Università Politecnica delle Marche
Facoltà di Ingegneria
Corso di Laurea in Ingegneria Elettronica

BLUETOOTH MESH

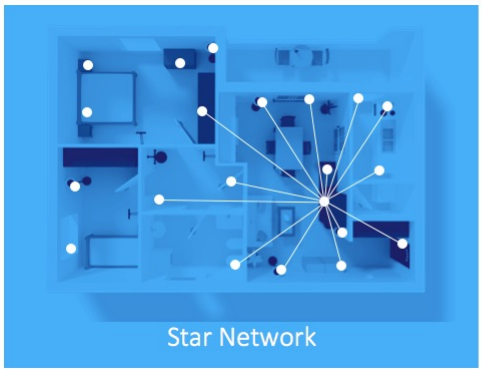
1

Università Politecnica delle Marche
Facoltà di Ingegneria
Corso di Laurea in Ingegneria Elettronica

What exactly is Mesh Networking?

2

2



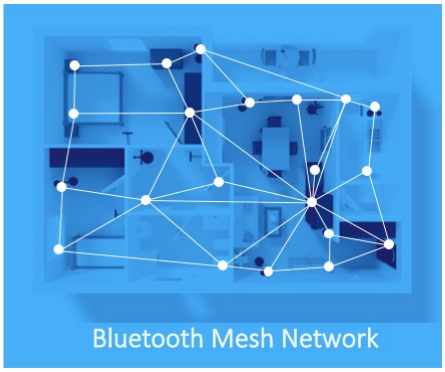
Bluetooth is what is referred to as a '**star-type topology**'. This means that all devices connect to **one central hub** rather than communicating with each other. The only way to expand the network is to connect more devices to the central hub.

3

3

Università Politecnica delle Marche
Facoltà di Ingegneria
Corso di Laurea in Ingegneria Elettronica

With **mesh networking**, all of the devices in a network can **communicate with each other**, rather than having to connect with one central hub. This makes the size and area of the network virtually unlimited, which is why it is so useful for industrial IoT applications like large connected sensor networks.



4

4

Bluetooth®
SPECIAL INTEREST GROUP

In July of 2017, the ***Bluetooth Special Interest Group (SIG)*** released an ***independent*** extension of the Bluetooth Core Specification called

Bluetooth Mesh.

5

5

Overview Bluetooth Mesh

- *Communication M:M*
- *Based on Bluetooth Low Energy*
- *Messages oriented*
- *Publish/Subscribe*
- *Advertising/scanning, NO connection between devices*
- *Transmission broadcast*
- *Menaged Flooding*
- *High security*

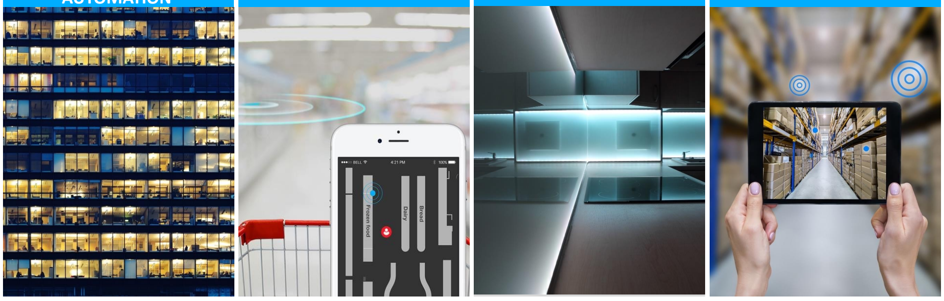
6

6

Università Politecnica delle Marche
Facoltà di Ingegneria
Corso di Laurea in Ingegneria Elettronica

Application for Mesh Network

HOME & BUILDING AUTOMATION	BEACONING	LIGHTNING	ASSET TRACKING



Scale system deployment Support device-to-device communication	Simplify beacon management Deliver location services Increase beacon service range	Deliver instant response to switch actions Provide advanced lighting control Integrate functionality	Eliminate manual scanning Determine location in real-time Simplify beacon deployment

7

7

Università Politecnica delle Marche
Facoltà di Ingegneria
Corso di Laurea in Ingegneria Elettronica

New Words…New Terms…New Concepts!!!

