Bluetooth Security

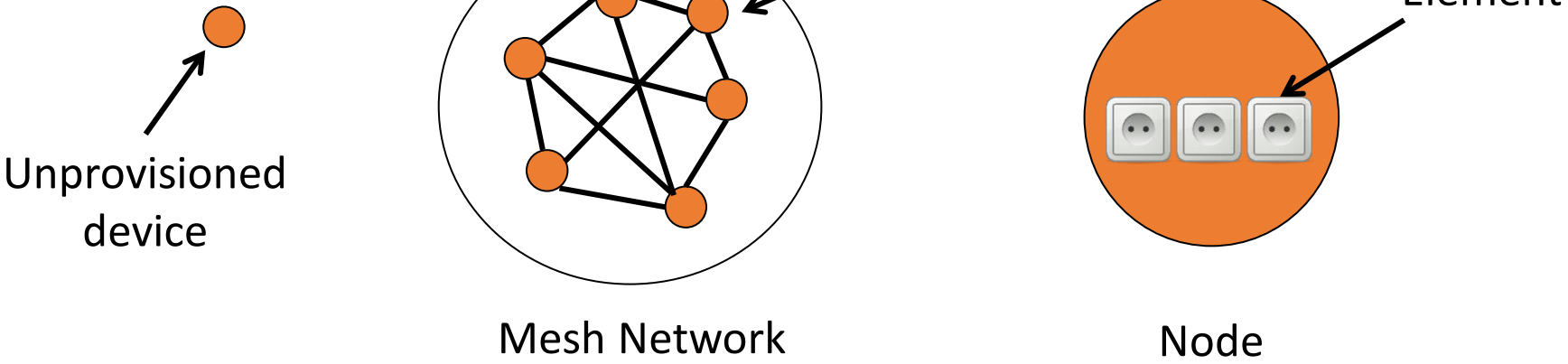
Mohit Sethi
Ericsson, Finland
Aalto University, Finland

Bluetooth Security - Outline

- Part 1:
  - Bluetooth standard evolution
  - Bluetooth stack and protocols
- Part 2:
  - Pairing and Bonding
  - Privacy with Private addresses
- Part 3:
  - Mesh and secure joining

Bluetooth Mesh

- Added in 2017 to support many-to-many topology
  - Builds on top LE and is a profile
  - Utilize advertising: no connections are setup
  - Low-power battery-operated nodes can be supported with Proxy



Bluetooth Mesh

- State: value representing the condition of an element
- Properties: add context to state
- Messages sent in a mesh network with managed flooding
  - Unacknowledged : sent when no response required
  - Acknowledged : message is acknowledged with a response (containing data)
  - get: get state of a peer element
  - set: set state of a peer element
  - status: sent in response to a get/acknowledged set or time intervals

Bluetooth Mesh

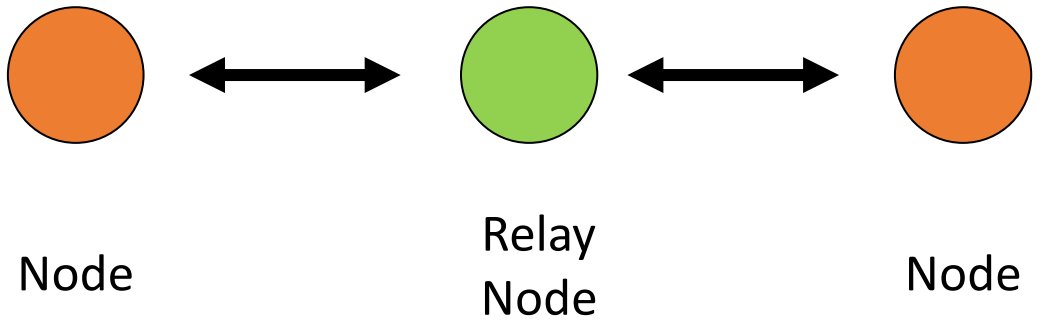
- Address: messages sent in a mesh must have source and destination
  - Unicast address: message sent to a particular node
  - Group address: identifies a group of nodes (SIG fixed or dynamically). Several group addresses within a mesh network
  - Virtual address: multicast address for multiple elements on one or more nodes
- Bluetooth mesh uses publish/subscribe paradigm

