ECEN 5823-001
Internet of Things Embedded Firmware

Lecture #21

05 November 2018

Be Boulder.

University of Colorado Boulder

Agenda

- Class Announcements
- Reading Assignment
- Final Exam
- Quiz 9 review
- Bluetooth Mesh

Class Announcements

- Quiz 10 due on Sunday, November 11th, at 11:59pm
- Course Project Proposal due Sunday, November 11th, at 11:59pm

Reading Assignment

ECEN5823-001, -001B – Reading List
Internet of Things Embedded Firmware
Week 11

Note: There is a quiz this week. The material covered on the quiz will be from the last several chapters of the course textbook as well as the below readings and course lectures.

1. Silicon Labs' White Paper, "Bluetooth Mesh Technology Wireless Technology for the World of IoT.pdf"
    a. Pages 11-24
    b. Located on the Canvas week 11 reading assignment folder

Final Exam information – Preliminary

- When: Monday, December 17th, at 4:30pm to 7:00pm
  - Distant Students will have from 4:30 to 11:59pm on Monday December 17th
- Where: TBD?
- Questions:
  - Similar style to mid-term
  - Total 80 questions
    - 40 new questions (1pt each)
    - 40 quiz questions (1pt each)
  - Question bank will be roughly 300 questions
- Quiz questions will be selected from quizzes 6 through 11

Final Exam information - Preliminary

- Final will be on Canvas
- 1 sheet (both sides) of notes is allowed (individual work)
- No access of electronic notes such as past quizzes, lecture slides, etc is allowed
- No phones are allowed at the exam
- Must be turned in at the end of the exam
- CU Honor code is to be enforced for the Final Exam

Quiz 9 review

Match the following application with the most appropriate Bluetooth standard.

In-car infotainment	[Choose] ▾
PC peripherals	[Choose] ▾
Asset tracking	[Choose] ▾
Way finding	[Choose] ▾

Quiz 9 review

Match the description with the Bluetooth Mesh feature.

Messages contain data to allow the receiving nodes to determine the number of hops between the nodes.	[Choose]
All Bluetooth Protocol Data Unit contain this field.	[Choose]
Compulsory for each node.	[Choose]
Receives and buffers addressed messages to configured Low Power nodes	[Choose]
If the transport Message Integrity Check is not successful, the message is discarded.	[Choose]

Quiz 9 review

[ ] mesh networks are easier to implement while [ ] networks have better scalability.

Quiz 9 review

Bluetooth mesh applications are defined using a _____ architecture communicating using a _____ paradigm.

Quiz 9 review

Match the following description to the type of Bluetooth Mesh node.

Relay	[Choose]
Proxy	[Choose]
Low Power	[Choose]
Friend	[Choose]
Gateway	[Choose]

Quiz 9 review

Match the Bluetooth Mesh Out of band authentication method with its definition.

Provisioner outputs a value - user inputs the value into the device	[Choose]
Device outputs a value - user inputs the value into the provisioner	[Choose]
Device communicates the value by non-Bluetooth means	[Choose]

Quiz 9 review

Match the description with the Bluetooth Mesh feature.

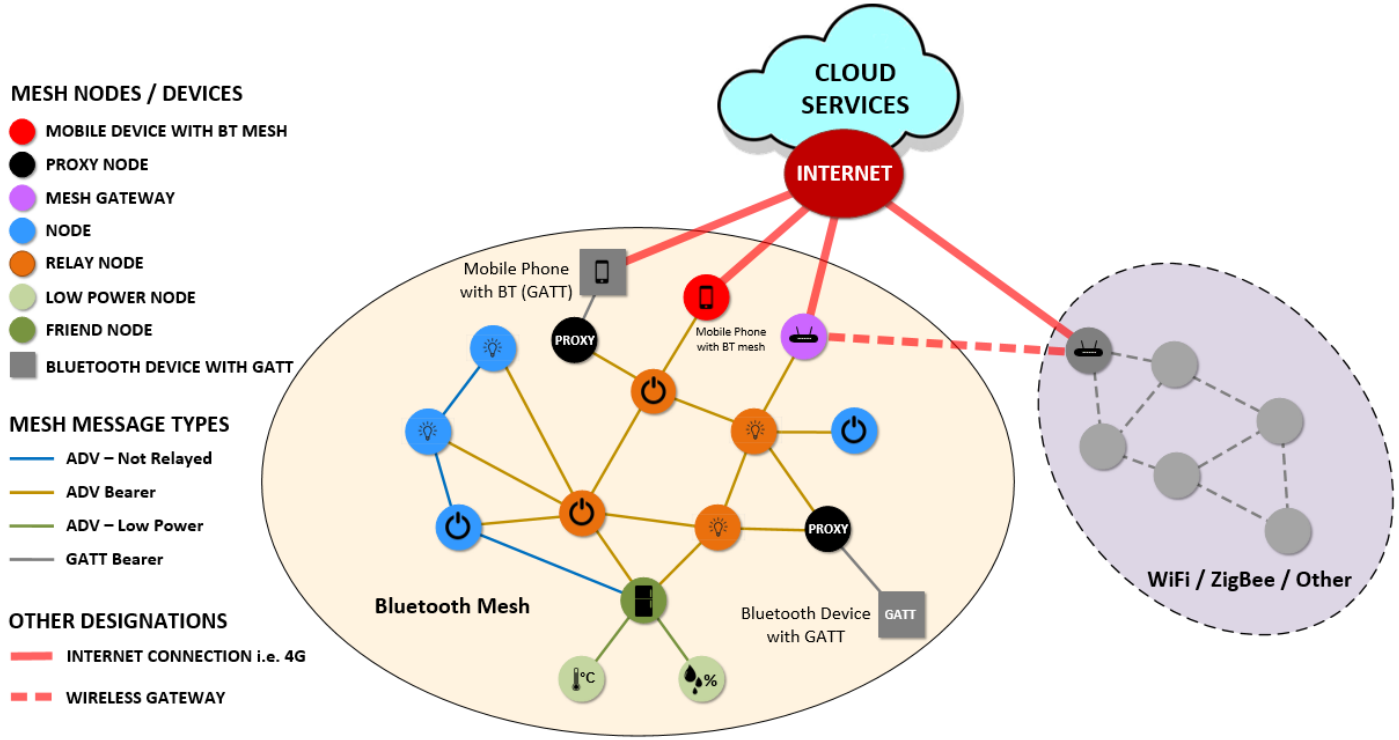
Nodes send messages periodically to indicate that they are functioning.	[Choose]
Controls the maximum number of hops.	[Choose]
Used to indicate that a message has already been received and processed, therefore the message is discarded.	[Choose]
Used in combination with Low Power Nodes.	[Choose]
Optimization of messages not addressed to the node.	[Choose]