8

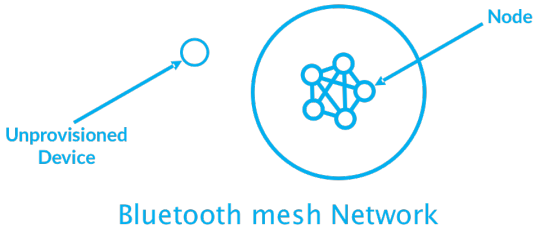
8

Device and Node

A **node** is a device that has joined a Bluetooth mesh network.

Devices that are not part of the network are called **unprovisioned devices**.

Once an unprovisioned device gets **provisioned**, it joins the network and becomes a node.



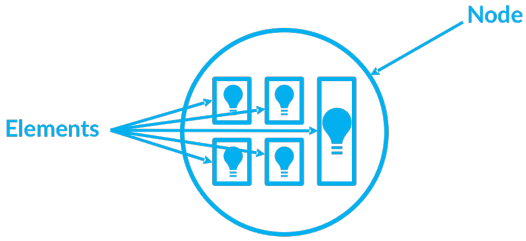
9

9

Università Politecnica delle Marche
Facoltà di Ingegneria
Corso di Laurea in Ingegneria Elettronica

Elements

A **node** may contain multiple parts which can be controlled independently.
(e.g a light fixture may contain multiple light bulbs which can be turned on/off independently).
These different parts of a single node are referred to as **elements**.



10

10

Messages and State

Communication between nodes in a mesh network is accomplished through sending ***Messages***. Messages are associated with Model and operate on States.

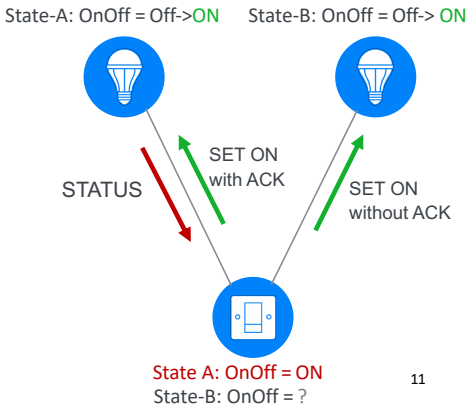
A ***State*** represents the condition of some aspect of an Element together with some associated behaviors.

All messages belong to three generic types:

GET : to request the value of a state at one or more nodes. It receives a STATUS message as a response.

SET : to change the state value of a node or group of nodes. Set messages can be with acknowledged or unacknowledged.

STATUS : notify current state.



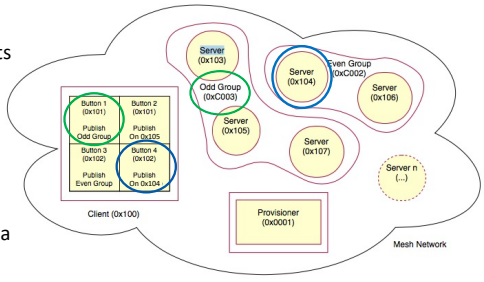
11

Address

Bluetooth mesh uses a system of various address types to identify individual Elements or set of Elements.

Unicast Address identifies a single, specific Element of a Node. A provisoner manages the allocation of unicast addresses and ensure that there are no duplicates in the network.

Group, it is a multicast address that represents one or more elements.
Bluetooth SIG has defined 4 standard group: ALL PROXIES, ALL FRIEND, ALL RELAY, ALL NODES
Moreover they can be dynamically defined by the user through the configuration procedure.
There may be up to 16383 group addresses in a mesh network.



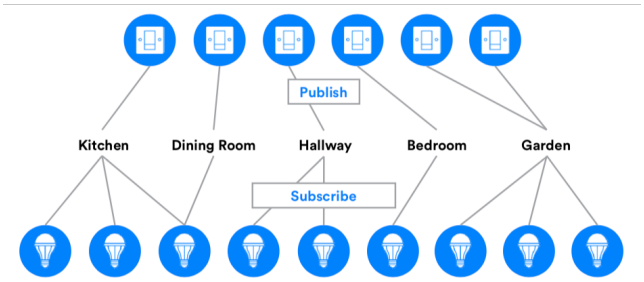
Virtual Address, may be assigned to one or more Elements. It takes the form of a 128-bit UUID value and it is much like a label. There may be up to 70 trilion of virtual addresses.

