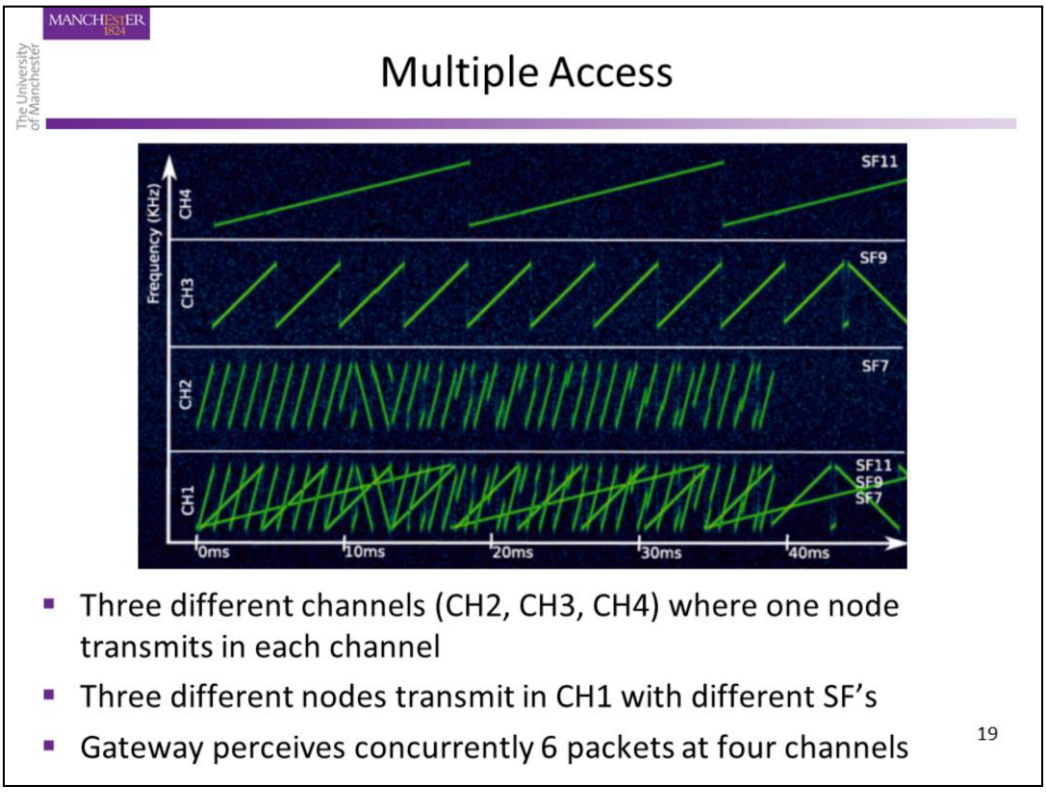


- *Source*: J. C. Liando, A. Gamage, A. W. Tengourtius, and M. Li, "Known and Unknown Facts of LoRa: Experiences from a Large-scale Measurement Study," *ACM Transactions on Sensor Networks*, Vol. 15, No. 2, Article 16, May 2019.