Bluetooth Mesh - Nodes

- Relay: Receive and retransmit mesh messages by using the Advertising Bearer to enable larger networks
- Proxy: Receive and retransmit mesh messages between GATT and Advertisement Bearers
- Low Power: Operation at significantly reduced receiver duty cycle in conjunction with a node supporting the Friend feature
- Friend: Enables helping a node supporting the Low Power feature by storing messages on its behalf
- Gateway: Used between a Bluetooth mesh and a non-Bluetooth wireless network to allow data sharing based on protocol conversion

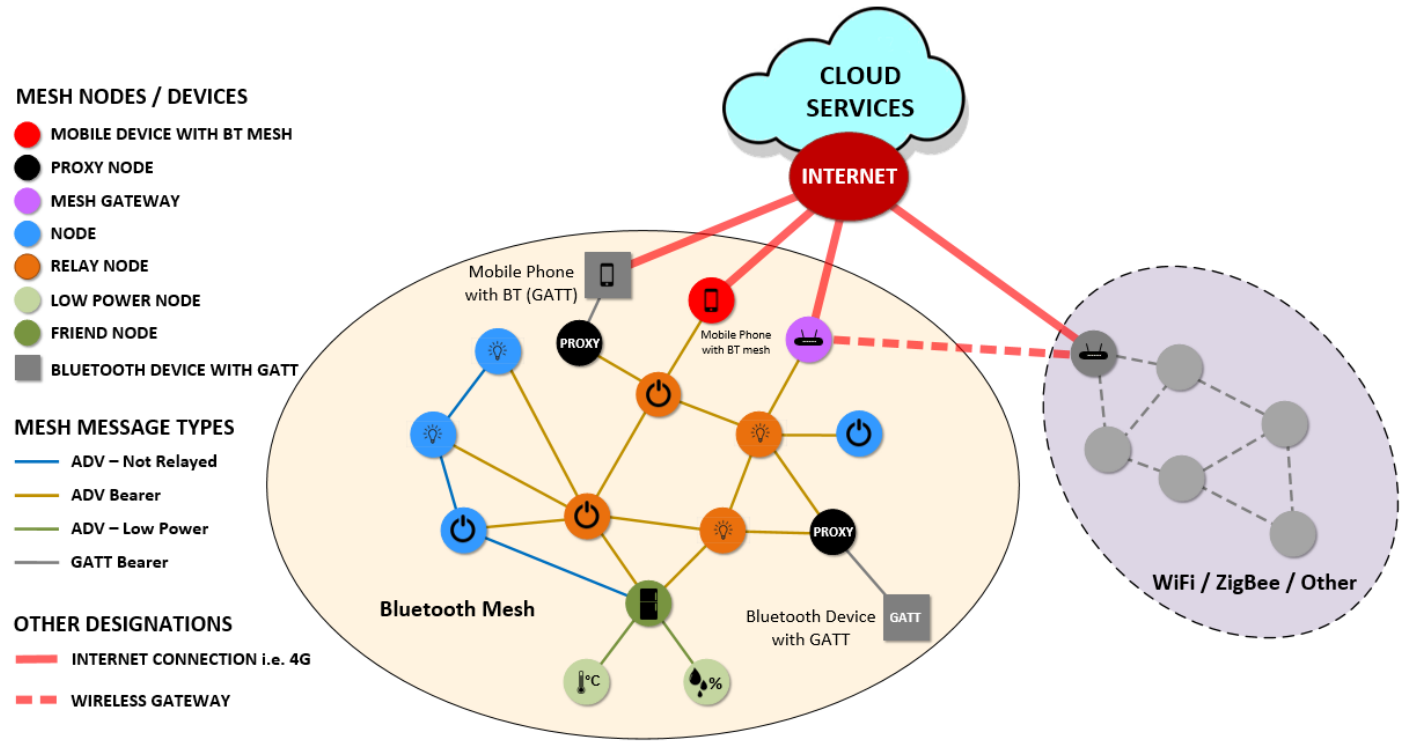
Bluetooth Mesh – Relay Node

- Relay nodes receive and retransmit mesh messages by using the Advertising Bearer to enable larger networks
- Relay nodes are typically powered from an electrical outlet and are awake all or most of the time to be able to receive and relay messages at any time.