12

Publish / Subscribe

Messages sent and received across the mesh network conform to a publish-subscribe model of communication.

- Sending messages from one node to a set of one or more other nodes is referred to as ***Publishing***.
- Configuring a node to receive certain messages is known as ***Subscribing***.
- Tipically, messages are addressed to group or virtual addresses.



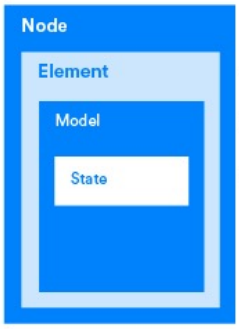
13

13

Models

A Model defines ***node functionality*** : States, States Tansitions, State Binding, Messages and other associated behaviors.

An Element within a Node must support one or more models.



There are three broad category of models:

- ***SERVER*** model defines the different states that the element to which the model belongs can send and receive.
- ***CLIENT*** model didn't define any state, but only messages that can be sent and receive (GET, SET e STATUS)
- ***CONTROL*** model contains both the server and client model.

Bluetooth SIG defines some standard types of models:

1. ***Foundation*** configuration and Health
2. ***Generic*** On/Off, Level, Power, Location, Transition Time, Properties
3. ***Sensors*** Sensor, Time
4. ***Lightinig*** Light, Lightness, CTL, HSL, xyL, Controller
5. ***Vendor specific models***

14

14

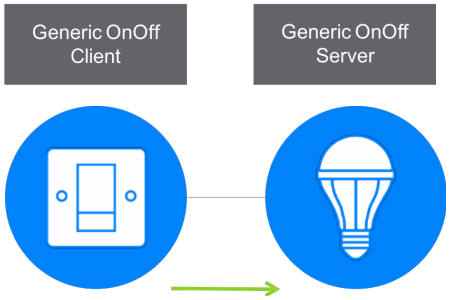
Generic OnOff Model

The simplest generic model is the Generic OnOff Model. It define a single State, called Generic OnOff, which may have value:

- 0x00 to rappresent Off
- 0x01 to rappresent On

The Model defines 4 type of messages:

1. Generic OnOff Get
2. Generic OnOff Set
3. Generic OnOff Set Unacknowledged
4. Generic OnOff Status



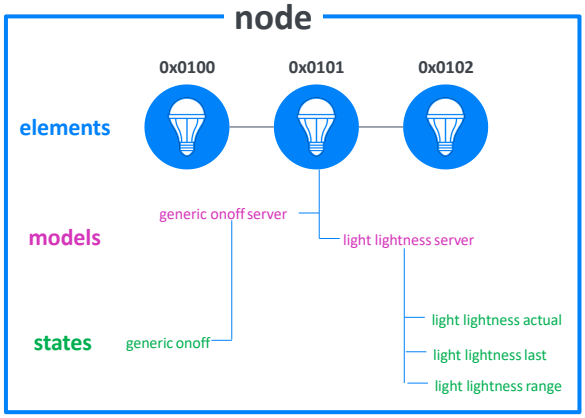
15

15

Università Politecnica delle Marche
Facoltà di Ingegneria
Corso di Laurea in Ingegneria Elettronica

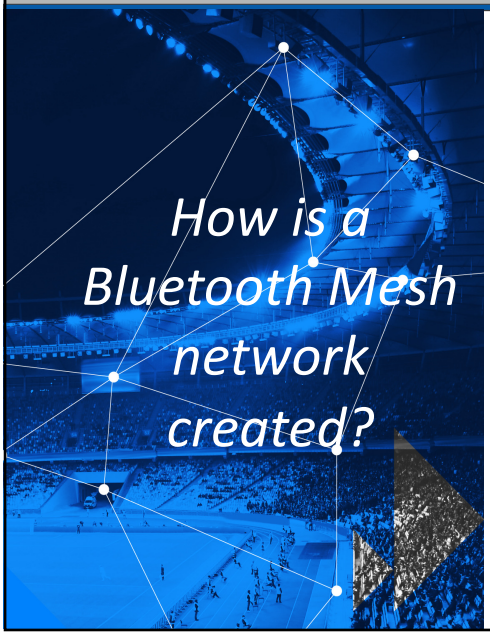
Summing up

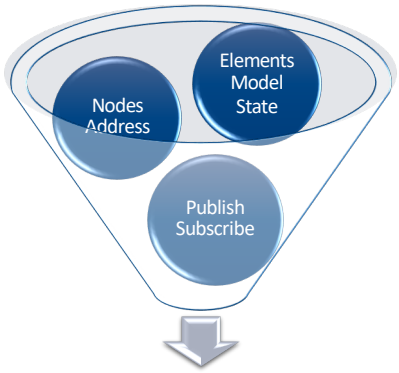
single node
3 elements
multiple models and states



