The Latest in HADM using Bluetooth LE
Agenda

01 Target Markets and Applications
02 Demand for HADM – Beyond RSSI
03 HADM & Channel Sounding
04 Performance Results
05 Early Access & Sample Applications
06 Next Steps
High Accuracy Distance Measurement (HADM) Applications
Target Markets & Applications

HOME

- Item Finding
- Keyless Entry
- Pet Tracking

COMMERCIAL

- Access Control
- Inventory management
- Asset Tracking
Demand for Improved Distance Measurement – 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 & Channel Sounding

Channel Sounding (CS) is the Bluetooth feature that enables HADM.

- CS is currently being defined by the Bluetooth SIG
- Defines support for phase based ranging (PBR) tone exchange and/or round trip timing (RTT) packet exchange
- Also defines procedures, events, sub-events etc to enable distance estimation
Phase Based Ranging (PBR)

- Tone exchange between two devices
- Phase of RF signals is a function of 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 transmitted and received signal
- Security
  - Manipulation of phase is more complex than RSSI
  - IQ sample quality
- Much more accurate than RSSI
- Key Considerations
  - Antenna radiation patterns
  - Board design specific calibration
Round Trip Timing (RTT)

Packet transmission time (ToF) is measured on both 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

Less accurate than PBR

\[ RTT = 2 \text{ToF} = (ToA_I - ToD_I) - (ToD_R - ToA_R) \]
Measurement Procedure Explained

- Connection-based 2-way ranging with encrypted Bluetooth LE connection events and secure CS events
  - Reflector sends received signal info via GATT indications during connection events
- 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 – RSSI, PBR, RTT
  - Trade-offs between accuracy, duration, and power
- 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.
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**
  - Line of Sight (LOS), Non-Line of Sight (NLOS)
  - Physical obstacles (metal, plastic, glass, etc.) in NLOS configurations

- **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 Office Performance Results

![Graph showing median absolute error (m) vs. distance (m) for PBR distance estimation.](image-url)
Early Access and Application Development

Early Access integrated into 23Q2 GSDK release

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
- RSSI, PBR, RTT modes

DEVELOPMENT TOOLS
- Simplicity Studio
- Initiator & Reflector Example
- Energy Profiler + Network Analyzer
- Application Note
- Salesforce Support
BG24 and BGM241S: 2.4 GHz SoC Ideal for Bluetooth Location Services

<table>
<thead>
<tr>
<th>SOCS AND MODULES</th>
<th>SOC DEVICE SPECIFICATIONS</th>
<th>DIFFERENTIATED FEATURES</th>
<th>SEGMENTS AND APPLICATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>BG24 SoC</td>
<td>High-Performance Radio</td>
<td>+20 dBm output power</td>
<td>Smart Home</td>
</tr>
<tr>
<td></td>
<td>• Up to +19.5 dBm TX</td>
<td>• Eliminates need for external power amplify</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• -97.6 dBm RX @ LE 1 Mbps</td>
<td>• High Accuracy Distance Measurement</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• -105.7 dBm RX @ Bluetooth LE 125 kbps</td>
<td>• Measures distance between connected LE devices w/ sub-meter accuracy</td>
<td></td>
</tr>
<tr>
<td>BGM241S SiP Module</td>
<td>Efficient ARM® Cortex®-M33</td>
<td>AI/ML accelerator</td>
<td>Connected Health</td>
</tr>
<tr>
<td></td>
<td>• 78 MHz</td>
<td>• Accelerates inferencing while reducing power consumption</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1536kB Flash, 256kB RAM</td>
<td>Secure Vault High</td>
<td>Industrial and Smart Buildings</td>
</tr>
<tr>
<td></td>
<td>Low Power</td>
<td>• Protects data and devices from local and remote attacks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 33.4 µA/MHz</td>
<td>20-bit ADC</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td>• 5.0 mA TX @ 0 dBm</td>
<td>• 16-bit ENOB for advanced sensing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 5.1 mA RX (802.15.4)</td>
<td>Antenna Diversity</td>
<td>HVAC</td>
</tr>
<tr>
<td></td>
<td>• 4.4 mA RX (LE 1 Mbps)</td>
<td>• Provides 6-8 dBm better link budget</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1.3 µA EM2 sleep</td>
<td>Improved Coexistence</td>
<td>Predictive Maintenance</td>
</tr>
<tr>
<td></td>
<td>Multiple protocol support</td>
<td>• Ideal for gateways and hubs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bluetooth (1M/2M/LR)</td>
<td>PLFRCO</td>
<td>Asset Tracking</td>
</tr>
<tr>
<td></td>
<td>• Bluetooth mesh</td>
<td>• Eliminates need for 32 KHz xtal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Proprietary 2.4 GHz</td>
<td></td>
<td>Smart Cities</td>
</tr>
<tr>
<td></td>
<td>SoCs and Modules</td>
<td></td>
<td>• EV Charging</td>
</tr>
<tr>
<td></td>
<td>• 5x5 QFN40</td>
<td></td>
<td>Commercial</td>
</tr>
<tr>
<td></td>
<td>• 6x6 QFN48</td>
<td></td>
<td>• Lighting</td>
</tr>
<tr>
<td></td>
<td>• 7x7 SiP Module</td>
<td></td>
<td>• Access Points</td>
</tr>
<tr>
<td></td>
<td>• 12.9x15.0 PCB Module</td>
<td></td>
<td>• Clinical Medical</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Indoor Real Time Location Services</td>
</tr>
</tbody>
</table>
Software Stack Architecture

- **Flexible mode of operation**
  - Host-NCP mode – RTL library runs on host
  - SoC mode - RTL Library runs on xG24
  - Supported host platforms - Windows x64, Ubuntu x64, Raspbian (Cortex A), Darwin x64

- **GATT Ranging Service**
  - Measurement results sent via GATT indications

- **Extend ranging application to other location services via trilateration**
Sample Applications – Out-of-Box Experience
What’s Next?

works with
BY SILICON LAB
VIRTUAL CONFERENCE
AUG 22-23, 2023

Silicon Labs
Thank You

Watch ON DEMAND
Wi-Fi 6 Benefits for IoT Applications
February 2nd at 10 AM CT
Register Today