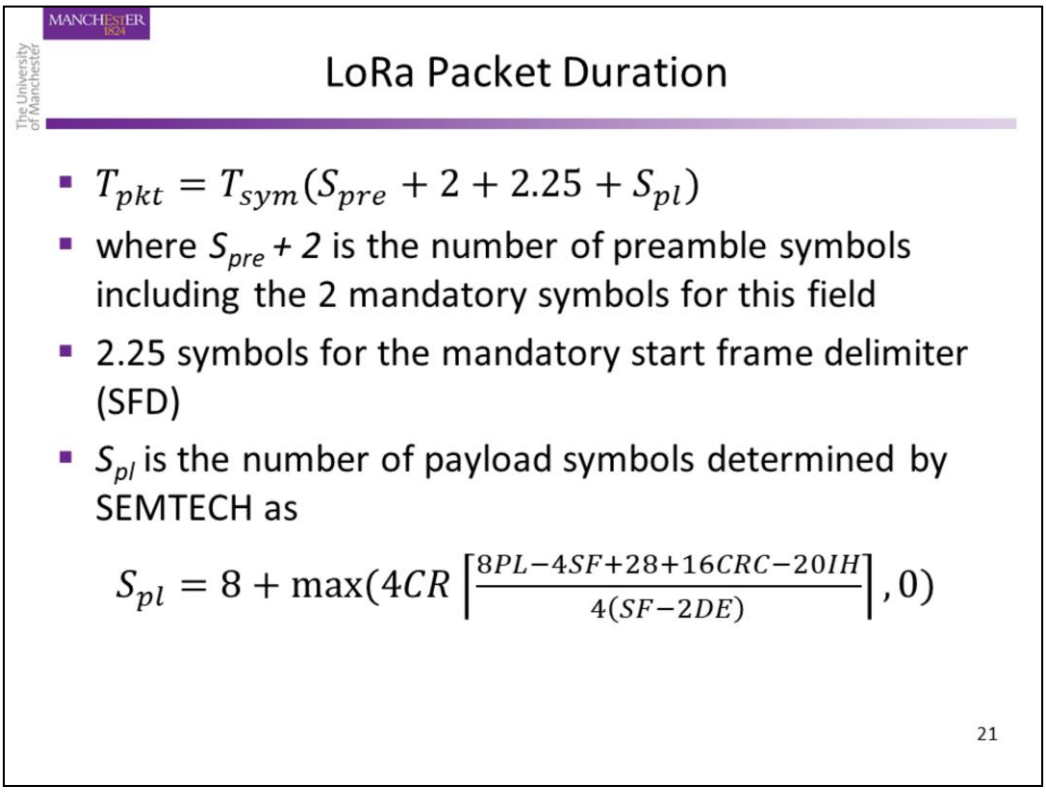
MANCHESTER 1824

The University of Manchester

What's the Lifetime of a LoRa-based IoT Node?

- Lifetime of the node: $L_t = T_{cycle} \times E_{batt} / E_{cycle}$
- T_{cycle} *duration of a transmission cycle with duty cycle*
- E_{batt} *stored energy in the battery (battery capacity)*
- E_{cycle} *energy dissipated per transmission cycle*
- Transmission cycle duration: $T_{cycle} = 100 \times \frac{T_{pkt}}{d.c.}$
- T_{pkt} *transmission duration of a packet*
- *d.c. -> duty cycle (e.g., 1% or 0.1%)*

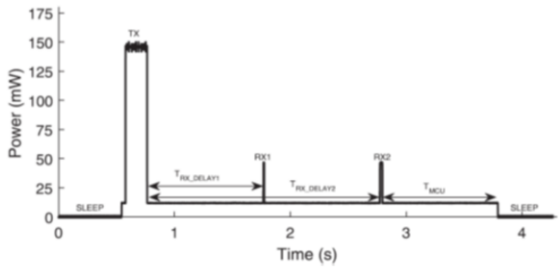
20



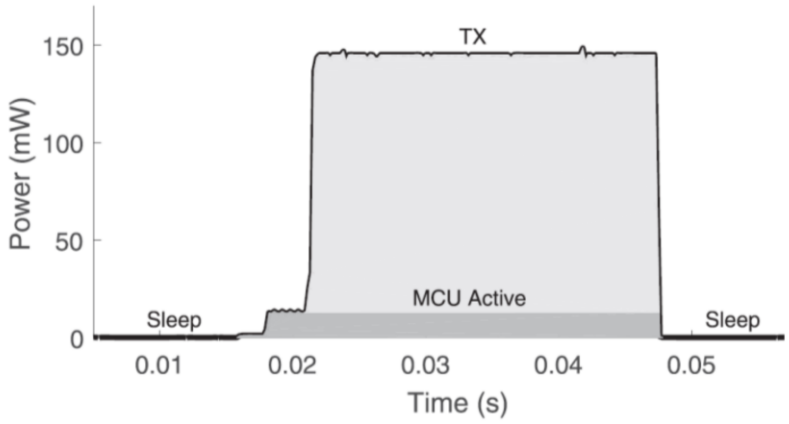
- The different terms included in the expression that describes the number of symbols for the payload are defined as follows:
  - PL: the payload in bytes
  - SF: spread factor
  - CR: code rate with values from 1 to 4
  - CRC: is 1 of CRC is present (uplink packet) and is 0 if the CRC field is absent.
  - IH is equal to 0 when the header is enabled (explicit header) and equal to 1 when no header is present (implicit)
  - DE: should be 0 or 1 to indicate presence or absence of low data rate encoding. DE is recommended to be set to 1, if Tsym exceeds 16 ms.