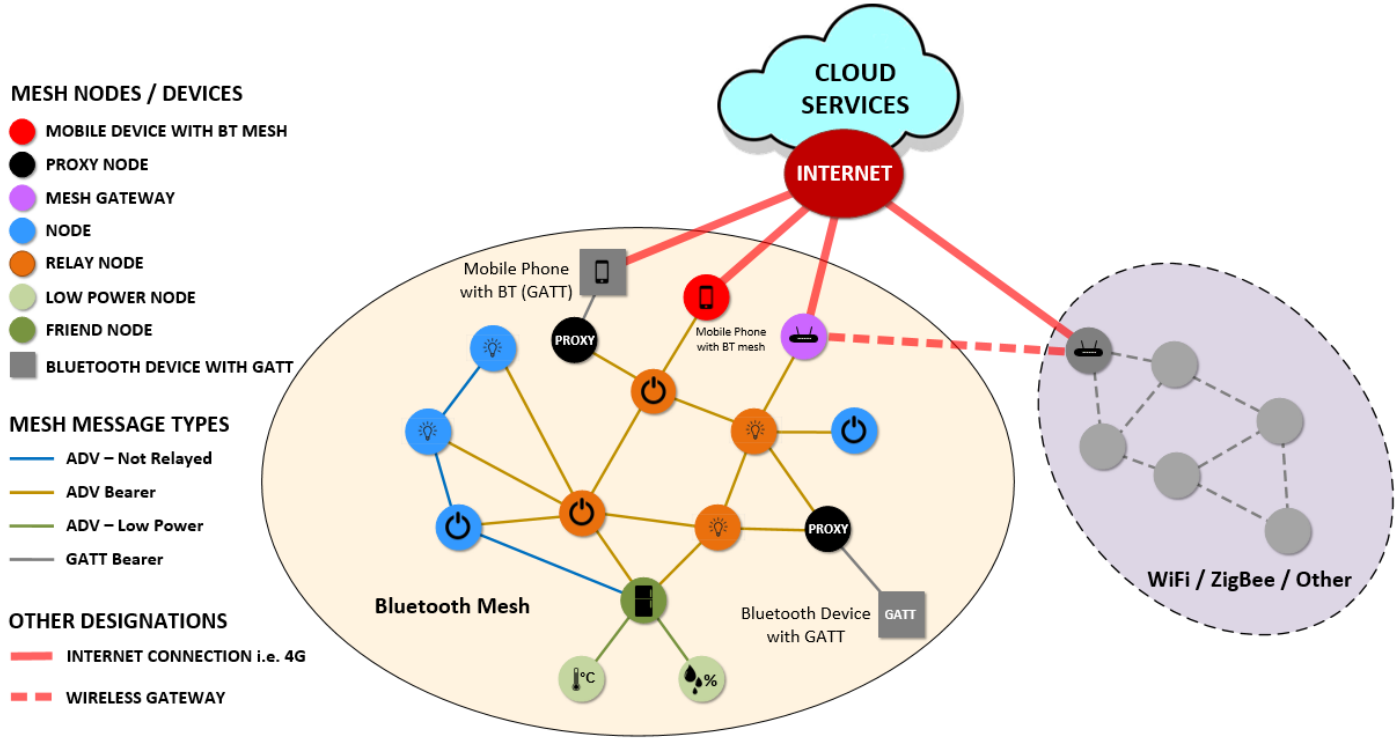
Bluetooth Mesh – Proxy Nodes

- Proxy nodes receive and retransmit mesh messages between GATT and Advertisement Bearers
- Proxy nodes are used to enable the use of older Bluetooth devices as part of a Bluetooth mesh network
- The prerequisite here is that the device in question must support Bluetooth GATT functionality



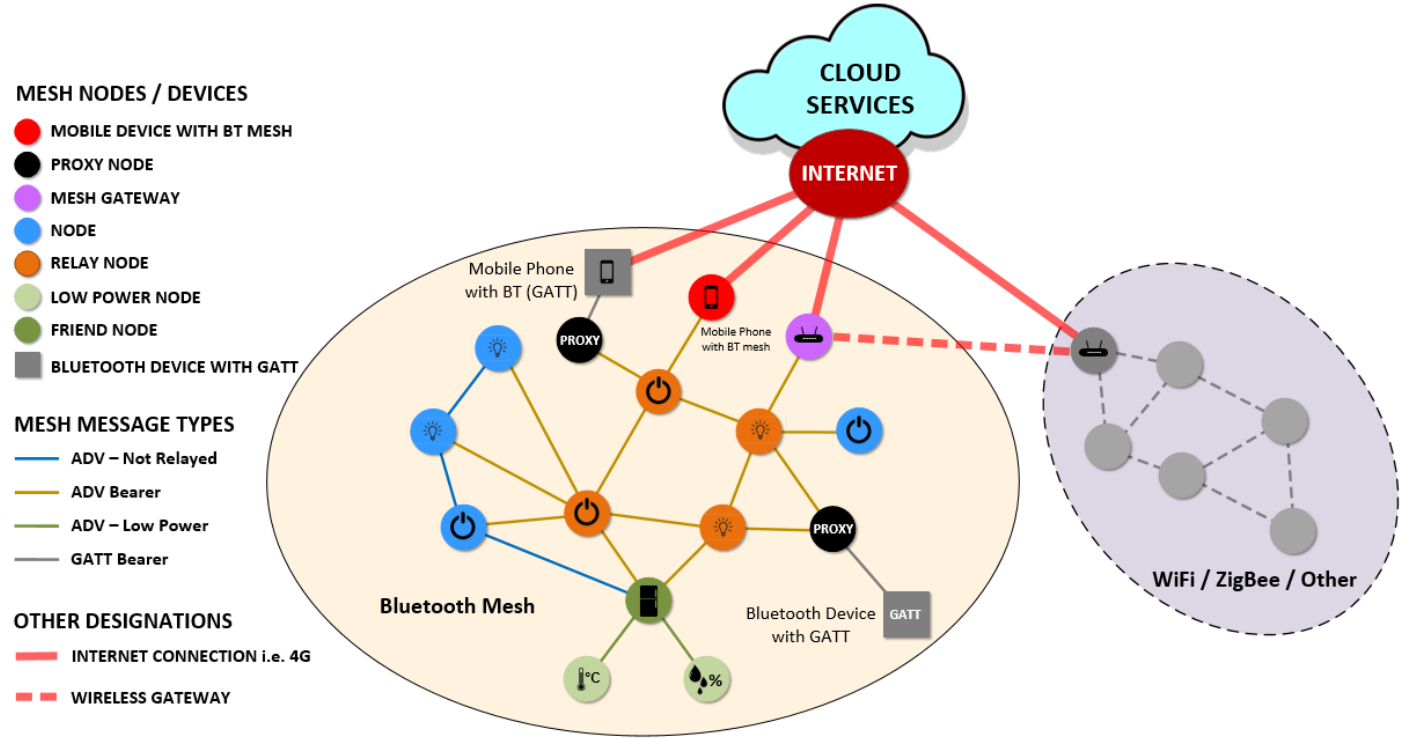
Bluetooth Mesh – Low Power Nodes

- Low Power nodes operate at significantly reduced receiver duty cycle in conjunction with a node supporting the Friend feature
- Low Power nodes are powered typically by battery power or may use energy harvesting methods
- They are programmed to wake up every now and then for receiving buffered messages from a Friend node and for transmitting messages to other nodes in the mesh



