Bluetooth LE Product Design

Sandeep Kamath | Founder and Principal Engineer | SwaraLink Technologies

Introduction

Common Issues with Bluetooth Low Energy Products:

Reliability

Power

Security

User Experience

Reasons that these issues occur:

Complexity of Specification

Limited Features Supported in Stacks

Confusing Marketing of Features

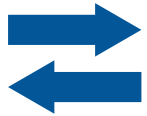
Limited Examples in SDKs

I read that my BLE product should last for years on a single coin cell battery… so how come it dies after just 2 weeks?

Use appropriate connection parameters & advertising parameters

The choices of these parameters will have the largest impact on the performance of your device:


Power


Throughput


Latency

Bad products: Use default parameters, which are not necessarily appropriate for the application

Good products: Set parameters to optimal values

Better products: Dynamically update connection parameters

Connection Parameter Tradeoffs – Cheat Sheet

Low		High	
Slave Power Consumption:	Increases	Slave Power Consumption:	Decreases
Master Power Consumption:	Increases	Master Power Consumption:	Decreases
Data Throughput:	Increases	Data Throughput:	Decreases
Slave-to-Master Data Latency:	Decreases	Slave-to-Master Data Latency:	Increases
Master-to-Slave Data Latency:	Decreases	Master-to-Slave Data Latency:	Increases

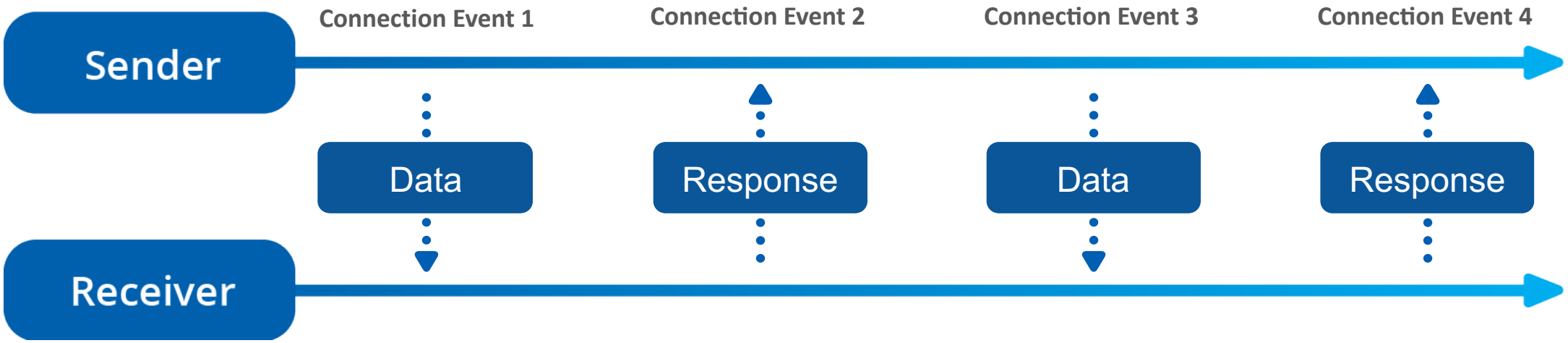
Low / Zero		High	
Slave Power Consumption:	Increases	Slave Power Consumption:	Decreases
Master Power Consumption:	No Impact	Master Power Consumption:	No Impact
Data Throughput:	No Impact	Data Throughput:	No Impact
Slave-to-Master Data Latency:	No Impact	Slave-to-Master Data Latency:	No Impact
Master-to-Slave Data Latency:	Decreases	Master-to-Slave Data Latency:	Increases

Isn't the throughput in BLE 2Mbps? I'm not getting anything close to that…

Optimize data throughput

- 2Mbps is the maximum PHY data rate
- Application layer throughout is significantly less, and can vary greatly based on many factors
- Certain procedures have protocol overhead that significantly reduces throughput
- Optimal packets to use to maximize throughput:
  - Notifications
  - Write Command (Write Without Response)
- All packets are acknowledged, regardless of the procedure used