16

16



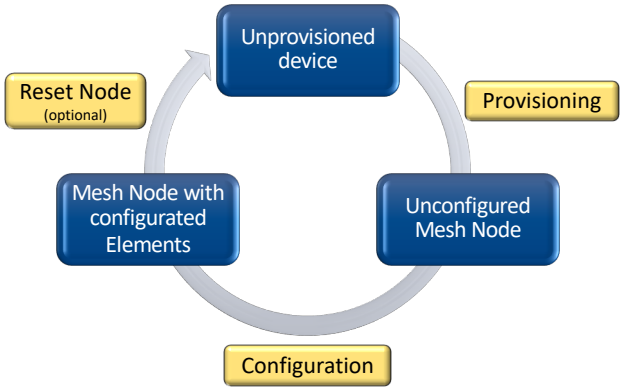


Bluetooth Mesh

17

17

To create a Bluetooth Mesh Network and make each device actively participate in the network, it must switch from a status of ***Unprovisioned Device*** to the ***Configured Mesh Node*** status.



18

18

Provisioning

Provisioning is the process by which a device is added to a mesh network. After being provisioned, a device is referred to as a **Node**.

Provisioning involves a five step process:

1. BEACONING
2. INVITATION
3. EXCHANGING PUBLIC KEYS
4. AUTHENTICATION
5. DISTRIBUTION OF THE PROVISIONING DATA

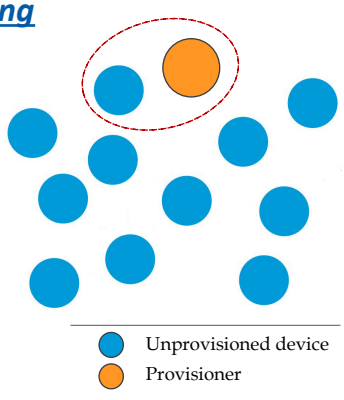
Università Politecnica delle Marche
Facoltà di Ingegneria
Corso di Laurea in Ingegneria Elettronica

Provisioning

1 - Beaconing

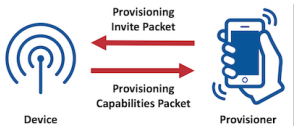
I – Each unprovisioned device communicates periodically in broadcast its availability to be provisioned by sending the **mesh beacon advertisement.**

II – when the provisioner detects a request for a unprovisioned node to be able to access the network, a 1:1 comunication begins.



2 – Invitation

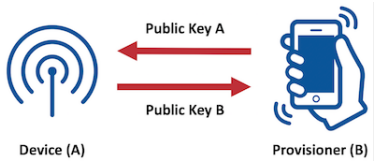
The provisioner sends an invitation to the device to be provisioned in the form of **Provisioning Invite PDU**
The device responds with information about itself sent via **Provisioning Capabilities PDU.**



Provisioning

3 -Exchanging Public Keys

Provisioner and unprovisioned node exchange their public keys, which can be static or ephemeral.

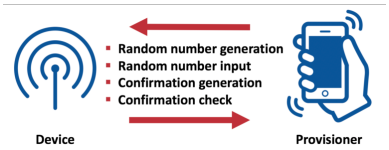


4 – Authentication

The device to be provisioned generates a pairing sequence based on its hardware capabilities:

- blinking led
- numerical sequence if a display is present

Side Provisioner an input device must be present, a button for the first method and a numeric keypad for the second.