IoT Node Energy Components

- Assuming a microcontroller with power-saving states and a radio module supporting LoRa
  - Two power states for the microcontroller
    - $E_{MCU_{OFF}} = P_{MCU_{OFF}} \cdot T_{MCU_{OFF}}$, the MCU is in sleep state
    - $E_{MCU_{ON}}$, an average dissipated energy when the MCU is active
  - Two (power) states for the LoRa radio module
    - $P_{R_{TX}}$, transmitting state
    - $P_{R_{OFF}}$, radio is off
    - A third energy component for the reception windows can be added if required



Energy Consumption Profile of LoRa-Based IoT Node



- Single LoRa transmission where SF7, CR4/5, 125 kHz BW, 2dBm Tx power, and 9 bytes payload

23

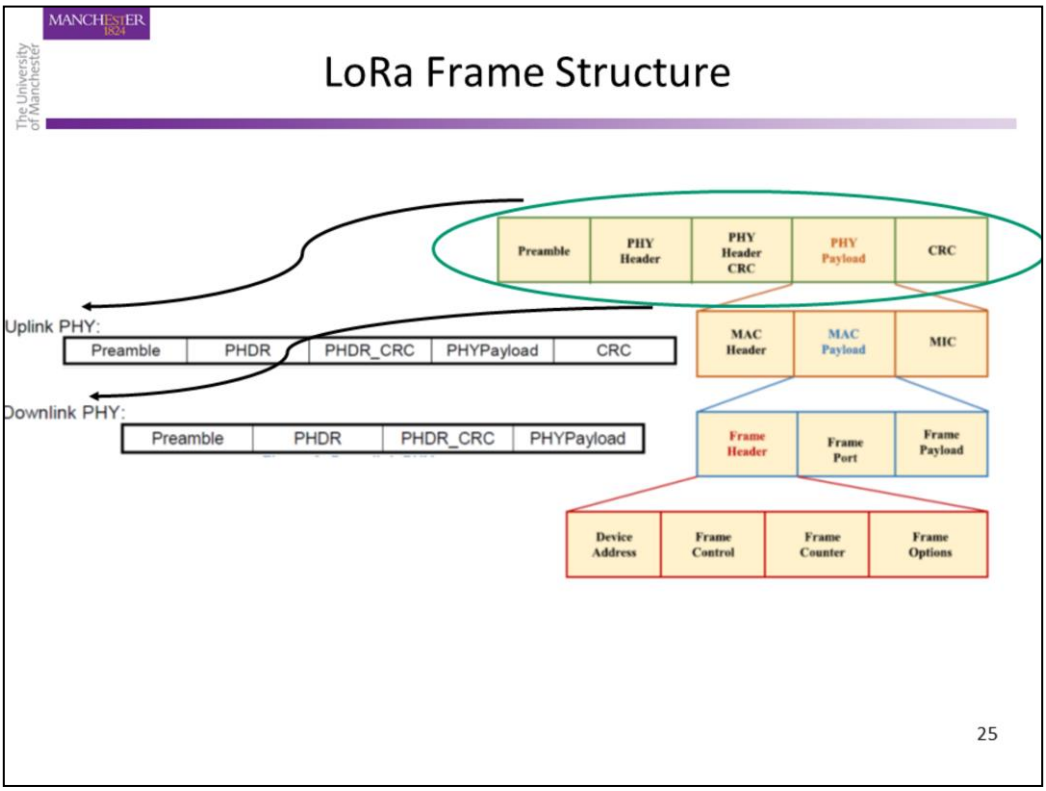
- The radio module SX1278 (SX1276) is provided here: https://modtronix.com/product/inair4/ (accessed on 16/2/2024)

