**Internet of Things (IoT) – Day 1 – 07.09.2022**

*Course held by professors from Bialystok University of Technology in Poland,*

*Dr. Grazyna Gilewska & Assist. Prof. Andrzej Zankiewicz,*

*Faculty of Electrical Engineering*

***Concepts***

* ***LoRaWAN technology and its applications in IoT systems***
* *Review of modern LPWAN technologies (Low Power Wide Area Networks)*
* *General information about LoRa and LoRaWAN techniques*
* *Basics of the operation of the LoRa radio interface*
* *Structure and operation of the LoRaWAN network*
* *A survey of LoRaWAN applications in Internet of Things systems*
* *Practical demonstration of using a LoRaWAN network in a simple measurement application*

***Part 1: Introduction to Internet of Things***

***General concept of Internet of Things (IoT)***

* *The IoT describes physical objects (or groups of such objects) with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications network. (****Technical approach****)*
* *Interconnected devices with sensors and actuators more and more invisible existed in the real world with processing and control moved to the virtual world. (****Uses experience approach****)*
* *The IoT compromises many technologies working together to create a seamless link between real and virtual worlds, that generates new qualities and benefits for our technical civilization. (****Philosophical approach****)*

***Review of transmission technologies used in IoT systems***

* *WPAN – Wireless Personal Area Network*
  + *Bluetooth Classic (BR/EDR), Bluetooth Low Energy (BLE)*
  + *Technologies based on IEEE 802.15.4*
    - *Zigbee*
    - *WirelessHART*
    - *6LoWPAN*
    - *IEEE 802.15.5*
    - *Thread*
  + *ANT (Dynastream Innovations)*
  + *WM-Bus*
  + *Z-Wave*
* *LPWAN – Low Power Wide Area Network*
  + *LoRa, LoRaWAN*
  + *Sigfox*
  + *3GPP technologies (mobile cellular services)*
    - *eMTC (LTE Cat M1)*
    - *NB-IoT (LTE Cat NB1)*
* *WLAN – Wireless Local Area Network – Wi-Fi (IEEE 802.11)*

***Protocols of data exchange***

* *6LoWPAN*
* *CoAP*
* *MQTT*
* *WebRTC*
* *Cloud Services*
* *The http and https protocol*

***Part 2: Foundations of LoRa and LoRaWan***

***What is LoRaWAN***

* *LoRaWAN is an implementation of LPWAN (Low Power Wide Area Network), in which distributed remoted nodes are connected using LoRA radio interfaces.*
  + *LPWAN is a type of wide area network designed for communication over long distances at a low transmission rate with low energy consumption.*

***LoRa***

* *Standard implementation of a single radio link between two points (e.g. between a measuring sensor and a wide area network gateway).*
* *It is a proprietary solution from Semtech company*

***LoRaWAN***

* *A wide area network used for data delivering from end nodes (e.g. measurement sensors) to the user application. Communication from the application to the end nodes can also be available, but usually in a limited form.*
* *The end nodes are connected using the LoRa radio interface.*
* *It is an open specification developed by LoRa Alliance.*

***Typical applications of LPWANs***

* *Data transmission from distributed battery-powered measuring sensors*
* *Transmission from sensor network hubs based on low-range technologies*

***LPWAN******Networks***

*LPWAN networks can be implemented as private networks, as a service or infrastructure offered by operators (e.g. Sigfox network, LTE Cat-M1) and also can operate in a ‘social’ model (e.g. The Things Network)*

***The LoRaWAN System layers***

*The LoRaWAN system includes the following parts (layers):*

* *LoRa PHY – Physical layer protocol*
  + *Proprietary solution from Semtech company*
* *LoRa MAC – MAC (Medium Access Control) layer protocol*
  + *Includes control of shared medium access and logical organization of transmission within the medium (including PDU creation, selection of a frequency channel, selection of transmission rate and power)*
  + *LoRa Alliance is responsible for its development and standardization that ensure mutual combability of devices from different manufacturers.*
* *LoRa over TCP/IP*
  + *It performs the encapsulation of messages from end nodes in IP packets sent over the standard IP network (e.g. Internet) between the LoRa gateway and the network server (LNS – LoRa Network Server), which, among others detect duplicate messages and provides…*