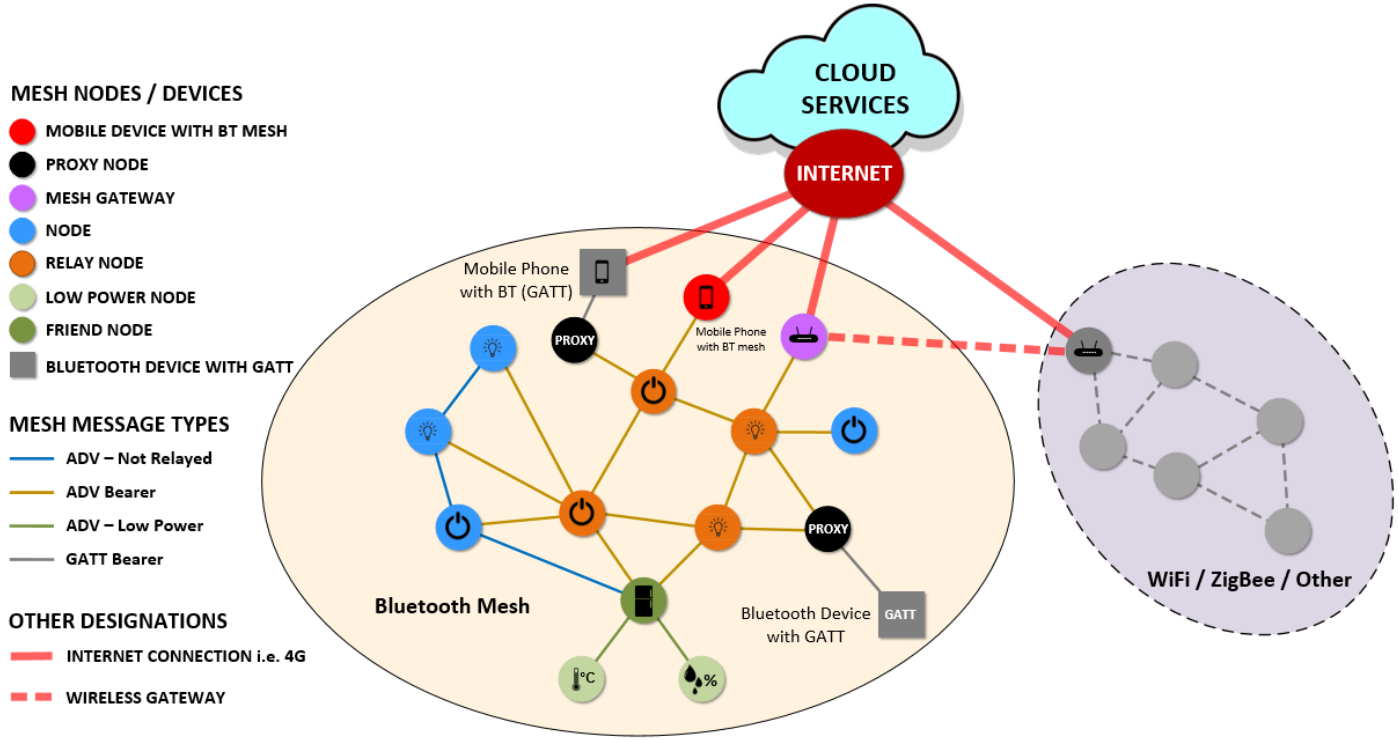
Bluetooth Mesh – Friend Node

- Friend nodes enable low power nodes by storing messages on its behalf (acting as data storage buffers)



Bluetooth Mesh – Gateway Nodes

- Gateway nodes are used between a Bluetooth mesh and a non-Bluetooth wireless network to allow data sharing based on protocol conversion



Bluetooth Mesh - Resources

- What are the resources that all Bluetooth Mesh nodes must have? (ex: what keys)
  - Network Addresses:
    - Identification of message sources and destinations
  - Network Keys:
    - Securing and authentication of messages at the Network Layer
  - Access Keys:
    - Securing and authentication of messages at the Access Layer
  - IV Index:
    - extend or limit the lifetime of the network

Bluetooth Mesh - Resources

- Network Keys and Application Keys both are generated by using a random number generator as defined in the Bluetooth Core Specification
- Both of these keys are shared between nodes
- Application Keys are related to Network Keys and an Application Key is bound to a single Network Key
- Thus, an Application Key is valid only when used with the proper Network Key
  - The application is only valid on this network

Bluetooth Mesh - Resources

- The IV Index field in the network PDU is a 1-bit value which is the least significant bit of the actual IV Index value used in the nonce to authenticate and encrypt the related Network PDU
- IV Index is a 32-bit value shared between all nodes and subnets of a particular mesh network
- If the IV Index is changed on a regular basis, what benefit does it provide to the system?
  - Since IV Index is changed on a regular basis the benefit is that possible obfuscation attacks would need to be started again

Bluetooth Mesh - Elements

- What are elements analogous to in Bluetooth Smart?
- Each node must have at least one defined element called the Primary Element
- Nodes may have one or more additional elements called Secondary Elements
- As long as a node is part of a mesh network the number of its elements remains the same
- The provisioner assigns an address to the Primary Element of the node, and the Secondary Elements are implicitly assigned consecutive addresses
- This unicast address points to the Primary Element of the node
  - Unicast element addresses are used by nodes to identify which element in a node is transmitting or receiving a message

Bluetooth Mesh - Elements

- All elements also have a GATT Bluetooth Namespace Descriptor value to help determine the part of the node the element in question represents
- Namespace descriptor value definitions are the same as in GATT
  - As an example, a temperature sensor has the values “inside” and “outside”.
- This also makes using older Bluetooth devices supporting GATT functionality as part of a Bluetooth mesh network possible

Bluetooth Mesh - Models

- Server Models are compositions of one or more states spanning over one or more elements
- Server Models also define State Transitions, State Bindings and transmittable and receivable messages of elements within the Model
- Server Models define Message, State and State Transition behavior
- What are these similar to in Bluetooth Smart?