Bluetooth Mesh

- Model: defines functionality. Applications are defined with models instead of profiles:
  - Server model: states, state transitions, messages which element can send or receive
  - Client model: defines messages such as get/set/status sent to server
  - Control model: contain client and server model and defines interactions with other devices containing client/server models
- Scene: collection of states. One action to set multiple states of different nodes

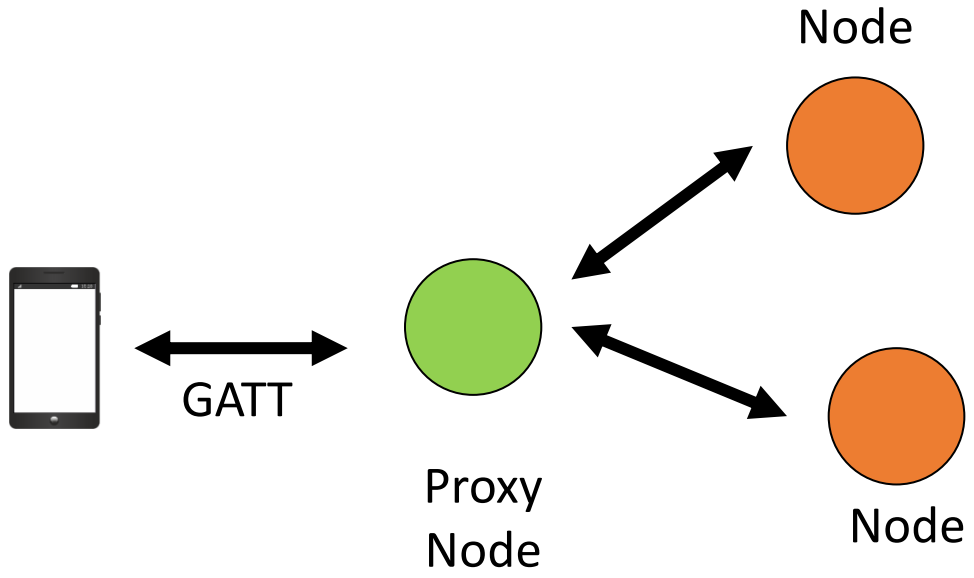
Bluetooth Mesh

- Nodes can support optional functionality:
  - Relay: able to forward messages that are broadcast. Necessary for messages to traverse the network. Time to live (TTL) controls relaying behavior.



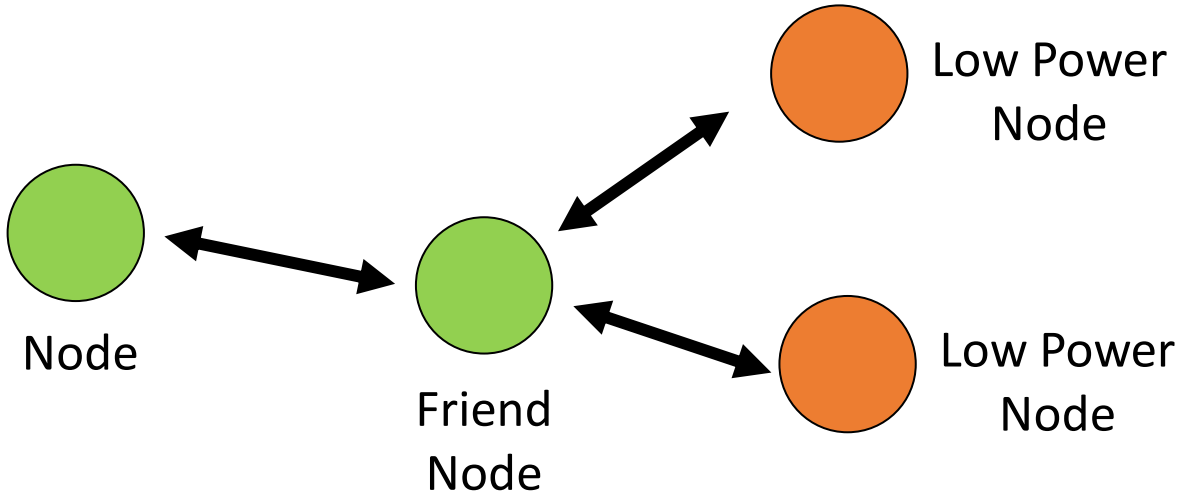
Bluetooth Mesh

- Nodes can support optional functionality:
  - Proxy: exposes a proxy service with GATT. Allows non-mesh device to interact with the mesh network



