Bluetooth HADM: Perfecting Location-Centric Services.

Priyanka Sukumar | August 22nd, 2023
High Accuracy Distance Measurement
HADM – Beyond RSSI

- **Accuracy & Reliability**: RSSI is sensitive to indoor multipath environment.
- **Simplicity**: Enable design of low-cost devices
  - Single antenna design
  - Reduce system resources
- **Security**: Attacker manipulation of RSSI via RF signal amplification
- **Interoperability**: Standards Based Feature
HADM – Target Applications

**PROXIMITY AWARENESS**
- Door locks
- Keyless entry
- Building access systems
- Geofencing - security alerts

**LOCALIZATION**
- Indoor asset management – hospitals, warehouses
- Pet tracking inside homes
- Item finding - wallet, keys, tools
Range Estimation Techniques

Draft Specifications publicly available at:
www.bluetooth.com/specifications/specs/channel-sounding/
Phase-Based Ranging (PBR)

- Tone exchange between two devices
- Phase of RF signals is a function of the frequency of the carrier and the distance traveled
  - Phase rotation due to spatial propagation determined
  - Measurements at multiple RF frequencies to resolve distance ambiguity
- Distance is calculated using the phase difference between the transmitted and received signal
- Security
  - Manipulation of phase is more complex than RSSI
  - Higher accuracy than RSSI
Round Trip Timing (RTT)

- Packet transmission time (ToF) is measured on both the initiator and reflector side using Time-of-Arrival (ToA) and Time-of-Departure (ToD)
  - Modulated packets exchanged over multiple channels to determine ToF and estimate distance
  - Fractional timing techniques used to resolve sampling uncertainty and improve resolution
- Time cannot be reversed -> RTT increases security
- PBR is more accurate than RTT

\[ RTT = 2 \, \text{ToF} = (\text{ToA}_I - \text{ToD}_I) - (\text{ToD}_R - \text{ToA}_R) \]
Connection-based 2-way ranging with encrypted Bluetooth LE connection events and secure CS events
- Reflector exposes received signal info via GATT service.
- Interchangeable device roles (central, peripheral) and CS roles (initiator, reflector)
- Initiator configures CS procedure parameters
  - Number of channels, channel map(randomized), TX power
  - Allowed duration of connection interval, CS event
  - Measurement modes – PBR, RTT
  - Trade-offs between accuracy, duration, power, number of channels

CS Event
- Calibration – frequency offset
- Modulated packets or tones exchanged over multiple channels
- Channel mapping is randomized to prevent attackers

Distance Estimation
- Initiator parses the measured data - IQ samples, time
- Signal processing – averaging, filtering outliers, detecting multipath, etc

Establish LE connection
Encrypt connection
Configure CS procedure parameters

Connection Event
Data Channel PDU

CS Event
Step 0
Step n

Connection Event
Data Channel PDU
Performance in Indoor Office Environment

- **Ceiling rail infrastructure**
  - Internal test environment
  - Multiple stationary EFR32 devices placed at different locations
  - Mobile EFR32 device for controlled measurements (repeatability)

- **Challenges - heavy multi-path in an indoor office setting**

- **Statistical analysis**
  - Static measurements at multiple distances up to 30 meters
  - Hundreds of measurements per distance to determine min/max, mean, median, std, absolute error
Indoor Performance Result – PBR

![Graph showing PBR Distance Estimation]

- Median absolute error (m)
- Distance (m)
## Power Consumption – HADM vs UWB

<table>
<thead>
<tr>
<th></th>
<th>PBR</th>
<th>Time (ms)</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sleep</td>
<td>71.80</td>
<td>4.16 uA</td>
<td></td>
</tr>
<tr>
<td>Measurement</td>
<td>27.60</td>
<td>4.74 mA</td>
<td></td>
</tr>
</tbody>
</table>