21

21

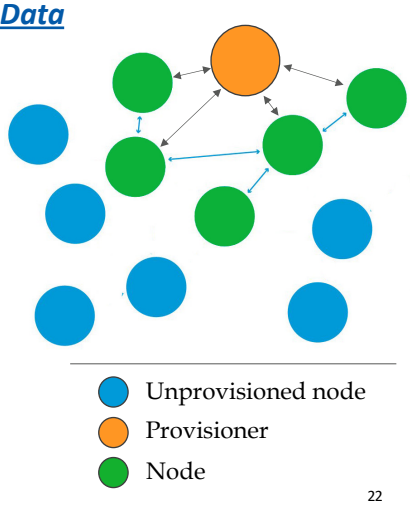
Provisioning

5 – Distribution Of The Provisioning Data

A SESSION KEY is generated from the private keys and the public key exchanged.
This key will be used to distribute all the data necessary to complete the provisioning process:

- *NetKey* (Network Key)
- *DevKey* (Device Key)
- A security parameter called *IV index*
- A *Unicast address*.

From this moment on, the device will be called ***NODE!!!***



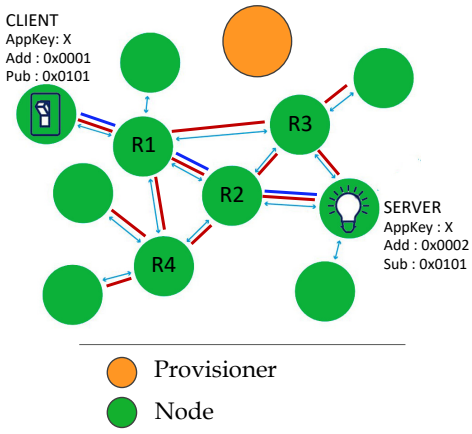
22

22

Configuration

Process by which the ***user defines*** for each model of the node: the intended use (AppKey), the publication address (Client) / subscription (Server) and any added features (ACK enabling, number of retransmissions, relay function , ...)

The configuration can be performed via provisioner or via smarphone/tablet/pc with a specific app.



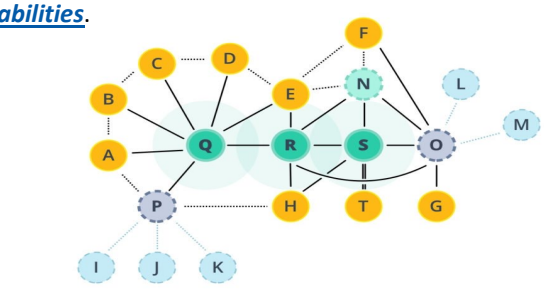
23

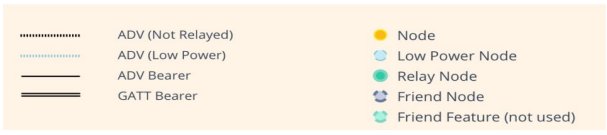
23

Type Of Node

In a mesh network all the nodes are able to receive and send messages, however there are some particular features that a node can possess, which allows it to have ***special capabilities***.

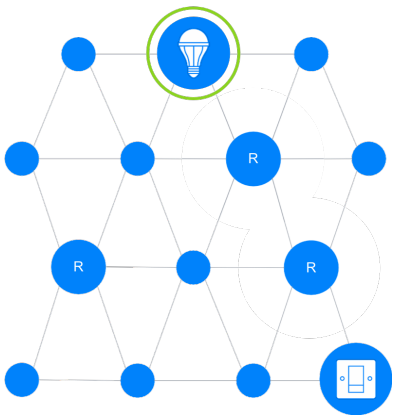
- ***Relay Nodes***
- ***Proxy Nodes***
- ***Friend Nodes***
- ***Low Power Nodes***





24

24



R = Realy function ON

Relay nodes

Messages get sent to the other nodes that are in direct radio range of the publishing node, but if the nodes to be reached are out of range, a "repeater" of messages is necessary to allow it to arrive at destination.

A Relay node can ***retransmit messages*** that are broadcast by other nodes.

This type of node is ***essential to extend network coverage*** and allow messages to be transmitted internally.

25

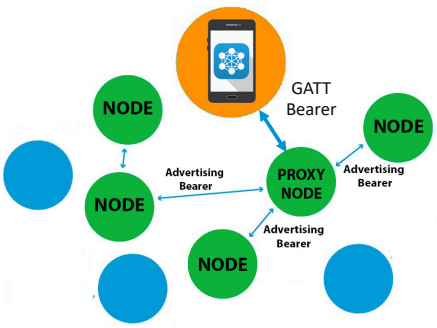
25

Proxy nodes

Enable message proxy between Bluetooth Mesh and ***GATT devices*** like Smartphones, ipad

This type of node is also necessary to perform the provisioning process via devices that don't support ***Advertising Bearer.*** (e.g. smartphone, tablet, pc) A specific app must be installed for this purpose.

