AirVibe LoRaWAN Security

Regarding LoRaWAN's security architecture, which has multiple layers of protection:

1. Device Authentication and Activation
LoRaWAN uses two methods for device activation:
- Over-The-Air Activation (OTAA) - The more secure method, **which we use,** where:
  - Each device has a unique DevEUI (like a MAC address)
  - AppEUI identifies the application
  - AppKey is a unique AES-128 root key

- There is also another activation method, **which we do not allow with our products**.
-Activation By Personalization (ABP) - Less secure but simpler:
  - Device Address (DevAddr)
  - Network Session Key (NwkSKey)
  - Application Session Key (AppSKey)

2. Message Security
- Each message is encrypted using AES-128 with the AppSKey
- Message integrity is protected by a 4-byte Message Integrity Code (MIC)
- Frame counters prevent replay attacks
- Messages use different keys for network operations (NwkSKey) and application data (AppSKey)

3. Protection Against Unauthorized Devices
The gateway cannot accept data from unauthorized sensors because:
- Each device must complete the activation process
- Without valid keys, devices cannot generate valid MICs
- The Network Server validates each message's MIC before processing
- Frame counters detect duplicated or replayed messages

4. Anti-Spoofing Measures
To protect against radio analysis and spoofing:
- All payloads are encrypted
- Each message has a unique MIC
- Session keys are unique per device
- Frame counters increment with each message
- Join requests use random numbers (DevNonce) to prevent replay

Even if someone captures LoRaWAN packets via radio:
- They can't decrypt the payload without the AppSKey
- They can't generate valid MICs without the NwkSKey
- They can't join the network without the AppKey
- Replay attacks are prevented by frame counters

The security is end-to-end, meaning even the gateways don't have access to the application payload - they only forward the encrypted data to the network server.

Revision #1
Created 12 February 2025 16:50:15 by Bach_L
Updated 12 February 2025 16:53:11 by Bach_L