Average power consumption over 100 ms = 1.31 mA

<table>
<thead>
<tr>
<th></th>
<th>UWB</th>
<th>Time (ms)</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sleep</td>
<td>89.89</td>
<td>24 uA</td>
<td></td>
</tr>
<tr>
<td>Measurement</td>
<td>10.11</td>
<td>26.03 mA</td>
<td></td>
</tr>
</tbody>
</table>

Average power consumption over 100 ms = 2.68 mA
Silicon Labs Offerings
BG24 and BGM241S: 2.4 GHz SoC Ideal for Bluetooth Location Services

SOCS AND MODULES

BG24 SoC

BGM241S SiP Module

SOC DEVICE SPECIFICATIONS

High-Performance Radio
- Up to +19.5 dBm TX
- -97.6 dBm RX @ BLE 1 Mbps

Efficient ARM® Cortex®-M33
- 78 MHz
- 1536kB Flash, 256kB RAM

Low Power
- 33.4 µA/MHz
- 5.0 mA TX @ 0 dBm
- 5.1 mA RX (802.15.4)
- 4.4 mA RX (BLE 1 Mbps)
- 1.3 µA EM2 sleep

Multiple protocol support
- Bluetooth (1M/2M/LR)
- Bluetooth mesh
- Proprietary 2.4 GHz

SoCs and Modules
- 5x5 QFN40
- 6x6 QFN48
- 7x7 SiP Module
- 12.9x15.0 PCB Module

DIFFERENTIATED FEATURES

+20 dBm output power
- Eliminates need for external power amplify

High Accuracy Distance Measurement
- Measures distance between connected LE devices w/ sub-meter accuracy

AI/ML accelerator
- Accelerates inferencing while reducing power consumption

Secure Vault High
- Protects data and devices from local and remote attacks

20-bit ADC
- 16-bit ENOB for advanced sensing

Antenna Diversity
- Provides 6-8 dBm better link budget

Improved Coexistence
- Ideal for gateways and hubs

PLFRCO
- Eliminates need for 32 KHz xtal

SEGMENTS AND APPLICATIONS

SMART HOME
- HVAC
- Locks
- LED Lighting
- Switches
- Sensors
- Gateways, Hubs and Panels

CONNECTED HEALTH
- Portable Medical

INDUSTRIAL AND SMART BUILDINGS
- Access Control
- HVAC
- Predictive Maintenance
- Asset Tracking

SMART CITIES
- EV Charging

COMMERCIAL
- Lighting
- Access Points
- Clinical Medical
- Indoor Real Time Location Services
Early Access and Application Development

SOC, DEV KITS
- 2x BRD4198A
- 2x Dipole Antennas
- Wireless Pro Kit
- EFR32MG24 + 10dBm OPN

STACK SOFTWARE
- In-house developed stack
- Supports Bluetooth 5.4 features
- All security features supported
- New and improved Ranging features

HADM DEMO
- Python based Visualization tool
- RTL Library (GATT, IQ reporting)
- EFR32xG24 NCP/SoC
- PBR, RTT modes

DEVELOPMENT TOOLS
- Simplicity Studio
- Initiator & Reflector Example
- Energy Profiler + Network Analyzer
- Quick Start Guide
- Salesforce Support

Early Access already integrated into GSDK release in June 2023!
Sample Applications – Out-of-Box Experience
<table>
<thead>
<tr>
<th>Feature</th>
<th>Now</th>
<th>Dec 2023</th>
<th>2024 *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase based ranging</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>RTT based ranging</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Simultaneous connections</td>
<td>1</td>
<td>4</td>
<td>4+</td>
</tr>
<tr>
<td>TX Power</td>
<td>0 dBm</td>
<td>0 dBm</td>
<td>0 dBm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10 dBm</td>
<td>10 dBm</td>
</tr>
<tr>
<td>Initiator</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Reflector</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Antenna switching</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Bluetooth Qualified</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* Subject to change
Get Started Right Away

CONTACT SALES
Work with Silicon Labs Sales and get access to hardware

DOWNLOAD
Download Simplicity Studio 5

HADM IN ACTION
See our accurate, reliable and simple distance estimating solution in action!
THANK YOU