Similar to BLE – Service Declaration

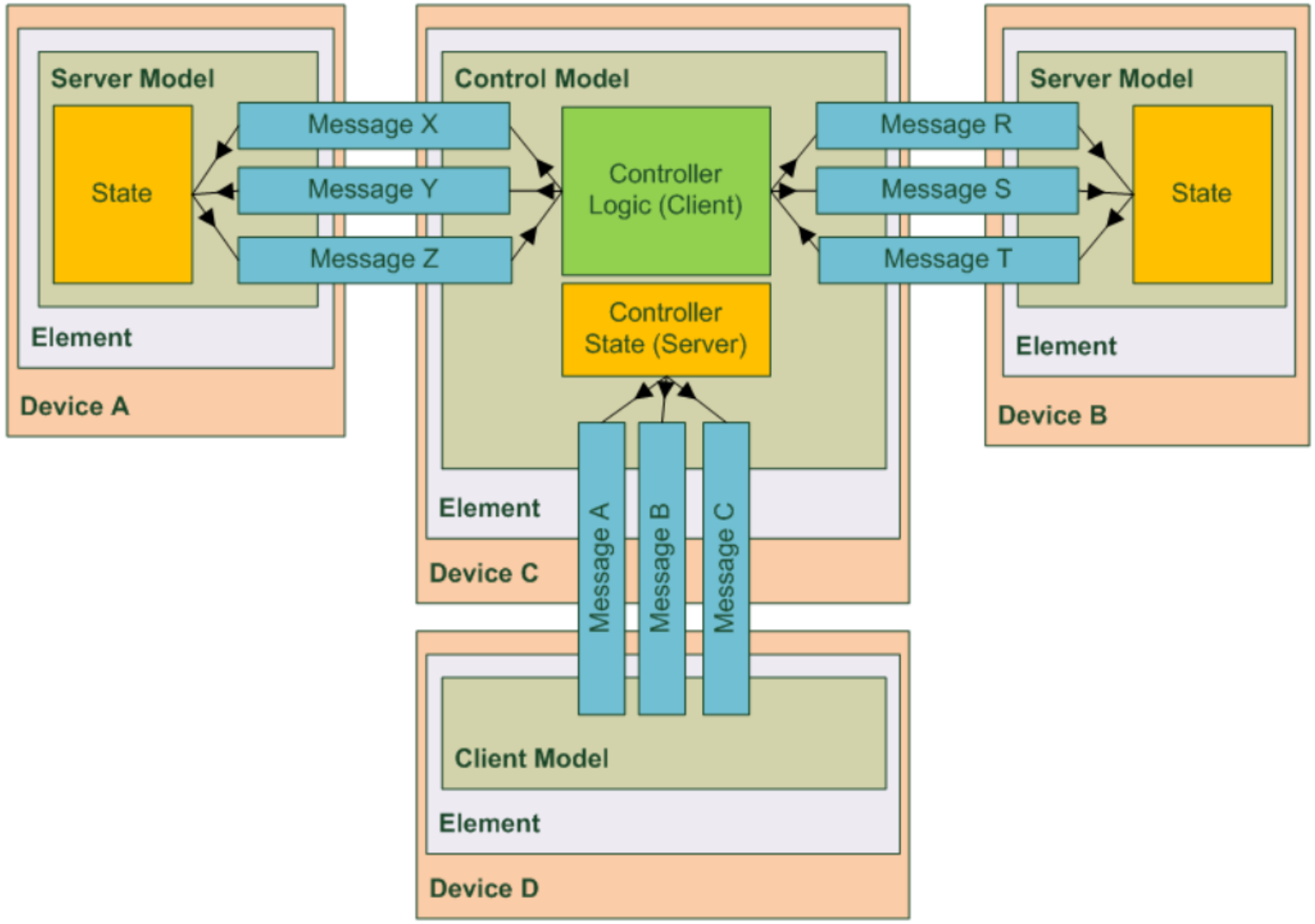
Bluetooth Mesh – Client Models

- Client models do not define any states and define a set of messages, mandatory and optional, used by a Client to request, change or consume related Server states
- Control models are combinations of the above described Models and can therefore contain Client Model functionality for communicating with other Server Models as well as Server Model functionality for communicating with other Client Models
- What are these similar to in Bluetooth Smart?

Similar to BLE – Client Profile

Bluetooth Mesh – Control Models

- Control Models may contain control logic which consists of a set of rules and behaviors for coordinating interactions between other models to which the said Control Model is connected to
- What are these analogous to in Bluetooth Smart?



Control Model communication with Client and Server Models [2]

Bluetooth Mesh - Publish and Subscribe

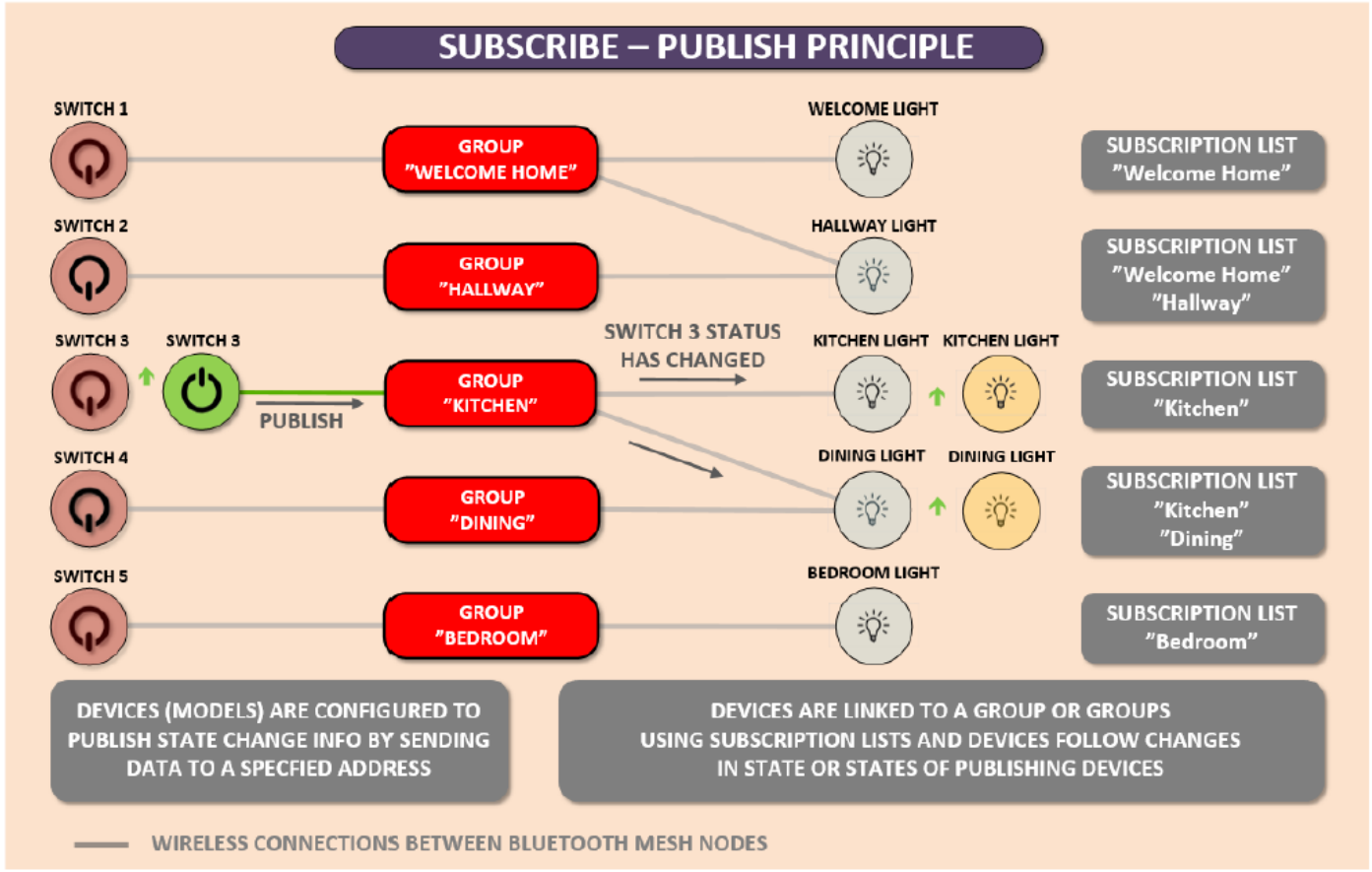
- Bluetooth mesh devices can publish information to multiple devices in the network
- Bluetooth mesh devices can also subscribe to follow information from one or more
- A feature called periodic publishing enables sending messages periodically regardless of whether the state has changed or not

Bluetooth Mesh - Publish and Subscribe

- An example of Bluetooth Mesh publish and subscribe
  - Let us consider a case in which a house has a room with two light switches and two lights
  - Each light needs to be controlled by a switch
  - In this case, the first switch publishes its state light subscribes to the said switch
  - The light that subscribes to the first switch will act accordingly to the published state of the switch
  - The other switch-light pair is managed in similar fashion