***Operation of the LoRa radio interface***

* *The LoRa technology was developed by Cycleo of Grenoble (France), acquired by Semtech (USA) in 2012*
* *The name LoRa comes from “Long Range” and emphasizes a key feature of the technology.*
  + *Range in urban conditions up to several km*
  + *Range in open space up to several dozen km*
    - *Experimentally,*
    - *a transmission distance over 700 km was obtained*
* *LoRa PHY transmission is a proprietary solution based on patents currently owned by Semtech:*
  + *EP2763321A1 – Low power long range transmitter*
  + *US7791415B2 – Fractional-N synthesized chirp generator*
  + *The information is encoded in the values of the frequency shift (FSK type) between successive chirp pulses*
* *LoRa PHY transmission range*
  + *In radio communication systems, correct signal reception requires that the signal level at the receiver input should not be lower than the value of the receiver parameter defined as its sensitivity.*
  + *The sensitivity of the receiver is the minimum signal power level at its input, at which correct reception is ensured (in the case of digital transmission it means the error rate below the assumed threshold value, e.g. 1%).*
  + *The receiver sensitivity is determined by the equation:*
    - *Rx sensitivity = -174 dBm + 10log10(BW) + NF + SNR, where:*
      * *-174 dBm is the average noise power of an ideal receiver for each 1 Hz of bandwidth at temperature 290K (it is k x T0)*
      * *K – Boltzmann’s constant, T0=290K – temperature value defined by IEEE as close to a typical “room” condition*
      * *BW – receiver bandwidth*
      * *NF – Noise Factor – noise level at the receiver output related to the ideal receiver*
      * *SNR – Signal to noise ratio required for the correct detection*
    - *The higher the SNR, the lower (“worse”) sensitivity of the receiver is and a stronger signal at the input is required for correct reception (that is, for the given transmission conditions and the given transmitter power, the transmission range will be shorter.)*
    - ***Conclusion****: A large transmission range requires the use of a type of detection that requires the lowest possible signal level at the input.*
  + *Proper detection at low signal levels can be provided e.g. by spread spectrum transmission systems.*
  + *They allow to obtain a high value of the so-called maximum link budget defined as the sum of transmitter power and receiver sensitivity.*