IoT Node Total Energy Demand

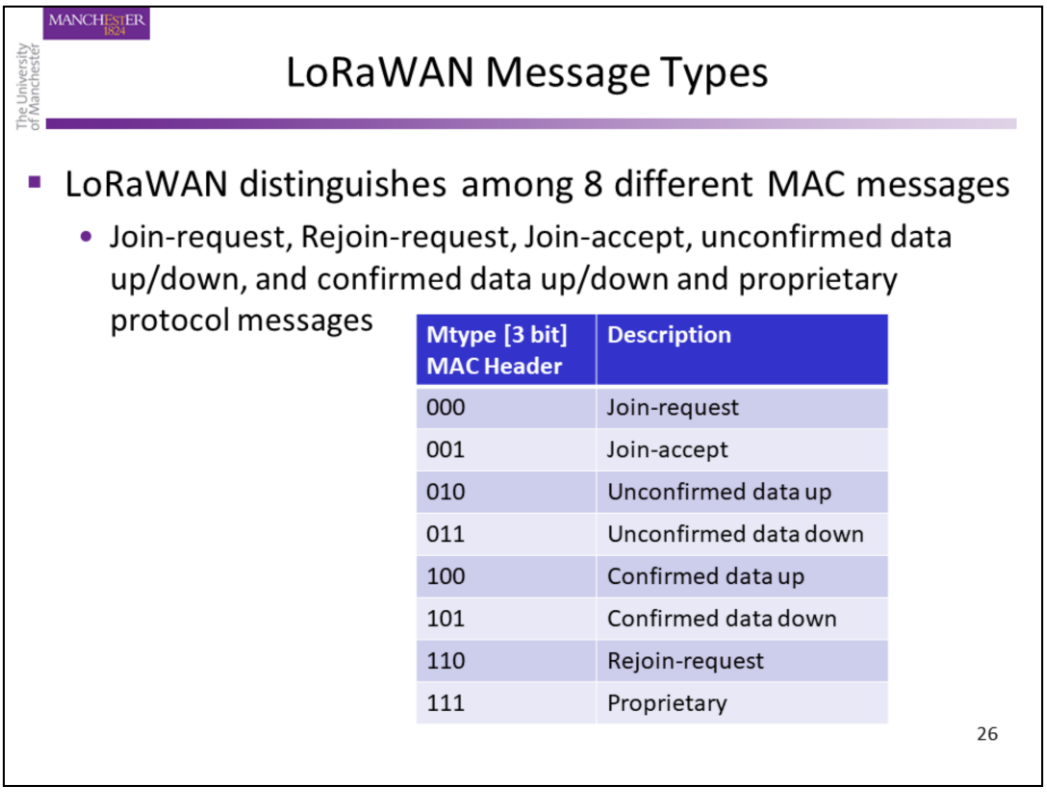
- The energy dissipated during a cycle comprising one transmission can be written as
  $E_{cycle} = [(T_{cycle} - T_{pkt})(P_{MCU_{OFF}} + P_{R_{OFF}})] + [T_{pkt}(P_{R_{TX}} + P_{MCU_{ON}})]$
- The energy that a battery of a charge capacity, notated a C_{batt} (in Ah), can provide, is described as
  - $E_{batt} = 3600 \cdot C_{batt} \cdot V_{batt}$
    - where V_{batt} is the nominal voltage of the battery
    - 1 hr = 3600 sec (all units should follow S.I.)
    - Ah = Amperes per hour

Node lifetime

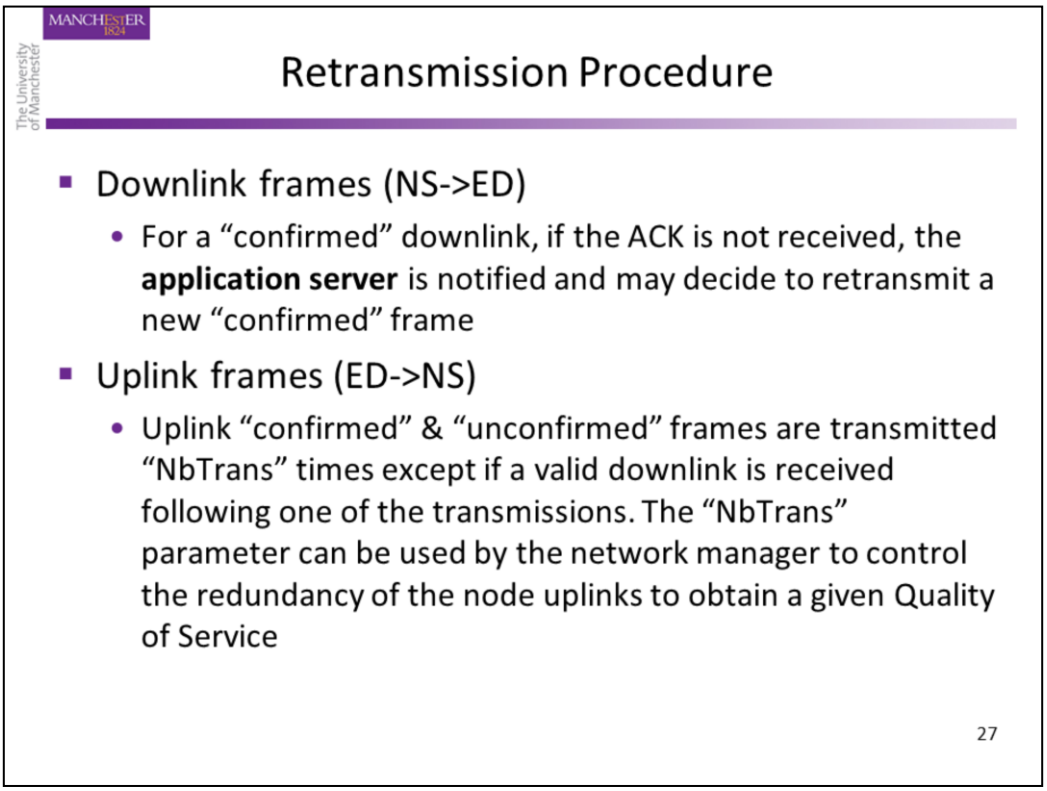
$$L_t = T_{cycle} \times E_{batt}/E_{cycle}$$