There may be ***one or more proxy nodes*** in a Bleutooth mesh network



26

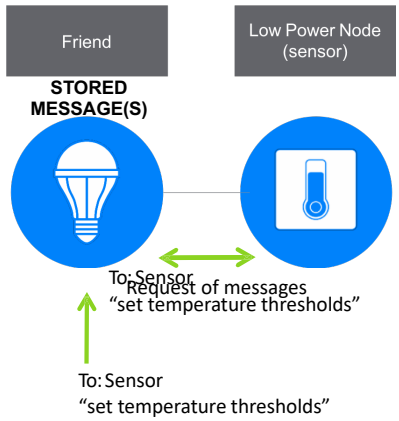
26

Friend Nodes and Low Power Nodes

Low Power Nodes are equipment with limited energy resources. (e.g sensors)

To avoid always listening on the radio channels to receive messages from the mesh, LPN works with a Friend Node.

The **Friend Nodes** store the messages addressed to the LPN with whom they are friends, and forward them when the LPN reactivates the radio channel.



27

27

Università Politecnica delle Marche
Facoltà di Ingegneria
Corso di Laurea in Ingegneria Elettronica

How data is transmitted within the Bluetooth Mesh

28

Data Transmission

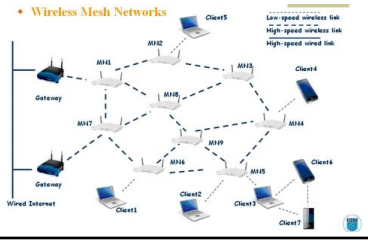
There are two primary techniques used to relay data across the mesh networks,namely ***routing*** and ***flooding*** .

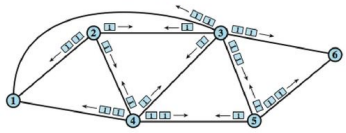
Routing

- Transmission along a selected path
- Use of specif nodes to relay messages: router
- Need for routing table
- Reliance on routers can give rise to single points of failure and a network which is not robust or reliable.

Flooding

- broadcast transmission to all nodes in direct range
- messages take multiple paths to reach their destination
- all nodes forward to all nodes
- No routers
- heavy network congestion





29

Managed Flooding

Bluetooth mesh networking uses a ***specialised and highly optimized*** version of flooding called ***Managed Flooding***.

No connection - No routing table - No set route - Broadcast transmission - Relay of messages (if enable) – No single point of failure - more reliable – more efficient

FLOODING + OPTIMIZATIONS
- Relay
- TTL (Time-to-Live)
- Message cache
- Friendship: Low Power Node and Friend Node
- Heartbeats
- Subnet

= **MANAGED FLOODING**

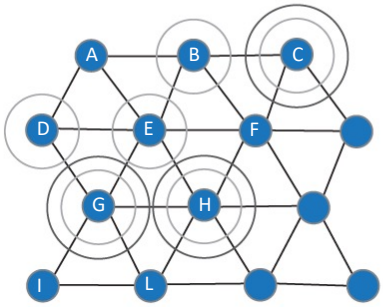
30

30

TTL Time to Live, is a field included in all bluetooth mesh PDUs. It controls the maximum number of hops, over which a message will be relayed.

Message cache a Network Message Cache must be implemented by all nodes. The cache contains all recently seen messages and if a message is found to be in the cache, indicating the node has seen and processed it before, it is immediately discarded.

Friendship probably the ***most significant optimisation*** mechanism in a Bleutooth mesh Network. It is the relationship betwenn Friend nodes and Low Power Node explained previously.



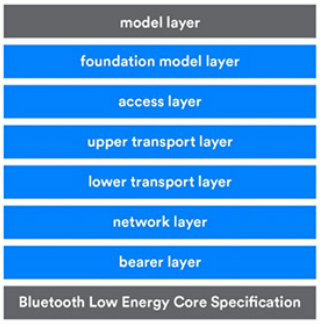
Heartbeats are messages transmitted by nodes periodically and they indicate to other nodes in network that the nodes sending the heartbeats is still active.
In addition, a data is inserted that contains how far the sender is, in term of the numebers of hops.