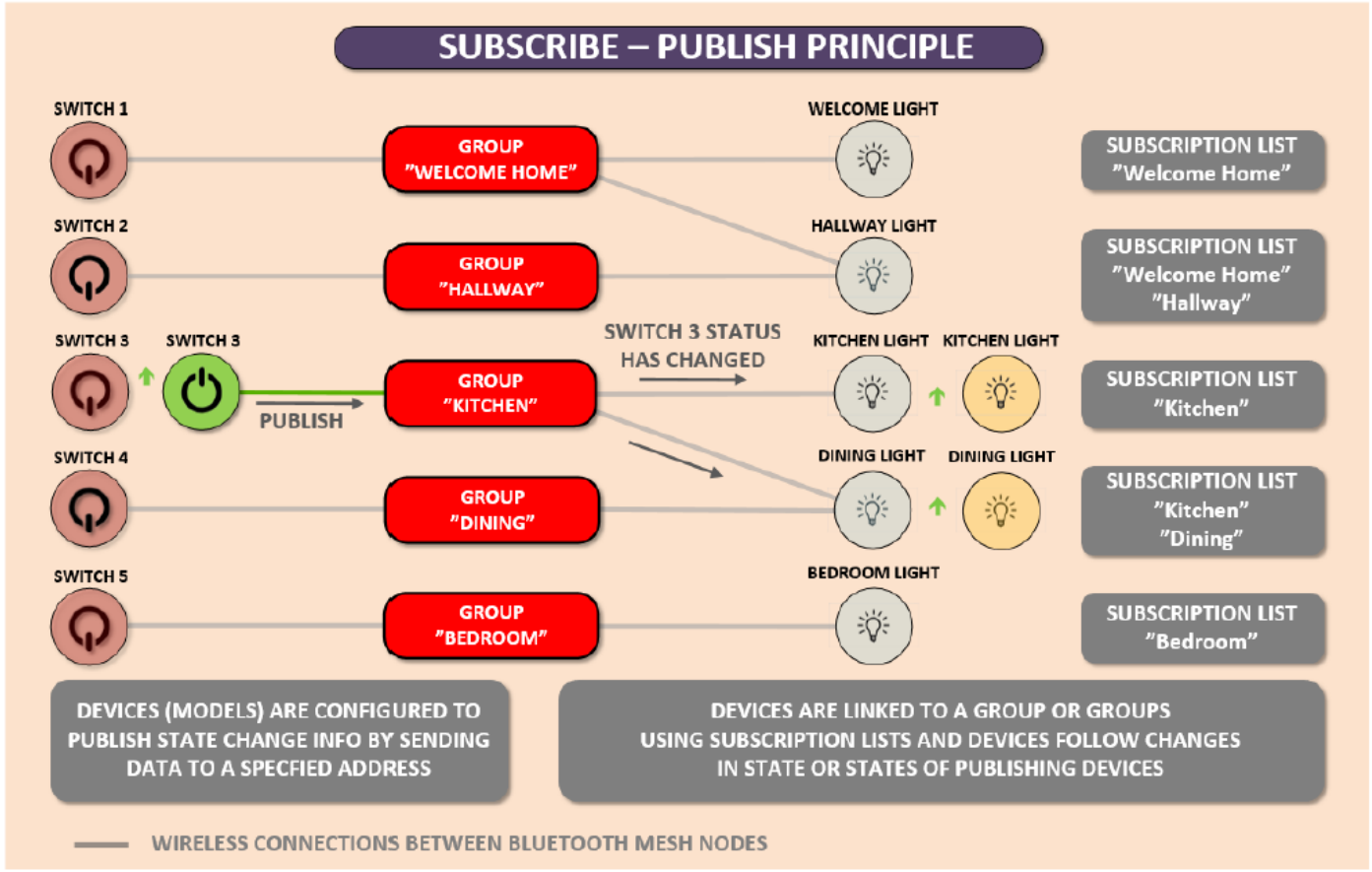
Bluetooth Mesh - Groups

- Let us now consider a more complex case in which a house has five light switches and five lights
- Some of the lights need to be controlled by just a single switch while several other lights need to be controlled by more than just one switch
- This is basically easy to set up but what if a broken switch needs to be replaced or the configuration needs to be changed?



Bluetooth Mesh - Groups

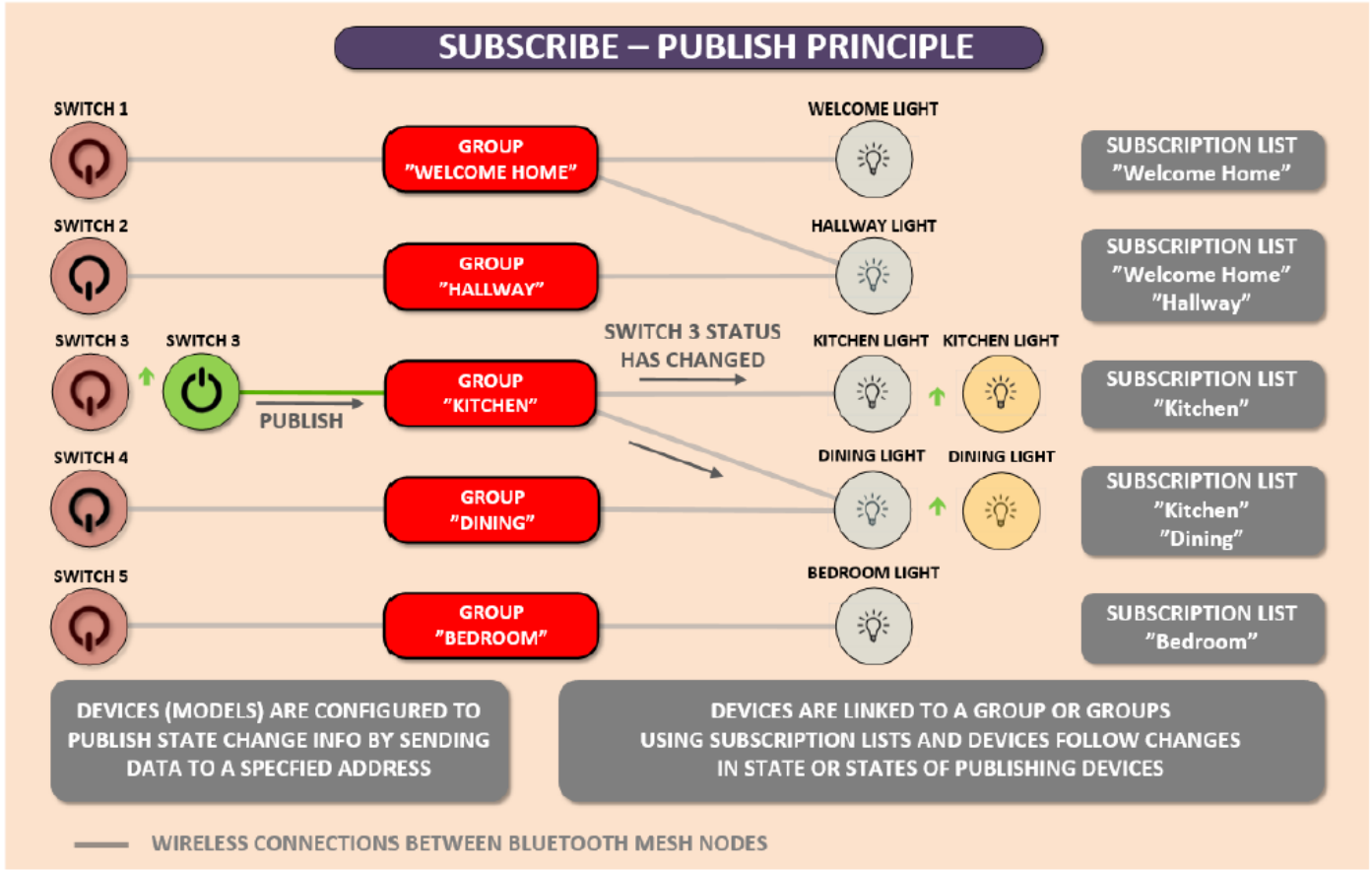
- In BLE, one would need to configure the new switch with all of the addresses of the lights to be controlled by that switch
- In an industrial or large deployment where the number of lights to be controlled increases, BLE could become unpractical
- Bluetooth Mesh solves this by enabling Groups to designate a virtual “switchboard” level
- Now switches can be configured to send their state to a Group and also lights can be configured to subscribe to Groups.