***LoRa PHY – Physical layer protocol***

* + *Transmission is realized using the spectral spreading method Chirp Spread Spectrum (CSS)*
  + *CSS uses the so-called chirp which is a sinusoidal pulse with a frequency varying in a polynomial (inn this case linear) manner, being a single modulation symbol.*
  + *Physical transmission can take place at different rates described by the equation:*
    - *Rb = , where:*
    - *Rb – transmission rate (b/s)*
    - *SF – Spread Factor – spectrum spreading factor, in this case also determines the number of bits encoded on one symbol (a single pulse)*
    - *SF – {6 (not used), 7,8,9,10,11,12}*
    - *BW – bandwidth (related to the range of the frequency sweep in the chirp pulse)*
    - *BW = {7,8; 1,4; 15,6; 20,8; 31,25; 41,7; 62,5; 125; 250; 500} (kHz)*
    - *CR – Coding Rate – the ratio of the number of data bits to the total number of bits transmitted in the radio transmission (additional bits are FEC correction codes)*
    - *CR = {4/5; 4/6; 4/7; 4/8}*
  + *A full frequency change range is divided into 2SF intervals (so-called chips)*
  + *The value of the currency transmitted symbol is encoded in the number of the interval from which the frequency sweep begins in the signal transmitting this symbol.*
  + *The signal is created with dependency:*
    - *BW = RC where RC is the chip rate (chips/s) which means that for a given SF, the slope (rate of change of frequency) does not depend on BW.*
  + *Obtaining a high value of the so-called maximum link budget defined as the sum of transmitter power and receiver sensitivity (without sign – the higher the better)*
  + *The radio signal is transmitted in unlicensed ISM bands depending on regional regulations*
    - *Europe: 433MHz, 868MHz*
    - *USA, Australia, Brazil: 915MHz (there are differences from country to country)*
    - *China: 470MHz, 780MHz*
    - *Detailed requirements are specified in the document “LoRaWAN Regional Parameters”*
* *The use of LoRa modulation with spread spectrum CSS method allows for:*
  + *Obtaining a high value of the so-called maximum link budget defined as the sum of transmitter power and receiver sensitivity*
  + *No need to use high-class reference clock (compared to DSSS)*
  + *Avoiding interference when transmitting signals with different SFs in the same frequency channel (signals with different SFs are mutually orthogonal)*
  + *Obtaining high resistance to multipath propagation and fading, which is particularly important in an urban environment*
  + *Low doppler effect (for mobile devices)*
* *Frequencies in EU863-870MHz ISM Band*
  + *These can be chosen by the creator of the network, for example: in The Things Network on the EU863 band, the standard set of channels is quite unique.*
* *ToA – Time on Air*
  + *In the case of LoRa transmission, an important parameter is the time of transmission of a single PHY packet (medium busy time), called ToA*
  + *Compared to other systems (e.g. Wi-Fi), it may be relatively long*
  + *Total ToA is the sum of the preamble transmission time and the PHY layer packet data:*
    - *ToA: = Tpreamb + Tpayload*
    - *Tpreamb = Ts (npreamb +4.25)*
    - *npreamb = the number of preamble symbols (for EU868 it is 8, 4.25 is the number of SFD symbols)*
    - *Ts = 2SF/BW (duration of a single symbol)*
  + *Higher SF means slower transmission and greater range, but also higher power consumption*
* *Use of radio resources (Duty Cycle)*
  + *The Duty Cycle parameter determines the percentage of time that it is taken by a radio transmission. For example, if we transmit for 1 second ever 10th second, it is 10%*
  + *In Europe, the permissible Duty Cycle factor is specified in the Commission Implementing Decision (EU) 2017/1482 of 8. august 2017 amending Decision 2006/771/EC on harmonization of the radio spectrum for use by short-range devices and repealing Decision 2006/804/EC (notified under document C(2017) 5464).*