Subnet to partition a mesh network. This is primarily for security purposes but it does also have the benefit that messages sent using a subnet are not relayed beyond that subnet. This conserves energy.

31

31

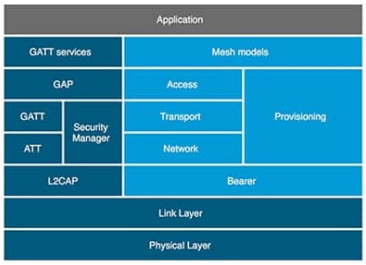
Architecture



The Bluetooth Mesh network introduces a new protocol stack and is based on Bluetooth Low Energy.

Any Bluetooth Low Energy chip of the previous generation (4.0, 4.1, 4.2, 5) can be modified to run Bluetooth Mesh with a simple firmware update, which is a good thing for field installations to take advantage of the new technology.

The reason for this backward compatibility derives from the fact that Bluetooth Mesh is ***not an integral part*** of the Bluetooth Low Energy stack, but is a ***separate new entity*** composed of seven levels.



32

32

Architecture

model layer	Defines models and thus functionality.
foundation model layer	Defines states, messages, and models required to configure and manage a mesh network.
access layer	Defines format of application data and how higher layer applications used the upper transport layer.
upper transport layer	Encrypts, decrypts, and authenticates application data.
lower transport layer	Defines how upper layer transport layer messages are segmented and reassembled into multiple lower transport PDUs.
network layer	Defines how transport layer messages are addressed towards one or more elements.
bearer layer	Defines how network messages are transported between nodes.
Bluetooth Low Energy Core Specification	Bluetooth Low Energy

33

33

Security in Bleutooth Mesh

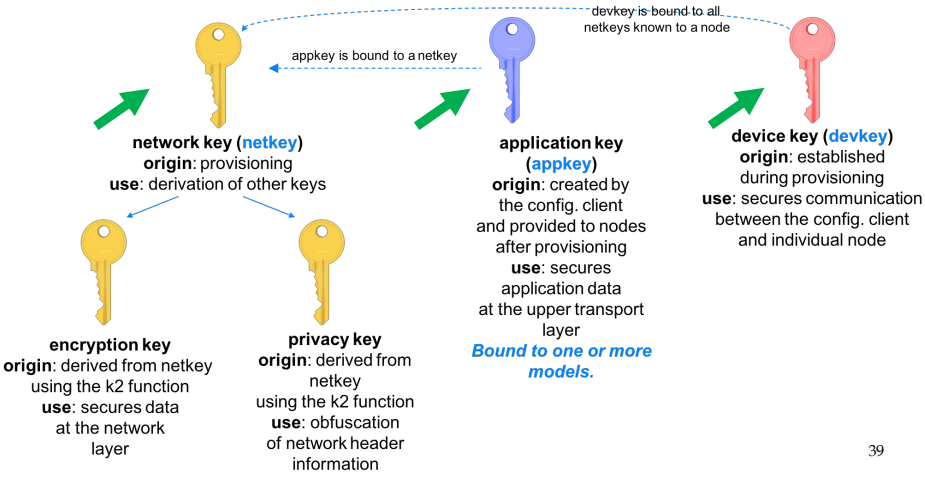
- Mandatory, cannot be reduced
- Encryption and authentication
- Separate security for network and each application
- Area isolation
- Message obfuscation
- Protection from replay and trashcan attacks
- Secure device provisioning

