Advantages of Bluetooth® Mesh in Smart Building Applications
Introduction: The IoT – Bluetooth evolution
Bluetooth Mesh
• Application
• Stack Architecture
• Topology
• Security
• Messaging
• ST BlueNRG-Mesh
• Mesh resources
The IoT Revolution…
... Powered by Bluetooth®

Classic Bluetooth

Bluetooth Low Energy

- 1.0 (1999)
- 1.1
- 1.2
- 2.0
- 2.1
- 3.0
- 4.0
- 4.1
- 4.2
- 5.0 (2016)

- First Adopted Spec
- Major Bug Fixes
- Advanced Frequency Hopping and discovery
- Enhanced Data Rate
- Secure Simple Pairing and NFC Support
- Alternate MAC & PHY 24Mbps, Enhanced Power Control
- Bluetooth Low Energy Specification simultaneously
- 4G LTE Co-existence, Hub and end-point
- Higher throughput, 6lowpan, FIPS
- LE 2M PHY, Long range, Advertising extension
Bluetooth Networking Evolution

**PAIRING**
one-to-one

- DATA TRANSFER
  - Sports & fitness devices
  - Health and wellness devices
  - Peripherals and accessories

**BROADCASTING**
one-to-many

- LOCALIZED INFORMATION
  - Point of interest beacons
  - Item finding beacons
  - Way finding beacons

**MESH**
many-to-many

- LARGE DEVICE NETWORKS
  - Building automation
  - Wireless sensor networks
  - Asset tracking
Bluetooth MESH is Here!

July 2017 - Bluetooth SIG Announces Mesh Networking Capability

Brings proven, global interoperability and the mature, trusted ecosystem of Bluetooth technology to industrial-grade device networks

Reliable, Scalable, Secure
- Reliability enables inherently self-healing networks with no single points of failure
- Scalability: Supports thousands of nodes with industrial-level performance
- Security: Provides industrial-grade security for protection against all known attacks

Interoperable
- A full-stack solution: A unique full stack approach that defines everything from the low-level radio to the high-level application layer, ensuring all levels of the technology are fully specified
- An interop-centric spec: Comprehensive interoperability testing conducted prior to specification release, not after
- Time-tested tools and processes: A 20-year history of delivering the qualification tools and processes necessary to ensure global, multi-vendor interoperability

Trusted Global brand: Bluetooth SIG
- Value-added services: A mesh network built on Bluetooth can also provide localized information, asset tracking and wayfinding services
- A mature ecosystem: The best enabling technology, along with the development and test tools and services needed to shrink your time to market
- Global brand awareness: A trusted global brand that stands for simple, secure wireless connectivity

Low-Power BLE SoC ARM Cortex-M0 programmable core with up to 256KB eFlash
Bluetooth Mesh Applications

The Bluetooth SIG MESH Specification intends to extend the capabilities of Bluetooth Smart chips to answer more and more complex applications. The protocol has been developed with the Smart Lighting industry in mind.

- Lighting
- Smart Home and Building automation
- Wireless sensor networks
- Asset tracking
- Healthcare

- Same network may have multiple applications running
  - Lights, sensors, switches co-exist
- Nodes in a single network have same “Network key”
- Different applications have different “Application key”
Mesh System Architecture

- User scenarios / Application, e.g., Lighting, Sensor
- Configuration of Mesh, Management
- Format of Application data:
  - Data format
  - Encryption/decryption
  - Data verification
- Encryption/decryption and authentication of application data passing to/from the access layer
- Segmentation and reassembly of PDUs
- Message address types and a network message formats. Relay and Proxy features may be implemented by the network layer
- How mesh PDUs are handled by a communication system. 2 bearers defined:
  - Advertising Bearer: uses LE GAP advertising and scanning to send and receive mesh PDUs.
  - GATT Bearer: though Proxy Protocol allows a device which does not support Advertising Bearer to communicate with nodes of a mesh network
- Standard BT LE Stack
The Bluetooth Mesh working group chose for mesh network mechanism a **flooding protocol**. Compared to routed protocols, it is **much more simpler** to deploy. To stay efficient, the BLE Mesh take advantage of a **managed flooding network**.

- Expose the interface for Smartphone/Tablet to interact with a mesh network
- Simple leaf node whom cannot relay messages
- Able to retransmit received messages
- Enable multiple “hops” in the network
- Battery operated devices
- Primarily send messages Rarely receive messages
- No need of 100% duty cycle
- Stores messages addressed to LPNs and delivers them whenever the LPN polls for “waiting messages”
The Bluetooth Mesh working group chose for mesh network mechanism a **flooding protocol**. Compared to routed protocols, it is **much more simpler** to deploy. To stay efficient, the BLE Mesh take advantage of a **managed flooding network**.