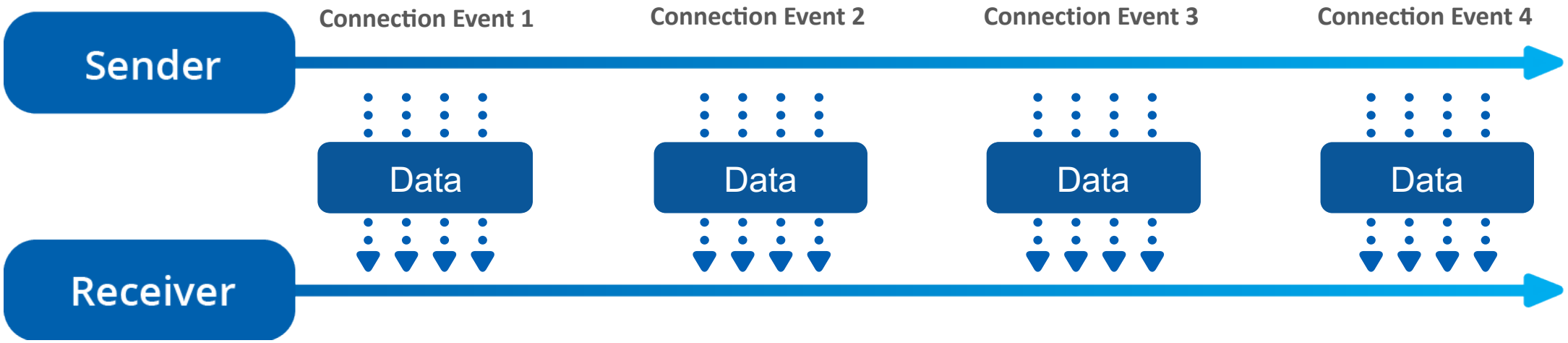
Write Requests or Indications



Optimize data throughput

- 2Mbps is the maximum PHY data rate
- Application layer throughout is significantly less, and can vary greatly based on many factors
- Certain procedures have protocol overhead that significantly reduces throughput
- Optimal packets to use to maximize throughput:
  - Notifications
  - Write Command (Write Without Response)
- All packets are acknowledged, regardless of the procedure used

Write Without Response or Notifications



Use a Large PDU length and ATT_MTU value

- Max packet length with **Bluetooth 4.0 and 4.1**: 27-bytes

- Max packet length with **Bluetooth 4.2 and 5.x**: 251-bytes

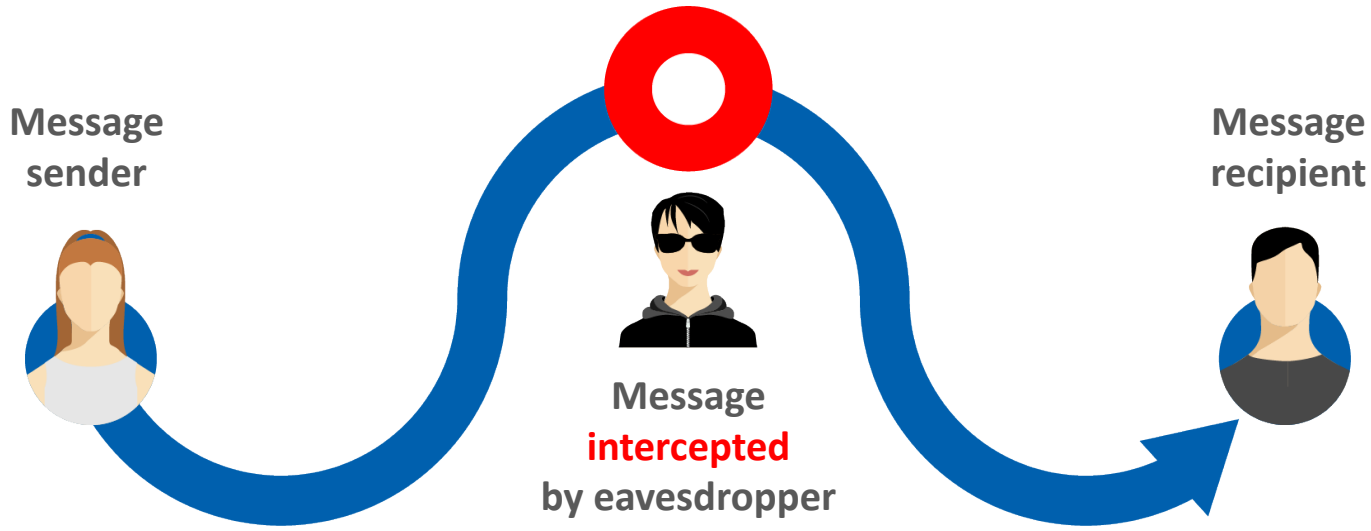
- Optimal settings:
  - Link Layer max PDU length: 251-bytes
  - ATT_MTU size: 247-bytes
- Note: actual PDU length and ATT_MTU size are not guaranteed, so application should be able to handle any legal values up to configured maximum.