Bluetooth Mesh - Groups

How does Grouping enable Industrial IoT applications?

- Bluetooth mesh configuration becomes much simpler with the replacement switch only needing to be configured to publish data only to the Group instead of a multitude of lights
- Using the Publish-Subscribe principle using Groups
- Messages generated by devices, or more specifically, elements within nodes, send their messages to mesh addresses (unicast, group, or broadcast address) from a single unicast address
- Acknowledged messages will cause a response message while unacknowledged will not



Bluetooth Mesh - Provisioning

- During provisioning network resources are managed and allocated to nodes by a Provisioner
- The Provisioner also allocates node addresses making sure there will be no duplicates of unicast addresses
- Device keys are known only to the device itself and the Provisioner and the device keys are used only during configuration
- The use of multiple Provisioners is allowed but the specifics of cached data sharing etc. need to be defined in the Implementation

Bluetooth Mesh - Device Authentication using OOB

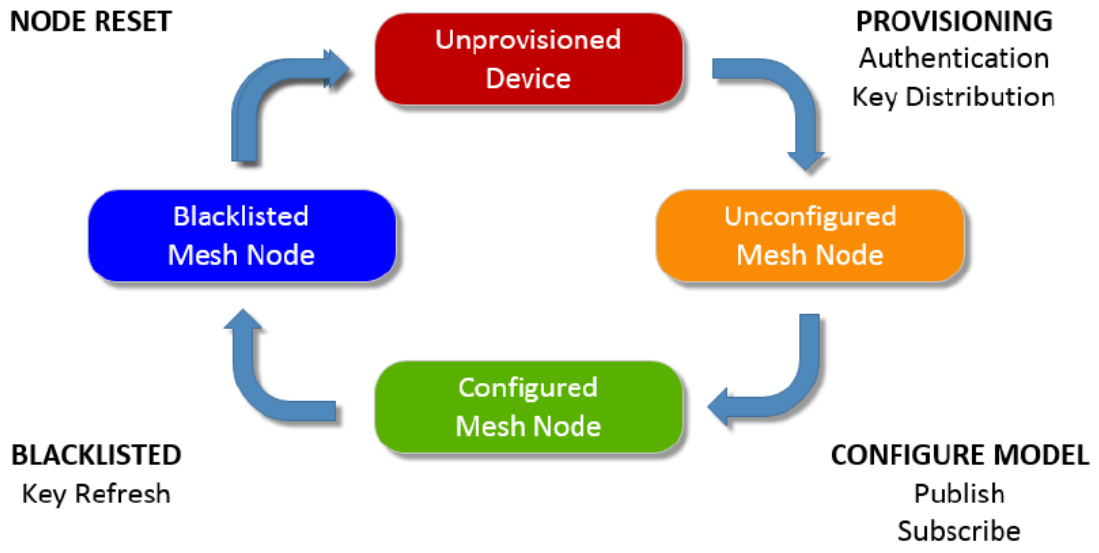
- For secure authentication during provisioning information must be passed between devices without using the actual Bluetooth RF channels, Out-of-Band (OOB) authentication

Method	Description
Input	Provisioner outputs a value – user inputs the value into the device
Output	Device outputs a value – user inputs the value into the provisioner
Out-of-band	Device communicates the value by non-Bluetooth means such as NFC

What is the security advantage of OOB?

Bluetooth Mesh - Lifecycle

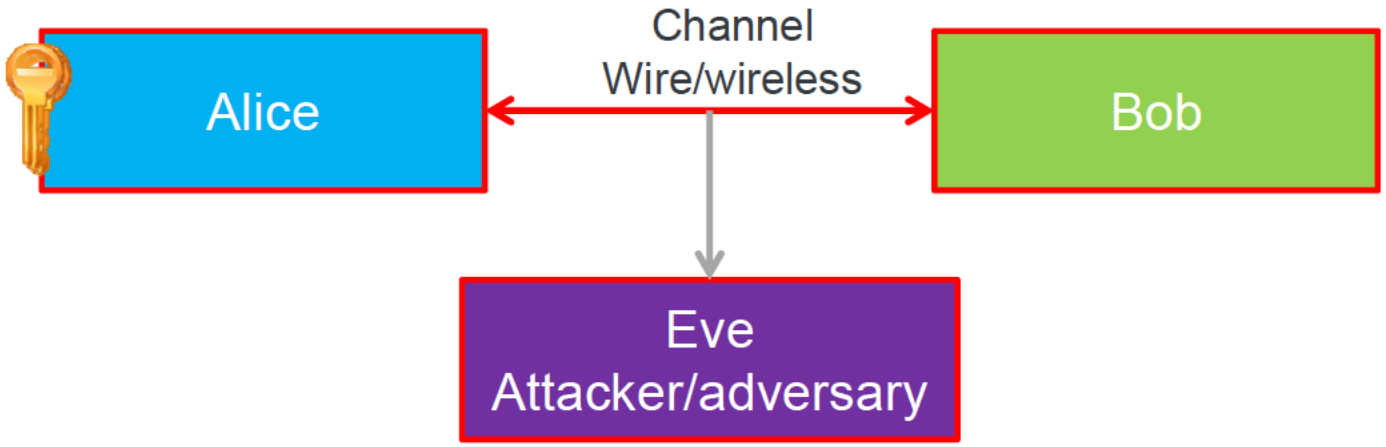
- First the Provisioner must detect an unprovisioned device and establish a provisioning bearer
- Then the Provisioner and the device use the Elliptic Curve Diffie-Hellman (ECDH) anonymous key agreement protocol to establish a shared secret