- No single point of failure: self healing
- Direct communication between adjacent nodes
- Messages contain sequence number to optimize the network usage and protect against replay attacks.
  - Reject already received messages.
- TTL/Time to Live method: Limit the number of times a message is relayed

---

**Bluetooth Mesh Topology**

**Managed Flooding**

Standard BLE Connection
Built-in Security

Unconfigured device

Provisioning
• 256-bit ECDH algorithm (public/private keys)
• Exchange several security keys
• Set a unique address for the device
• Two separate BLE connections to secure the communication link

Configured node

Mesh communications
• Encrypted with 128-bit AES-CCM
• Multiple layers security thanks to the network/application keys shared during provisioning
• Privacy through obfuscation
• Protection from multiple types of attack:
  ▪ Replay attack
  ▪ Bit-Flipping attack
  ▪ Eaves Dropping attack
  ▪ Man-in-the-middle attack
  ▪ Trashcan attack
Security Keys

• **Network Key**
  - Net Key secures the communication at the Network Layer and is shared across all Nodes in the network. The possession of a given Net Key is what defines membership of a given mesh network.
  - Allows a node to decrypt and authenticate up to the Network Layer and to relay messages throughout a network.
  - A single compromised device can compromise the whole network. Some nodes (outside the house) can be given a subnet key instead of the main network key.

• **Application Key**
  - Same network may have multiple applications running: Lights, sensors, switches co-exist.
  - Different applications have different “Application key”.

• **Device Key**
  - Unique key for each device, only known by the Provisioner and a single device, used for provisioning, configuration and key management.
Why both Network and Application Keys?

• We can’t have a compromised door bell allow anybody to unlock door.

• Light nodes can relay door access messages without being able to decrypt them.
• Publish to Single Group: send a message to unicast /virtual /group address
  • A client device (switch) can publish messages (ON/OFF control) and a server device (light bulb) can be notified (if subscribed) of new command arrival.

• Subscribe on Multiple Groups: nodes (e.g. Lights) configure themselves to receive messages sent to specific addresses. Different nodes can subscribe to the same address.
  • A virtual address can have a semantic meaning to users: e.g. the name of a room
“Elements” and “Models” based on a full-stack specification and models

The Bluetooth SIG MESH Profile defines a standard access layer to exchange messages between a BLE device and a Smart Application (Controller) for simple control and monitoring applications using “Elements” and “Models”.

**Elements**: parts of a single node, can be independently controlled. Messages can be sent from one element to one or more elements.

**Model**: represents a specific service and defines a set of states and messages that act on these states. Model examples: Device Configuration, Sensor Reading, Light Control or Vendor Specific models.
**Example: ST BlueNRG-MESH SDK**

**BLE network processor vs BLE application processor**

**Network processor:**
- Dual chip solution
- Peripheral/memory flexibility
- Adding BLE connectivity to existing designs
- SPI interface
- External MCU examples based on STM32
- Support BLE 4.1

**Application processor:**
- Single chip solution
- Cost reduction
- Hosting customer application
- Small form factor
- Can also behave like a network processor
- UART, SPI interfaces when used as network processor
- Support BLE 4.2
ST BlueNRG-Mesh Facts and Figures

- **Power consumption**: 7 mA average
- **Provisioning procedure**: 15 seconds average
- **SoC Memory footprint**: 109 KB Flash, 20 KB RAM
- **Dual chip Memory footprint**: 88 KB Flash, 19 KB RAM
- **Application Payload**: 8 bytes unsegmented, 64 bytes segmented
- **Network size**: Constantly tested on 30 nodes network
- **Compatible with both BLE 4.X or 5.0**
- **BLE Mesh 1.0 certification**: End of June 2018
- **Hop latency**: 10-20 ms
How to Get Started on BlueNRG-Mesh

BLE Mesh SDK resources

HW resources (BlueNRG-Mesh node evalboards)

BlueNRG-1
BlueNRG-2

STEVAL IDB007Vx
STEVAL IDB008Vx

BlueNRG-MS

+ NUCLEO-L152RE
+ IDB005V1

Documentation resources

- UM2290: Android API Guide
- UM2180: Getting started with Android
- UM2361: Getting started for iOS App
- UM2295: Getting started with Mesh Embedded Firmware
Bluetooth Mesh Roadmap: Routing

FLOODING network
All nodes participate to broadcast messages
Available now in BlueNRG-MESH SDK

ROUTING network
Routing path Tx-to-Rx is known in advance
Specs ongoing by BT SIG (H1’18 for BlueNRG-MESH)

Packet format is optimized for small control packets, issuing single commands or reports, and is not intended for data streaming or similar high-bandwidth applications.
Additional Resources

- Bluetooth Mesh deep dive:
  - Bluetooth Mesh specification
  - Bluetooth Mesh overview
  - Bluetooth Mesh FAQ

- Software resources available this week (firmware, Android):

- BlueNRG-Mesh Android application available on Play Store:
Thank you!

Q&A