Is Bluetooth secure?

Use the LE Secure Connections Feature

With BLE, there are two options for pairing

- 1: **LE Legacy Pairing:**
  - Original method for pairing in BLE and was the only option with Bluetooth 4.0 and 4.1.
  - Has a known security vulnerability during the pairing process



Use the LE Secure Connections Feature

With BLE, there are two options for pairing

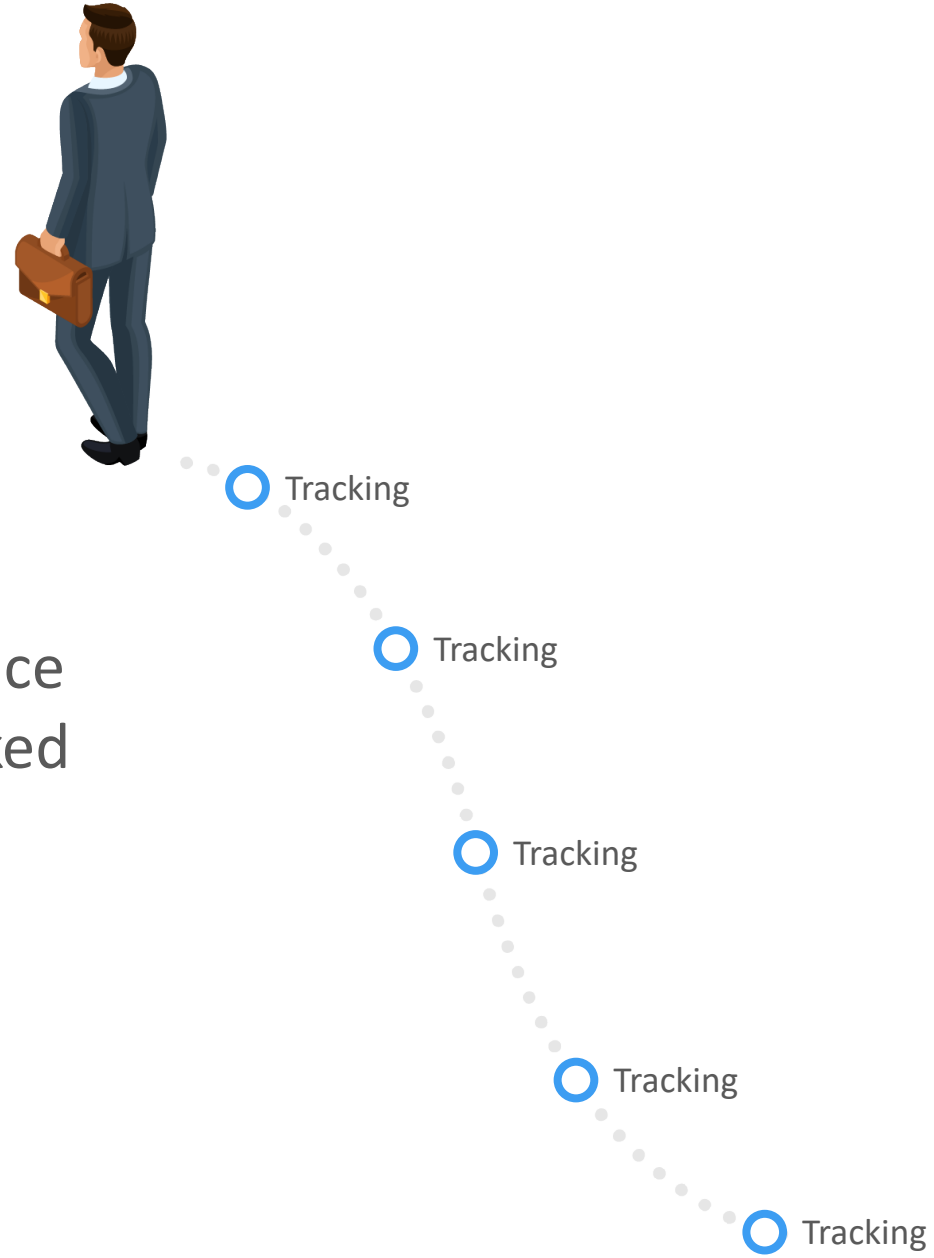
- 1: **LE Legacy Pairing:**
  - Original method for pairing in BLE and was the only option with Bluetooth 4.0 and 4.1.
  - Has a known security vulnerability during the pairing process
- 2: **LE Secure Connections:**
  - Introduced in Bluetooth 4.2 with improvements in Bluetooth 5.x.
  - Based on the Elliptic Curve Diffie-Hellman (ECDH) Key Exchange algorithm for secure key exchange