***LoRa – Data link layer protocol (L2, link layer)***

* *The LoRaWAN specification defines, among others, data link layer protocol (LoRaWAN L2, Link Layer)*
* *LoRaWAN L2 provides logical organization of transmission between end nodes (e.g. sensors) and LoRa gateways.*
* *LoRaWAN L2 features include:*
  + *Encapsulation of transmitted data in frames*
  + *Support for downlink transmission modes*
  + *Management of frequency, power, and bit-rate*
  + *Transmission security*
    - *(AES128-based encryption, authentication)*
* *LoRaWAN defines three transmission classes:*
  + *Class A: Asynchronous communication*
    - *It is a basic class, and its implementation is mandatory on all devices*
    - *The end device spends most of its time in sleep mode*
    - *The end device can start uplink transmission at any time*
    - *After each transmission from the end device to the gateway (uplink), two short transmission windows (about 1s) are opened in the downlink direction (RX1 and RX2)*
    - *The server cannot initiate a downlink transmission*
    - *This is the most energy-saving mode*
    - *If no transmission is received in the RX1 window, the device, after a short sleep period, opens the second window (RX2)*
    - *The device will not initiate another uplink transmission until one of the following conditions is met:*
      * *A message has been received in the RX1 window*
      * *Waiting or transmission in the RX2 window has ended*
  + *Class B: Deterministic delay, synchronous communication*
    - *In addition to the mode as in class A (each device starts from class A), the end device cyclically opens the downlink window after receiving a Beacon message from gateway (thanks to this the server knows when the device can receive data)*
  + *Class C: Lowest delay, highest ability of downlink*
    - *The end device has the downlink window open almost all the time (it is closed only for the time of sending data)*
    - *Implementation is analogous to class A, but the RX2 window is not closed until the next uplink transmission*
    - *Continuous power consumption by receiver*
    - *Class C is useful for updating the firmware of the device (FOTA)*
* *LoRaWAN – Types of messages*
  + *Join-request and join-accept messages – used to activate the device in over-the-air mode*
  + *Confirmed-data – receipt of the message must be acknowledged by the recipient*
  + *Unconfirmed-data – no confirmation of receipt of the message required*
* *The maximum message size (MAC Payload) depends on the transmission mode and ranges from 59 to 230 bytes (up to 250 assuming no repeater is used).*
* *There are four levels of devices in the structure of the LoRaWAN network:*
  + *End nodes*
    - *These are sensors or actuators that communicate wirelessly with the gateway using LoRa radio interface*
    - *During production unique identifiers are saved in end devices, which allow for safe activation of the device in the network and secure communication*
  + *Gateways*
  + *Servers: LoRaWAN Network Servers (LNS), Join Server, Application Server*
  + *Devices with a user interface*
* *LoRa gateway runs a Packet Forwarder process which communicates with:*
  + *LoRa interface circuit (usually through the HAL layer) to send and receive messages and to configure the interface*
  + *LoRaWAN Network Server (via the IP network) to transmit data received from end devices and to receive MAC commands and data for end devices*
* *Packet forwarder is usually provided by the gateway manufacturer or server operator (e.g. The Things Network)*
* *For example on The Things Network platform you can use the following packet forwarder solutions:*
  + *Semtech UDP Packet Forwarder – practically for all types of gateways*
  + *TTN Packet Forwarder – more modern solution, but available for a limited number of gateways – currently development of this software has been stopped*
  + *Semtech Basics Station – a modern solution, available for an increasing number of gateways. In addition to the functionality of communication with the LNS server (via websockets) it also provides remote configuration management and device updates (via CUPS – Configuration and Update Server)*
* *LoRaWAN Network Server (LNS)*
  + *LNS messages the entire network, dynamically determines network parameters depending on the current conditions and sets up an encrypted AES-128 connection between the end device and the application (LNS does not have access to application data)*
  + *Checks the correctness of the frame authentication codes and the frame counter*
  + *Confirms received messages (in confirmed mode)*
  + *Responds to MAC Layer (L2) Request messages from end devices*
  + *Forwards data to the appropriate application servers (uplink)*
  + *Queues data from application servers to end devices*
  + *Forwards join-request and join-accept messages between end devices and join server*

***Security aspects in the LoRaWAN network***

* *Fundamental requirements for secure communication:* ***confidentiality****,* ***integrity****,* ***availability***
* *Security threats in LoRaWAN network*
  + *Wiretapping of communications (sniffing)*
    - *LoRa radio level*
    - *TCP/IP network level*
  + *Unauthorized connection to the network*
  + *Jamming of radio signal*
* *Communication security means included in the LoRaWAN specification*
  + *OTAA, ABP activation procedures (end node authentication)*
  + *Protection of communication integrity between the end device and the LNS server*
  + *Encryption of communication between the end device and the application server*

***Creating a secure communication channel***

* ***Confidentiality*** *can be ensured by encryption -> for symmetric ciphers a common secret (encryption key) must be present on both sides.*
* ***Integrity*** *of communication can be ensured by secure authentication (proving of identity) using:*
  + *A digital certificate issued by an authority trusted by the other side*
    - *PKI infrastructure is required*
  + *Verification of the common secret in a way that makes it impossible to obtain it by a third party (e.g. by eavesdropping on communication): a challenge-response method can be used here, in which party A generates a random request and sends it to party B, which then encodes it using the common secret and sends it back to side A- Side A compares the received response with the self-encoded challenge (or decrypts the response and compares it with the sent challenge)*
    - *Encoding can be realized using encryption algorithm (ciphers) or authentication codes (e.g. MAC, HMAC) based on hash functions.*
    - *Both parties must have a common secret agreed in an authenticated manner.*
* *Secure agreement (exchange) of a common secret can be achieved through:*
  + *Its exchange through a separate secure communication channel (OOB – Out-of-Band):*
    - *E.g. manual configuration on all devices, sending by letter, dictating over the phone and so on.*
  + *Generating the secret by side A, encrypting it with the public key of side B and sending it to side B*
    - *PKI infrastructure is required to validate the public key*
  + *Key exchange using Diffie-Hellman or similar algorithms*
    - *In the version without additional authentication of public numbers, this method is vulnerable to Man-in-the-Middle attack.*