Bluetooth Mesh

- Nodes can support optional functionality:
  - Low-power: resource-constrained. Sleep most of the time and send data on wakeup. Polls friend nodes on wakeup
  - Friend: not resource-constrained. Caches messages for low-power nodes



Bluetooth Mesh - Provisioning

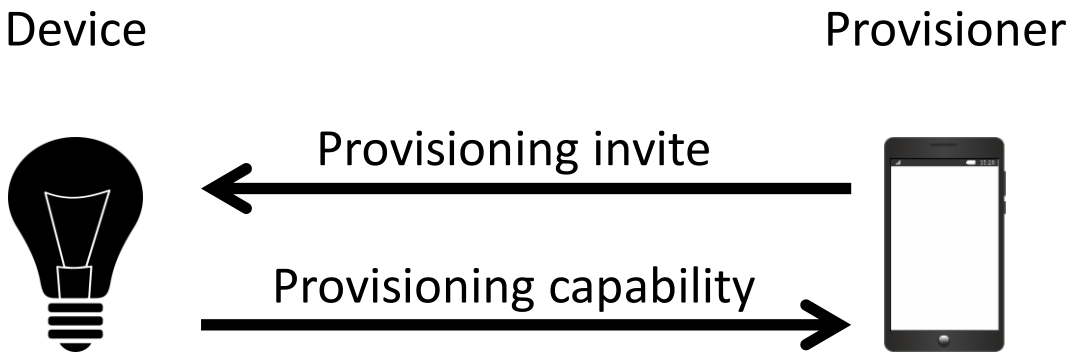
- Provisioning: adding a new device to the mesh network
- Provisioner: smartphone for provisioning new devices
  - Beaconing: unprovisioned device sends advertisements to indicate that it is waiting to be provisioned

Unprovisioned device

Provisioner

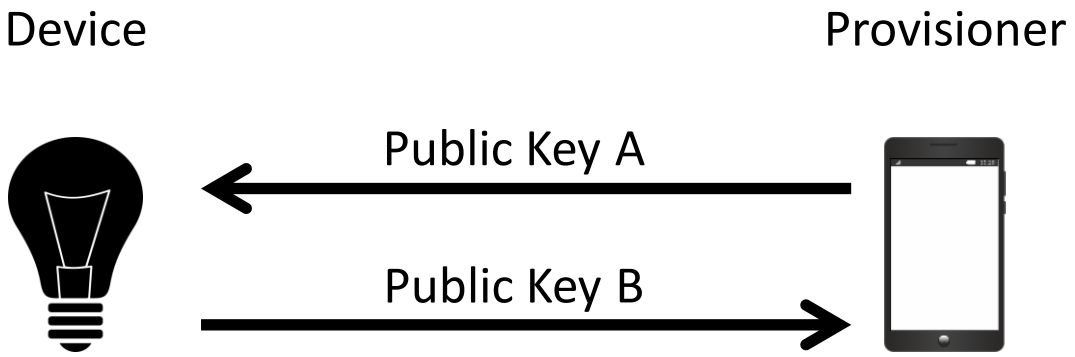
Bluetooth Mesh - Provisioning

- Provisioning: adding a new device to the mesh network
- Provisioner: smartphone for provisioning new devices
  - Invitation: provisioner discovers new device via beacon and sends an invitation. New device responds with provisioning capabilities (including elements, security algorithms, I/O capability etc.)