38

38

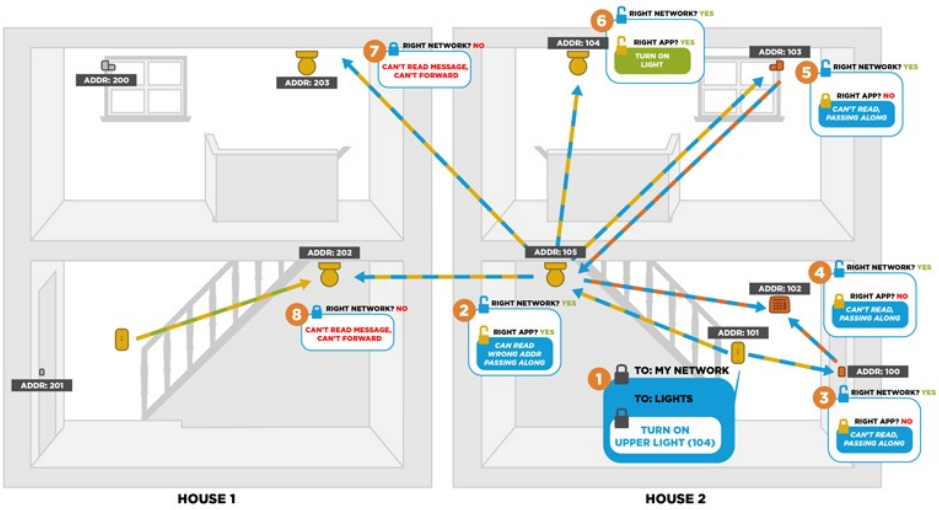
Securety handled in Bleutooth Mesh

In the Bluetooth Mesh there are many types of security key, each for a specific purpose : Encryption, Obfuscation, Authentications



39

Example



41

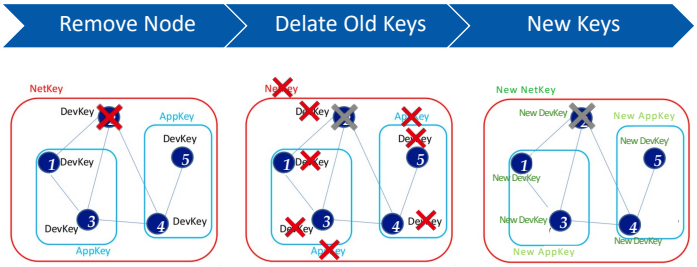
Key Refresh

When a node is removed for any reason (broken, network reduction, HW update)

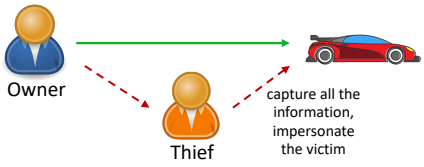
A possible flaw is created in the security system of the mesh. Teh Keys can be recovered from the deleted node

SECURITY WARNING

The standard provides a **Key Refresh** of all the keys of the entire network

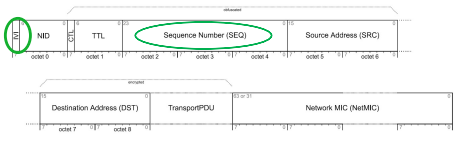


Protection from replay attack



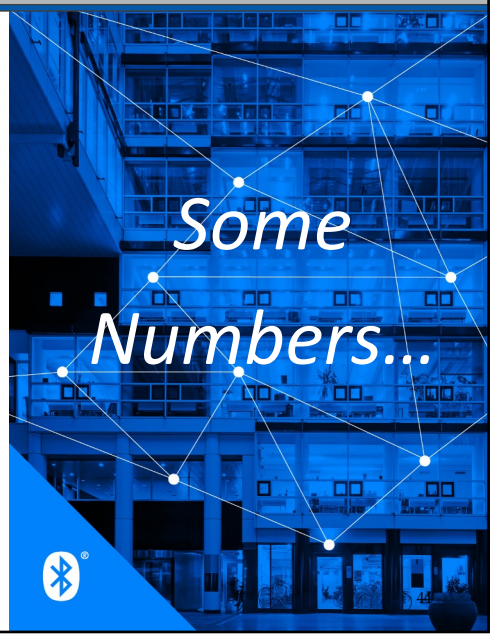
Replay Attack

The Bluetooth Mesh standard, to protect against these types of attacks, uses two fields of the network PDU : ***Sequence Number*** and ***IV index.***



Rules:

- Elements increment SEQ each time they send a command.
- A node, receiving a value of SEQ equal to or less than that of a previous valid message, will eliminate it.
- The values of the Index IV within the messages of a given element must always be equal to or greater than the last valid message of that element.



32767 Elements in a mesh network

127 Max number of Hops can be made by a mesh message

16383 Group Address in a mesh network

70 trillion (10^{18}) Virtual Address in a mesh network

340 unidecillion (10^{66}) mesh networks

4096 Applications in a mesh network

4096 Subnets in a mesh network

65535 Scenes in a mesh network

44

Thanks for Your attention

46