***LoRaWAN – activation of end devices***

* *In order for the end node to become an element of a particular LoRaWAN network, the procedure of its activation must be carried out*
  + *This provides control over which end devices who can join the network and then communicate with specific applications*
* *Activation of end devices in the LoRaWAN network can be carried out in two modes:*
  + *Over-The-Air Activation (OTAA)*
  + *Activation by Personalization (ABP)*
* *Nevertheless of the activation method (OTAA or ABP) this process results in the following parameters gets stored in the memory of the end device:*
  + *Device address (DevAddr)*
    - *A 32-bit address identifying the device on a given network*
    - *It consists of the N-bit network prefix (AddrPrefix, N = 7 … 25) derived from the unique identifier of the LNS server (NetID, specified in the document “LoRaWAN Backend Interfaces Specification”) and the (32-N) bit network address of the device (NwkAddr)*
    - *AddrPrefix allows to identify the LNS that has assigned a given DevAddr*
    - *DevAddr is a non-secret parameter*
  + *Network session key (NwkSKey)*
    - *An individual network key assigned to a given device and its specific session in the network*
    - *NwkSKey is used by LNS and the end device to calculate the Message Integrity Code (MIC) of data sent in frames (it is also used to encrypt data in MAC-only frames with Fport = 0)*
    - *The NwkSKey should be stored in the device in a manner that is protected against unauthorized reading*
  + *Application session key (AppSKey)*
    - *Individual application session key for a given device*
    - *Used by application server and end device to encrypt and decrypt data in application-specific frames*
    - *The AppSKey should be stored on the device in a manner that is secured against unauthorized reading*
* *Activation of end devices using the Over-The-Air Activation method (OTAA)*
  + *The following parameters should be pre-configurated in the end device:*
    - *DevEUI – globally unique device identifier (in IEEE EUI64 format) – non secret*
    - *JoinEUI – a global application ID in the IEEE EUI64 address space that uniquely identifies the Join-Server that is able to assist in the processing of the Join procedure (previously the name AppEUI was used) – non secret*
    - *AppKey – the main key (root key) of the AES-128 encryption algorithm assigned to a given end device – secret*
      * *The same key should be known to Join Server*
  + *OTAA activation process is performed using the Join-Request and Join-Accept messages, which securely (by using the hash function and encryption) connects the device to the network by providing the NwkSKey and AppSKey session keys and the DevAddr.*
    - *In the first step, the device sends the Join-Request message to the Join Server with JoinEUI, DevEUI and DevNonce*
    - *DevNonce is a 16-bit value representing a “counter” of device activation. When initializing the device, DevNonce = 0 is assumed. This value in incremented by 1 with each subsequent activation. Since Join server remembers the current DevNonce value and does not allow activation with lower values, the device should keep the current DevNonce value permanently*
      * *If the device in its life cycles may exceed 65,536 activations, it should be planned to configure many JoinEUIs.*
    - *The frame with the Join-Request message contains the MIC authentication code calculated with the AppKey.*
* *Activation of end devices using Activation by Personalization (ABP)*
  + *NwkSKey and AppSKey and the DevAddr address are statically configured on the device instead of DevEUI, JoinEUI (AppEUI), and AppKey.*

***Over-The-Air Activation (OTAA)***

* *The end device has pre-set parameters that allow for the generation of individual session keys.*
* *Session keys are valid for a given device activation in the network and after its disconnection (or loss of the session context) they lose their validity.*
* *The device may have saved parameters for activation in various LoRaWAN networks.*
* *This is the recommended activation method that provides effective protection against any breach attempts.*

***Activation by Personalization (ABP)***

* *Data (keys) securing communication of the device are permanently stored in it at the production stage and their possible change is difficult to carry out in a safe manner.*
* *One advantage is the immediate network readiness of the device without a separate dynamic activation procedure.*
* *Devices are permanently assigned to a given network (NetID is part of the device address).*
* *It is a simplified, less secure, activation method (e.g. for resource-constrained devices).*