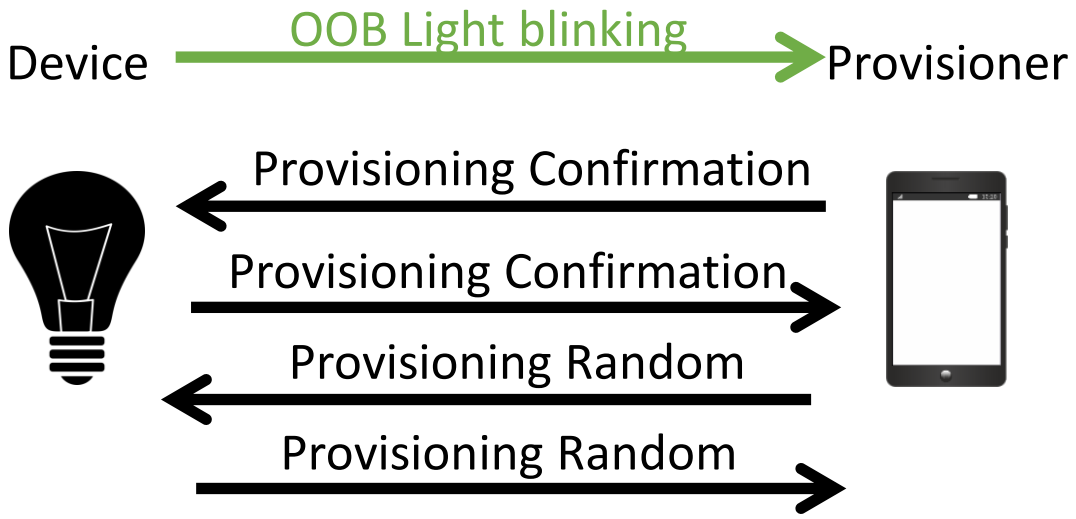
Bluetooth Mesh - Provisioning

- Provisioning: adding a new device to the mesh network
- Provisioner: smartphone for provisioning new devices
  - Public key exchange: ECDH key exchange with fresh keys (or static for device, i.e. printed on a sticker)



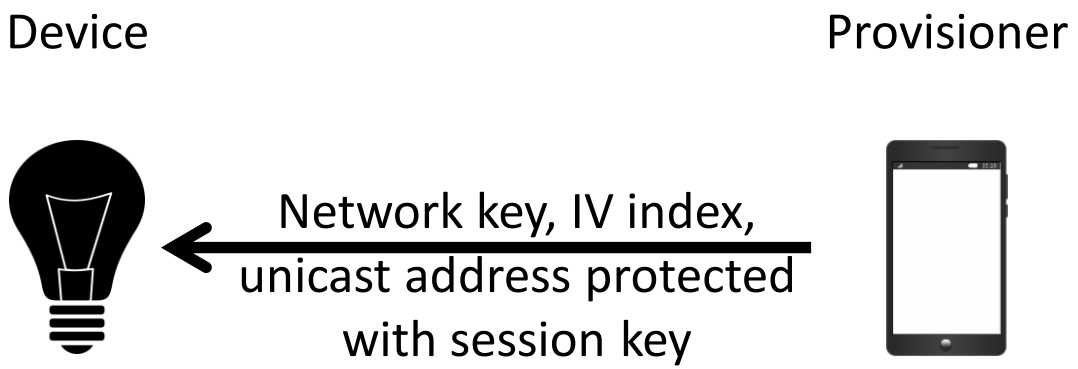
Bluetooth Mesh - Provisioning

- Provisioning: adding a new device to the mesh network
- Provisioner: smartphone for provisioning new devices
  - Authentication: Device or Provisioner generate and show a random number (as blinking LED, audio etc.) that is input on the other side. Both send commitments with random number and reveal random numbers after. Generate session key.



Bluetooth Mesh - Provisioning

- Provisioning: adding a new device to the mesh network
- Provisioner: smartphone for provisioning new devices
  - Distribution of provisioning data : Provisioner sends data: network key, IV index, unicast address assigned etc.



Bluetooth Mesh - Security

- Key Separation:
  - Application Key: shared by a subset of nodes in the mesh network, e.g., light bulbs and switches
  - Device Key: shared between device and provisioner for sending network information
  - Network Key: shared by all nodes in the mesh network. Used for deriving network encryption key and privacy key

- Privacy key derived from network key
- Network header including source address obfuscated with this key