Mobile Communication

Exercise Sheet # 3

Cüneyt Erem, Karim Baidar, Gular Shukurova

June 21, 2020

30 of 30

Exercise 1: Basics of LoRa and LoRaWAN

1. Using the lecture material and additional online sources, try to give a brief explanation for each of the elements of a typical LoRaWAN architecture. Specifically, identify for each element of the network architecture the functionality provided by this element.

   (a) **End-devices (nodes):** The endpoints are the elements of the LoRa network where the sensing or control is undertaken. They are normally remotely located. End devices send data through a gateway to the network server only when one or more of their sensors notice a particular change in their environment or when some other event is triggered, such as a timer expiring. After the end device sends the uplink, it "listens" for a message from the network one and two seconds after the uplink before going back to sleep. End devices spend most of their time asleep. During this time, they consume less than one microampere of energy. This power-saving method ensures that applications can achieve a lifespan of 10 to 15 years on a very small battery.

   (b) **Gateways:** Packets broadcast by end devices will be picked-up by one or more gateways within the network**.** Gateways are embedded with a multi-channel and multi-data rate radio-frequency device that can scan and detect packets on any of the active channels and then demodulate the packets. They are connected to power grid and backhaul IP network**.** Gateways are simply passages to the core network and typically have no built-in intelligence. They are placed in different locations to increase network coverage and connectivity quality**.**

   (c) **Network server:** The core network server is the central component of any LoRaWAN network. It carries all the required intelligence to manage the network and dispatch data to other servers. The network server is responsible for:

      i. **Message Routing**: For messages sent from the server to an end device (downlinks), the network server decides which is the best route to send a message to a given end device. Typically, this decision is based on a link quality indication that is calculated based on the Received Signal Strength Indication (RSSI) and the Signal-to-Noise Ratio (SNR) of the previously-delivered packets. Alternately, this decision can be made with respect to the availability of the gateway (is it free to transmit, or has it exhausted it Tx duty cycle?).

      ii. **Network Control:** The link quality can also help the network server decide the best spreading factor (i.e. communication speed) for a given end device. This is the Adaptive Data Rate (ADR) policy, which is managed by the network controller.

      iii. **Deduplication:** Multiple copies of the same data packet may reach the network server via multiple gateways (due to connection between one end device and several gateways). The network server must keep track of these, analyze the quality of the packets received and inform the network controller.

      iv. **Network and Gateway Supervision:** Gateways typically connect to the network server via an encrypted Internet Protocol (IP) link. Similarly, the network usually has a gateway commission and supervision interface allowing the network provider

to manage their gateways, handle breakdown situations, monitor alarms, etc. In addition, the core network communicates with other servers to organize roaming, links to application servers and more.

(d) **Application server:** The Application Server generates and stores the keys used by the End-nodes in the activation process and message encryption. The keys must be stored in a secure way and accessible only by the Application Server, the exception being the network keys (NwkSKey), which have to be transmitted to the Network Server. The payloads received from End-nodes must be validated and sanitized by the Application Server before performing any other operations. The Application Server must implement functions that check if the payload meets a set of criteria (e.g. testing for length, format, range, and allowable characters), accepting only expected payload formats. These techniques are used to provide an in-depth defense at application level. The Application Server employs also an Application Programming Interface (API), which is used for application and End-node management and to expose End-node data. This interface is an important component as it provides access to sensitive data outside of the controlled network area to applications making use of these data. Usually, the API exposes data through a web server. Hence, the web server must implement a secure connection by using Hyper Text Transfer Protocol Secure (HTTPS). ✓

2. In the lecture we have learned about the different parameters which can be set by the user (spreading factor, coding rate, device class, ...). Think about some examples where LoRa devices might be deployed and argue which parameters might be used in this case.

   (a) Smart Fire Evacuation System: a system where Exit Signs integrated with LoRa Technology intuitively help people navigate complex hazardous zones in real-time by indicating the quickest and safest direction out of the premises. In this case a Class C device is required to operate without any latency. Spreading factor should be long for preventing data loss or connection loss. Coding rate also should be long as the integrity is important (wrong information can lead people into hazard zones). ✓

   (b) Smart door locks: we need a Class C device. Spreading factor should be long so it can provide better detectability of command from a remote controller ✓

   (c) Location detector for Alzheimer and Dementia patients: we need a Class A device.

A2) No plot/results 0/20

A3) Code does not work, partially nonsensical, no results −25 25/50