***Part 3: Practical demonstration of creating LoRaWAN IoT measurement application***

***Components***

* *Sensor & End node: Pycom FiPy + Pysense*
* *Gateway: LoRaWAN Gateway*
* *Server solutions: The Things Network*
* *End user application: Google Docs Spreadsheet*

***What to do:***

* *Power up the LoRaWAN Gateway and connect to it*
* *Create a user account on The Things Network*
* *Connect the end node to your The Things Network environment*
  + *Determine the frequency for the location (Europe)*
  + *Choose the LoRaWAN version*
  + *Find the DevEUI code*
  + *Create an AppEUI,*
  + *Generate an AppKey and*
  + *Insert the End device ID*
* *Create python code for the end node or fetch one from pycoms website. (IDE in demo is Atom)*
* *Upload project to the end-device and run it*
* *Check that the data is received by The Things Network environment*
* *Use Payload formatters to make the results more readable in The Things Network environment (e.g. a custom JavaScript formatter)*
* *Go back to live data, to ensure that the received data now gets decoded*
* *Experiment with the stimuli/exposure of the sensors to confirm that the IoT device actually registers the different impressions (e.g. point a flashlight at the light sensor)*
* *Create a new spreadsheet on Google Docs*
* *Open Googles Apps Script*
* *Insert the script which connects to the rest of your IoT system*
* *Deploy the script as a web application with open access*
* *Copy the web application link*
* *Open Integrations in The Things Network environment*
* *Create a custom webhook where the base URL is the link copied*
* *Allow uplink in your webhook*
* *Check that the data now is uploaded to the spreadsheet*
* *If you want to change the code from Apps Script, you can redeploy it as a new version. Which automatically connects to the already created webhook*

***LoRaWAN application for the IoT system***

* *A LoRaWAN application usually consists of 4 main components, with a connection line between one component and the next one:*

1. *Sensor and end node*
2. *LoRa transmission*
3. *LoRaWAN Gateway*
4. *Internet connection*
5. *Servers*
   1. *Network Server*
   2. *Join Server*
   3. *Application Server*
   4. *Integration Services*
6. *Internet connection through the HTTPS-protocol*
7. *End user application*

* *Such applications can also use Bluetooth. In that case, the system could look like this:*

1. *BLE sensors*
2. *BLE transmission*
3. *BLE-to-LoRa Gateway based on Pycom FiPy module*
4. *LoRa transmission*
5. *LoRaWAN Gateway*
6. *Internet connection*
7. *Servers*
   1. *Network Server*
   2. *Join Server*
   3. *Application Server*
   4. *Integration Services*
8. *Internet connection through the HTTPS-protocol*
9. *End user application*

***Conclusion of the topics of today:***

* *LoRaWAN can provide long distance rate communication in urban and rural areas for outdoor and indoor applications.*
* *LoRaWAN is suitable for:*
  + *Gathering small amounts of data from distributed battery-powered sensors.*
    - *Smart cities, homes and buildings, communities, agriculture, metering and utilities, healthcare, environment, supply chain and logistics*
  + *Control of distributed main-powered actuators*
  + *Limited control of distributed battery-powered actuators*
* *LoRaWAN is not suitable for:*
  + *Internet access*
  + *Real-time communication*
  + *Massive data transmission (e.g. multimedia, streaming, security cameras, etc.)*

***More information:***

* *Semtech LoRa Developer Portal*
  + [*https://lora-developers.semtech.com/*](https://lora-developers.semtech.com/)
    - *LoRaWAN Academy*
    - *Hands-on labs*
* *LoRa Alliance Portal*
  + [*https://lora-alliance.org/*](https://lora-alliance.org/)
    - *Resource Library*
      * *Technical Specifications*
      * *Technical Recommendations*
* *The Things Network*
  + [*https://www.thethingsnetwork.org/*](https://www.thethingsnetwork.org/)
    - *The Things Network consists of an inclusive and open community of people, companies, governments, and universities who are learning, experimenting and building with The Things Stack to realize LoRaWAN solutions*