**AGENDA**

* LoRa
* LoRaWan
* Security
* Devices
* Gateways
* Getting Started

**LORA**

* Lora is complementary to existing IoT communctation technologies
* Range, power consumption, data rate
* *Lora modulation (sender side) use a chirp spread-spectrum modulation*
  + Bandwith in which the communication symbols are modulated
  + There is a center freq. which has symbols that are modulated
  + 8 up-chrips -> preamble
  + 2 down-chrips -> synchronization
  + 5 up-chirps -> data
* *LoRa demodulation (receiver side)*
  + Demodulation process is
    - Dechirping
    - spectral analysis
* *bidirectional communication*
  + simple demodulation process -> end-devices
  + LoRa devices and gateways -> modulator-demodulator modules
    - Uplinks (transport from end device to gateway)
    - Downlinks (gateway to end device)
* *Spreading factor (sf)*
  + Orthogonality: improving efficiency and throughput
  + Indicates the number data bits per second the symbols that are modulated per time unit (higher the sf the slower the communication is)
  + Increasing the sf increases the time it takes to send a message
  + Lower sf has shorter range and less time to send a message, higher data rates
  + ALWAYS A TRADE OFF NO SINGLE BEST SF
* *LoRaWan has Adaptive Data Rate Mechanism to deal with sf*
  + Choosing the best SF based on link budget requirements (particular scenario)
  + This is an algorithm that can mesasure the signal to noise ratio and based on this the network can instruct an end device to change the data rate (dynamically)
* *Doppler effect*
  + Frequency shift due to mobility
  + LoRa device moving from or towards the gateway
    - Completely negligible in conditions of low data rates and high spreading factors
    - Not insignificant for high data rates
  + When device moves really fast away/towards from gateway, so can install lora on moving objects
* *Summary: key LoRa modulation properties*
  + Long range
  + Low power consumption
  + Enhanced network capacity
  + High robustness
  + Multi-path and fading resistance
  + Doppler shift resistance