Prevent Unauthorized Connections

- What can a malicious device do by establishing a BLE connection?
  - Denial of service
  - Cause increased power consumption
  - Increase attack surface
- Whitelist filtering:
  - Allows a BLE device to restrict connections to authorized peer devices only
  - Incoming connection requests from devices that are not on the whitelist are ignored
  - Ideal for applications with one-to-one pairing

Protect User Privacy

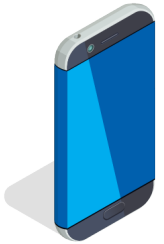
- **Did you know?**
  - Bluetooth-enabled nodes are everywhere: airports, shopping centers, and even on city streetlights
- The privacy feature protects a Bluetooth device (and its user) from having their location tracked
- **How it works:**
  - Bluetooth device advertises using a random, periodically changing address rather than a fixed address
  - Only trusted peers can decode this using an Identity Resolving Key (IRK)



Future-Proof Your Product by Supporting Firmware Updates

- Several types of security vulnerabilities:
  - Application-layer code
  - Bluetooth stack code (typically from device manufacturer or open source)
  - Bluetooth specifications
- Support over-the-air firmware updates to patch vulnerabilities in the future
- Best practices:
  - Use authenticating bootloader and sign firmware images
  - Encrypt firmware images to protect against reverse-engineering

