LoRaWAN &

The Things Network (TTN)

A Global IoT Community Network

IETF 106 GAIA

These materials, originally developed by Jonathan Brewer for nsrch.org, are licensed under the Creative Commons Attribution-NonCommercial 4.0 International license (http://creativecommons.org/licenses/by-nc/4.0/)
What is LoRa?

- PHY Radio Protocol for the Internet of Things
- Operates in sub-GHz ISM bands worldwide
  - 433, 470-510, 779-787, 863-870, 902-928 MHz
- Derivative of Chirp Spread Spectrum
- Proprietary to Semtech
- Designed for long range, low power, low data rate
- Star topology (not mesh or p2p)
- 250 bits per second to 22 kilobits per second
  - depending on channel width & modulation
What is LoRaWAN?

• Wireless Network for the Internet of Things
  • Open, non-proprietary standard
• Adds addressing, mobility & localisation to LoRa
• Multiple base stations can receive & process packets
• Adaptive data rate scheme to improve performance
• Multiple levels of encryption (Network & Application)
• Supports time slot scheduling of device transmission
LoRaWAN Entities
LoRaWAN Architecture Overview

- Based on RFC 8376 (Ed. Stephen Farrell)
  - https://datatracker.ietf.org/doc/rfc8376/
- Verbatim text is italicised
- Important terms are bolded
- RFC8376 detail ends with OTA join process
LoRaWAN: End Device

• a LoRa client device, sometimes called a mote
  • Also sometimes called a node

• Communicates with gateways
  • And never with other motes or nodes

• Has a globally unique identifier called DevEUI
  • In the format of an IEEE EUI64 (64 bit)

• Has a network unique identifier called DevAddr
  • Only network unique 32 bit
LoRaWAN: End Device

Size: 55mm x 20mm x 3.5mm

Operating temperature: -40 to 85 degrees celsius

ESP32 Dual Core Microcontroller and WiFi/Bluetooth 4.2 radio

3V3 Ultra-Low Noise switching regulator

LoRa transceiver

32Mbit flash memory

WS2812 RGB multi-colour LED

External LoRa antenna connector

Reset switch

RF switch U.FL connector

Internal WiFi and Bluetooth Antenna
## LoRaWAN: Device Classes

<table>
<thead>
<tr>
<th>Class A (lowest power)</th>
<th>ALOHA based, with comms always initiated by end device. After transmit, device listens for replies or network control for a short time period.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class B (deterministic downlink)</td>
<td>Supports Class A transmissions, plus periodically listens for network messages on a schedule. Still suitable for battery use, but less efficient than Class A.</td>
</tr>
<tr>
<td>Class C (lowest latency)</td>
<td>Supports Class A transmissions, plus actively listens for network messages. Not suitable for battery use.</td>
</tr>
</tbody>
</table>
LoRaWAN: Gateway

- A radio on the infrastructure side
- Sometimes called a concentrator or base-station
- Communicates with end devices via LoRaWAN
- Communicates with a network server via TCP/IP
- Can co-exist on multi-protocol base stations
- Typically runs a software instance per gateway radio
LoRaWAN: Gateway
LoRaWAN: Network Server (NS)

- The Network Server terminates LoRaWAN MAC layer
- for End-Devices connected to the network
- It is the centre of the star topology
- The Network Server decides:
  - which Gateway will talk to which End Device
  - what data rates will be used by End Devices
LoRaWAN: Network Server (NS)
LoRaWAN: Join Server (JS)

- *Server on the Internet Side of a Network Server*
- *Processes join requests from end-devices*
- End devices cannot be used without joining a network
- Often combined with the Network Server
LoRaWAN: Uplink Message

- *Communications from end devices to the network server or application*
- *Received via one or more gateways*
- Uplink Messages received by more than one gateways are de-duplicated by the Network Server
LoRaWAN: Downlink Message

• *Communications from network server or application*

• *via one gateway*

• *to a single end-device*

• *or a group of end devices*

• Network Server decides which gateway is in the best place to send a downlink message to a particular device.
LoRaWAN: Application

• Application layer code running on the end device
• Application code running “behind” the network server
• Most end devices will run only one application
• Identified by a registered IEEE EUI64 value (AppEUI)
• “Applications” typically run on Network Servers
  • Provide for device management
  • Route data to external applications
• Misleading name: Could be called application router
LoRaWAN: Encryption

• *All payloads are encrypted*
  • No possibility for attackers to read payloads
  • No possibility for network operator to read payloads

• *and have data integrity*
  • No possibility for changing data in flight
  • No possibility for intercepting & replaying data

• *MAC commands are protected (except frame options)*
  • No possibility for attackers to read metadata
LoRaWAN: Pre-Joined Devices (ABP)

• *End devices must have two symmetric session keys*
• Devices are personalised with AES 128-bit keys
• Network Session Key (**NwkSKey**)
  • Known only by the network operator
  • Protects network metadata
• Application Session Key (**AppSKey**)
  • Common to all End Devices using an Application
  • Known only to the Application Operator
LoRaWAN: Over the Air Join (OTAA)

- *End devices must have two symmetric keys*
- Network Session Key (**NwkSKey**)
- Application Key (**AppKey**)
  - Different from the **AppSKey**
  - Unique to every End Device
- Device sends **DevEUI**, **AppEUI**, and **AppKey**
- Network sends data allowing Dev to derive **AppSkey** and **NwkSKey** (then proceed as a pre-joined device)

What is The Things Network (TTN)?

- TTN is a free, distributed, LoRaWAN platform
- It provides a Network Server, Join Server, and Application Servers
- Web platform allows gateway owners to create coverage
- And application owners to register devices
- All gateways process all traffic!
- TTN helps communities organise & communicate too.
Where is The Things Network (TTN)?
TTN Console Views
TTN Integrations

- MyDevices v2.6.0
- OpenSensors v2.4.0 The Things Industries B.V.
- TTN Mapper v2.7.1 JP Meijers
- AllThingsTalk-Maker v2.3.0 AllThingsTalk
- COLLOS v2.7.10 Sen-tech Corporation
- Data Storage v2.0.1 The Things Industries B.V.
- TagoIO v2.7.5 TagoIO
- ThingSpeak v2.7.14 MathWorks®
- Ubidots v2.7.10 Ubidots
- EVERYTHING v2.6.0 EVERYTHING
- HTTP Integration v2.6.0 The Things Industries B.V.
- IFTTT Maker v2.6.0 The Things Industries B.V.
LoRaWAN & TTN Device Ecosystem

Devices from https://lpwanmarket.com/