**LoRaWAN**

* Is a communications protocol that can be used on top of LoRa
* Has different types of regions where lorawan can be used, freq to use and limitations etc etc
* *Device Classes*
  + Class A
    - Implemented by all end devices end device initiates transmission
    - End device can send message any time
    - Used by devices that are measuring things like sensor nodes
  + Class B
    - Beaconing, beacon is by network on fixed interval by gateways and the end device can pick up this beacon and wake up to receive a downlink message
    - Class b devices are in deep sleep but wake up on a time interval and listen for traffic on network
    - Not as low power as class a communication
    - Allows the network to send a message to the end device even tho the latency is sometimes tens of seconds or minutes
  + Class C
    - Continuous downlink, end device is continuous listening for downlink messages
    - Allows the network to send message to the end device at any time
    - Typically this is temporary mode for end device (temporarly listening to downlink messages)
* *Limitations of LoRaWAN*
  + Limited payload – 51 bytes to 241 bytes (depending on data rate)
    - Simply binary encoding mechanism for payload so don’t send any text, json, xml messages be mindful of bits and bytes end device is sending
  + Low data rates – max 5.5 kbps on 125 kHz bandwidth
    - Transmission is quite slow
  + Region-specific rules, i.e
    - Duty cycle restrictions in EU
    - Dwell time restrictions in US
  + Asynchronous communication – more uplink than downlink capacity
    - Gateway is also a device that has to comply with spectrum regulations so the gateway also has a duty cycle
* *Is LoRA PHY secure*
  + Physical layer does not provide security mechanisms
  + Optional CRC field – helps detecting transmission errors
  + Lorawan provides 3 pillars of security
    - Authenticity
      * You know with which devices you are communicating with
    - Integrity
      * The data that is being sent and received is not tampered with you know for sure who sent the message but also that the message hasn’t changed by an intermediate party
    - Confidentiality
      * You can encrypt the data
* *LoRaWAN two-layer security*
  + Two layer security with AES encryption algorithm:
    - 128-bit NwkSKey
    - 128-bit AppSKey
  + First the network layer security is provided by the network section key
    - Is used for integrity and authenticity
    - Second the application layer security is provided by the application section key
      * Is used for confidentiality
* *LoRaWAN session*
  + Network session – maintained by the end device and the network server
    - Device address (DevAddr)
    - Network session key (NwkSKey)
    - Frame counters (FCntUp, NFCntDwn)
    - MAC state (channels, data rates, etc)
  + Application session – maintained by the end device and the Application server
    - Application session key (AppSKey)
    - Frame counters (FCntUp, AFCntDwn)
  + During one LoRaWAN session:
    - Sessions key don’t change
    - Frame counters are incremented and never reused
* *Two ways to establish LoRaWAN session*
  + Dynamically by joining a network -> **OTAA (over-the-air Activation)**
    - Join procedure performed between the end device and the Network Server (when a device is not on the network it sends a join request and the network server responds to allow the device to join. Performs cryptographic operations)
    - DevAddr assigned to the device, issued by the Network Server security keys negotiated at each activation
  + Hardcoded session -> **ABP (Activation by Personalization)**
    - No need for a join procedure
    - DevAddr and security keys are hardcoded into device
    - Typically more efficient but not as secured bc you can’t change networks throughout the lifetime of the end device.
* *OTAA vs ABP – which one is safer*
  + OTAA
    - New session on every join procedure
    - Supports rekey on every rejoin
    - Join any LoRaWAN network
    - Highly recommended to use OTAA bc there is a new session every time a device joins
  + ABP
    - Fixed session, no join procedure
    - Security keys stored in a persistent memory
    - Preconfigured network
* *Keys in LoRaWAN version 1.0.x*
  + Application key (AppKey) this is the root key generates bottom two keys
    - Application Session Key (AppSKey)
    - Network Session Key (NwkSKey)
* *Keys in LoRaWAN version 1.1.x*
  + There are keys per purpose
  + Application Key (AppKey) One of two root keys used to generate key below
    - Application Session Key (SKey) with the sole purpose of decrypting and encrypting application payload
  + Network Key (NwkKey) two of two root keys used to generate keys below
    - Forwarding Network Session Integrity Check (FNwkSIntKey)
    - Serving Network Session Integrity Key (SNwkSintKey)
    - Network Session Encryption Key (NwkSEncKey)
      * Used to encrypt instructions that are sent to the end device
* *LoRaWAN is secure by design, but implementation matters*
  + Look at video for picture and explanation around min 43
* *Privacy considerations – public (meta)data*
  + Lorawan is a protocol that uses unlicensed spectrum so anyonce can setup a lora gateway and start receiving lorawan traffic even tho payload is encrypted but the metadata is public application and lorawan developers need to mindful of this
  + JoinEUI (AppEUI)
  + DevEUI
  + DevAddr
  + Frame counters
  + Ports
  + Application payload length
  + MAC commands (sometimes
* *Proisioning end devices*
  + You need to program them with a join ui and app ui and share the root key (app key and network key) in a secure way
  + AES – symmetric encryption
  + Root keys need to be shared in a secure way
    - Giving keys to the network operator -> **not recommended** bc you might get locked-in
    - Using a trusted Join Server -> **recommended**
      * Backend service you can use to provision your root keys with and the joint server decides which network is allowed to activate the device on
      * EXAMPLE: Very simple claiming procedure you build the devices you provision these root keys on a join server and then when you sell device you provide proof of ownership so that the owner can claim device and go on joint server to allow the join request
* *Join Server*
  + A dedicated server handling the sensitive part of the device activation in any LoRaWAN network
    - Authenticates Network and Application Servers
    - Stores root keys
    - Generates session keys
  + Using Join Server is recommended for all deployments
* *Other security features*
  + **Link check MAC commands –** checking link quality and availability
    - Be useful to know if devices are still on the network
  + **Data messages confirmation –** know whether a message has been received
  + **Adaptive data rate algorithm –** packet loss reduction
  + **Frame counters –** to avoid replay attacks
  + **Nonces for device activation (DevNonce) –** increment with every join attempt for each JoinEUI
* *Security tips*
  + Be careful not to expose root keys
  + Do not reuse root keys for multiple devices
  + Root keys aren’t based on public information
  + Never reuses nonces for device activation and frame counters
  + Prefer over the air activation (OTAA) over activation by personalization (ABP)
  + **Prefer using a trusted third parted Join Server that is interoperable with any network**
* *Optimization points*
  + Devices should **always** comply to the LoRaWAN specification
  + Avoid unnecessary join requests
  + Be mindful about the frequency of transmitting messages
  + Shorter message -> shorter transmission time -> longer battery life -> more capacity
  + Expect packet loss -> implement forward error correction to account for packet loss
  + Beware of device synchronization
    - Add random jitter to intervals
    - Back-off mechanism; 5, 10, 30 seconds, to 5 minutes, 1 hour etc
  + Use adative data rate (ADR) mechanism for stationary devices
  + Prefer OTAA over ABP
  + Use persistent memory in the end device
    - After a power cycle, the device won’t reuse numbers for security
  + Assume a link loss only after at least 3 missed acknowledgements from the network