Bluetooth mesh device lifecycle

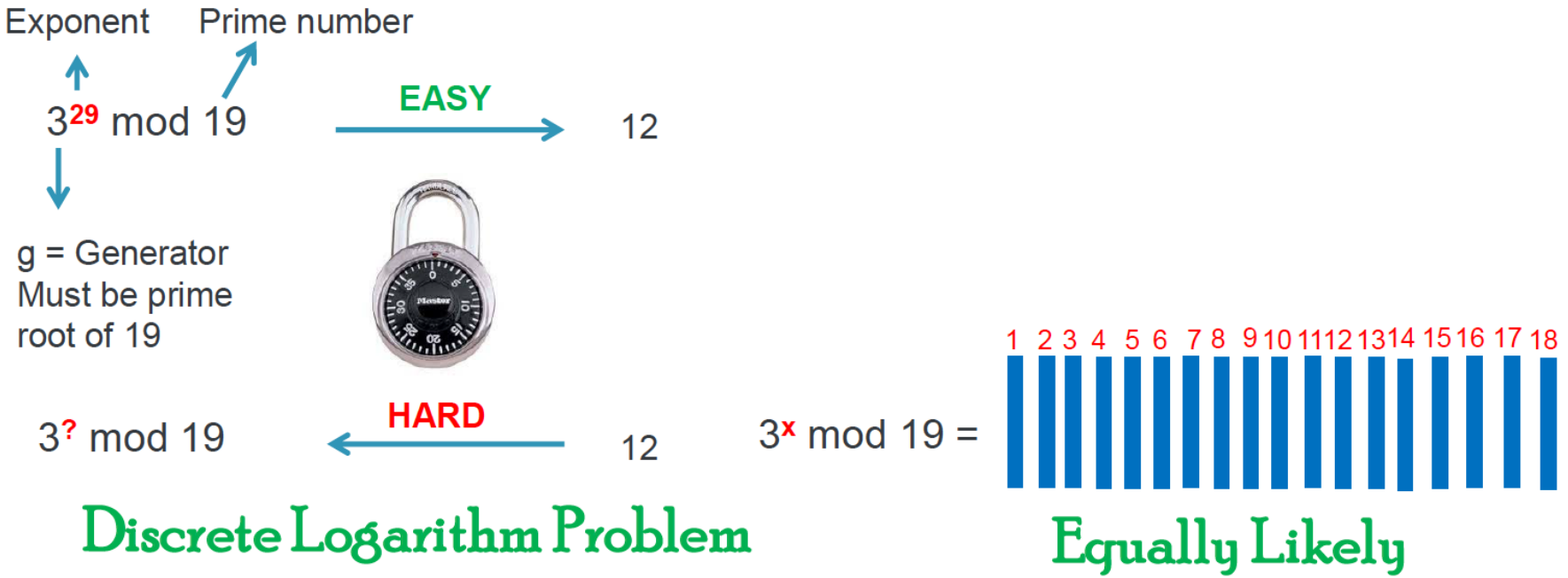
Public Key Cryptography

- Two parties would like to share a secret shared random number (known as a key) in order to transfer data between them
- How could two parties who have never met agree on a secret shared key, without letting Eve who is always listening also obtain a copy?

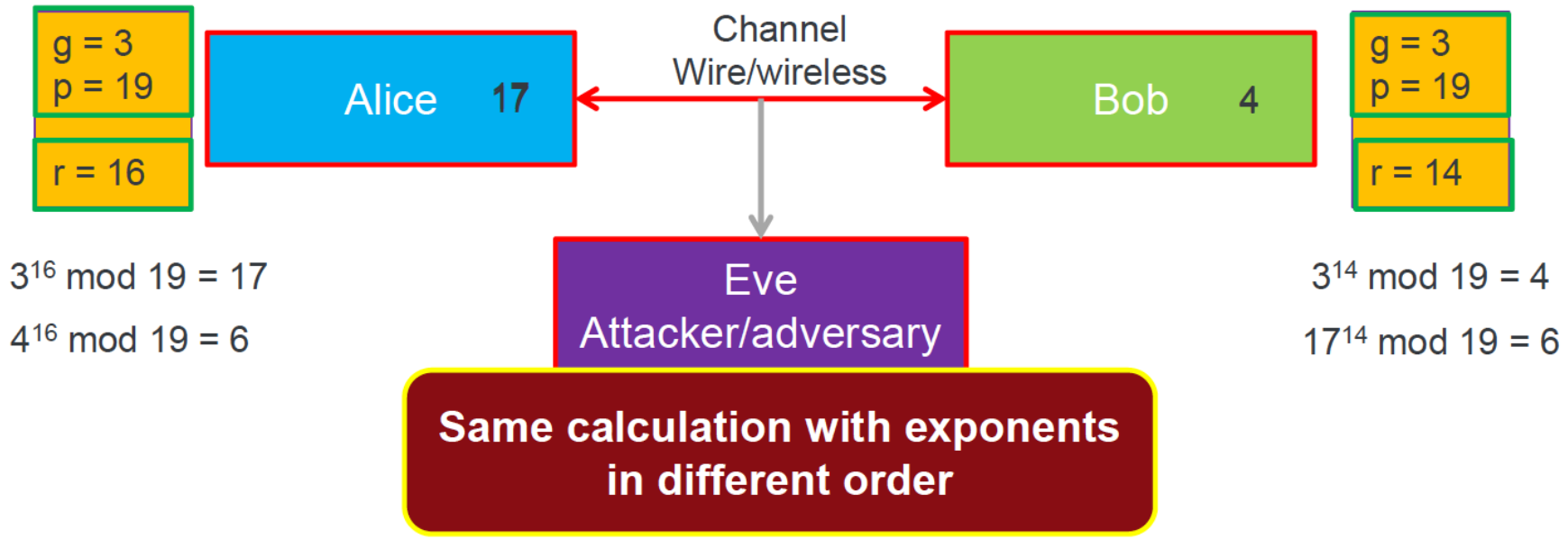


One-Way Function

- In 1976 Whitfield Diffie and Martin E. Hellman advised an amazing trick called the one-way function
  - Numeric procedure that its easy to generate in one direction but hard to reverse
  - Modular arithmetic (x mod p), known as clock arithmetic
  - The strength of the one-way function is the time needed to reverse it (brute force attack)
- This is not an encryption algorithm, only key exchange algorithm



Diffie-Hellman Key Exchange Algorithm



1. Alice and Bob agree **publically** on a prime modulus and a generator
2. Alice selects a private random number, calculate the modulus and sends it publically to Bob
3. Bob selects his private random number, calculate the modulus and send it publically to Alice
4. Alice takes Bob public result and raises it to the power of her random number to obtain the share secret
5. Bob takes Alice public result and raises it to the power of his random number to obtain the share secret

Eve cannot find a solution without the secret numbers!

freescale™ External Use | 94