Latest firmware package pushed to app



Over-the-air firmware update via Bluetooth

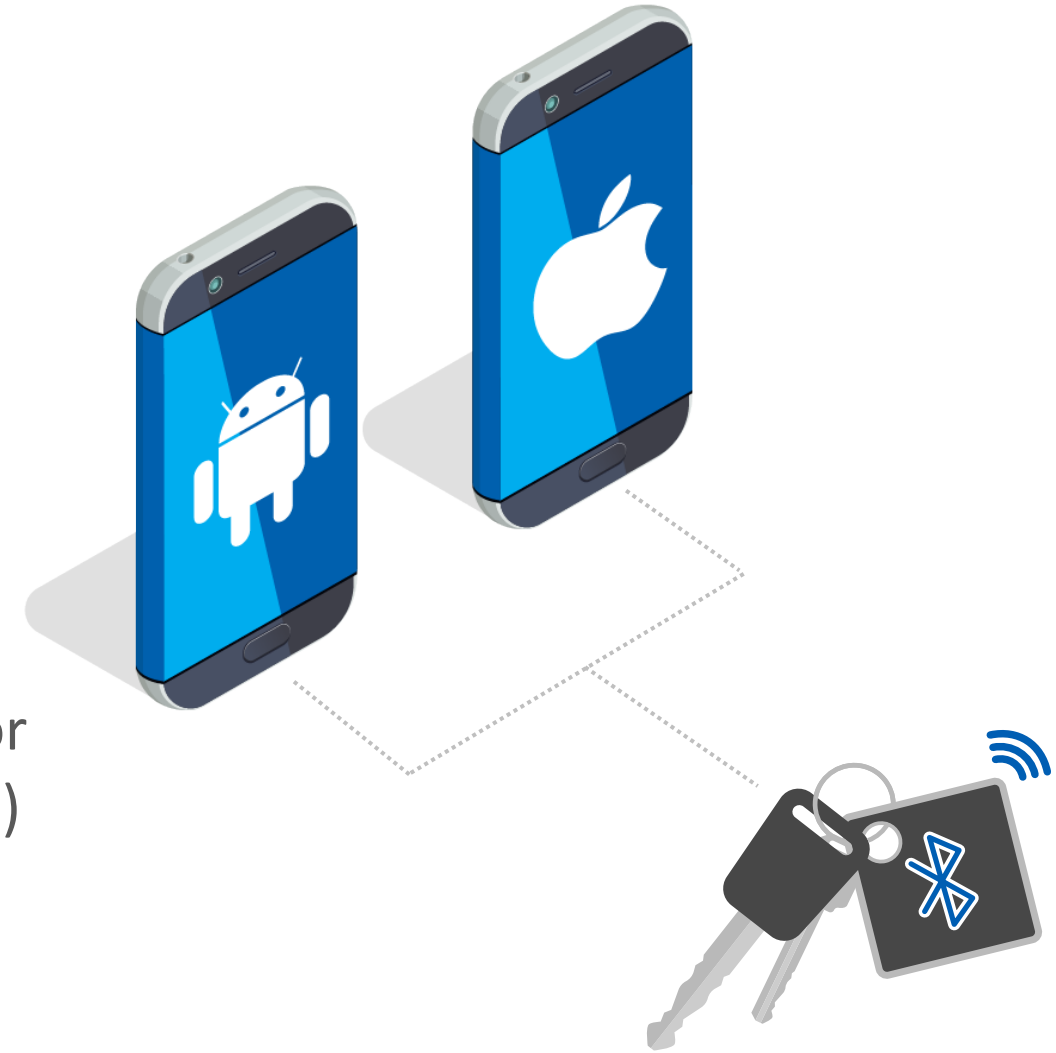
“My device won’t pair with my phone”

. . .

“The connection seems unreliable…”

Ensure Interoperability

- Even though all devices follow the Bluetooth core specification, exact behavior and feature support can vary
  - **iOS:** Follow Apple's "Accessory Design Guidelines" document
  - **Android:** Sometimes inconsistent behavior (especially older versions or older devices)
- Consider requiring a minimum operating system version



Use Appropriate UUIDs

- Every service and characteristic referenced via a UUID (Universally Unique Identifier)
- Version 4 (random) 128-bit UUIDs:
  - Simple, safe, and free way to create UUIDs
  - No registration with any central database required
  - Statistically improbable odds of collision
- Consider purchasing a 16-bit UUID from the Bluetooth SIG for your service UUID:
  - Reduce the size of the advertising or scan response data and therefore reduce your overall power consumption
  - Reduce service / characteristic discovery times

Additional Information

BLE Developer's Checklist PDF – free download:

www.blechecklist.com

About SwaraLink Technologies:

www.swaralink.com

SWARALINK TECHNOLOGIES

Embedded Bluetooth Low Energy Experts

Thank you!

Questions?

Contact Information

Name: Sandeep Kamath
Email: info@swaralink.com
Web: www.swaralink.com