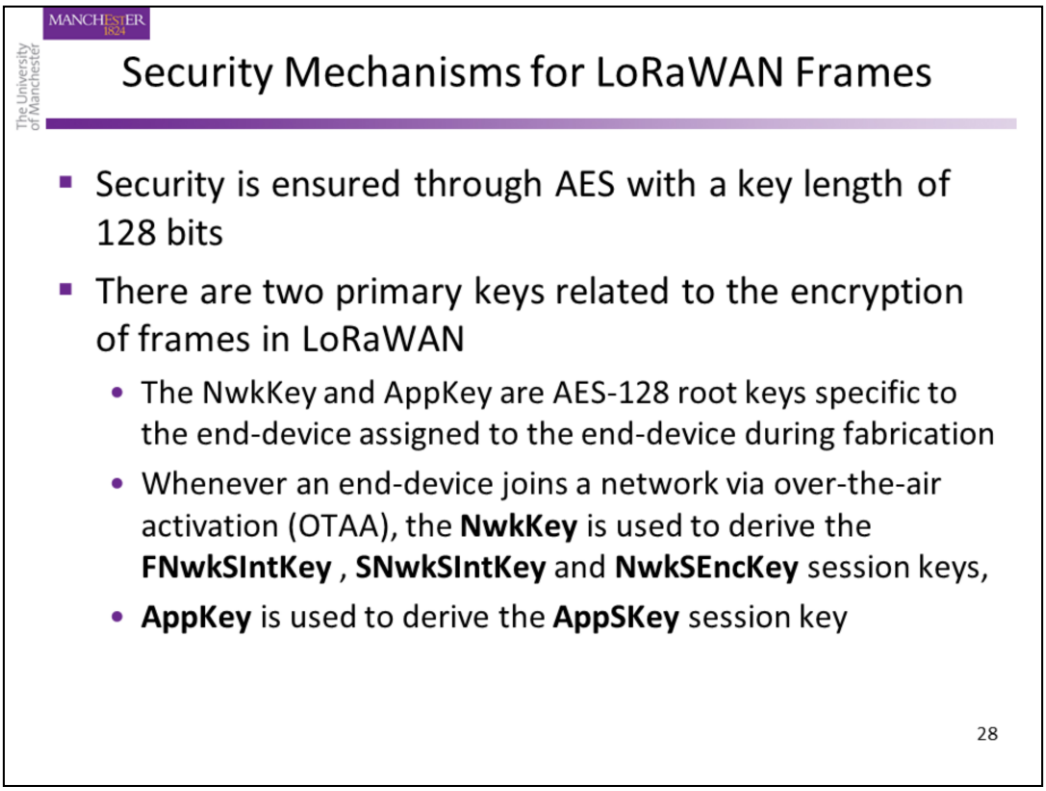
- The following elds are included in the LoRa packet:
- *Preamble Field:* Serving for synchronization purposes and comprising eight successive reference chirps which indicate the packet modulation scheme, the preamble field is modulated with the same spreading factor as the rest of the packet.
- *Header Field:* Two operating modes are available. The number of bytes in the header field indicates the FEC code rate, the length of the payload, and the presence of CRC in the frame in the default explicit operational mode. In the second implicit mode of operation, it is understood that the code rate and payload in a frame remain fixed. This field is not included in the frame when using this mode, which helps to reduce transmission time. A 2-byte CRC field is also present, allowing the receiver to reject packets with invalid headers. The header field, including the CRC field, is 4 bytes long and has a coding rate of 1/2. However, the coding rate for the rest of the frame resides in the PHY header. Note that the length of the payload is determined by the first byte of the header field.
- *Payload Field:* The payload's size ranges from 2 to 255 bytes. This field also includes the following elements:
    - MAC header (species the frame type, protocol version, and direction); MAC payload (including actual data); and MIC (corresponds to the digital signature of the payload).
- *CRC Field:* It is optional and contains Cyclic Redundancy
    - Check (CRC) bytes to protect the payload from errors (2 bytes).



- Data messages are used to transfer both MAC commands and application data, which can be combined together in a single message. A confirmed-data message must be acknowledged by the receiver, whereas an unconfirmed-data message does not require an acknowledgment.
- Proprietary messages can be used to implement non-standard message formats that are not interoperable with standard messages but must only be used among devices that have a common understanding of the proprietary extensions.
- When an end-device or a Network Server receives an unknown proprietary message, it shall silently drop it.

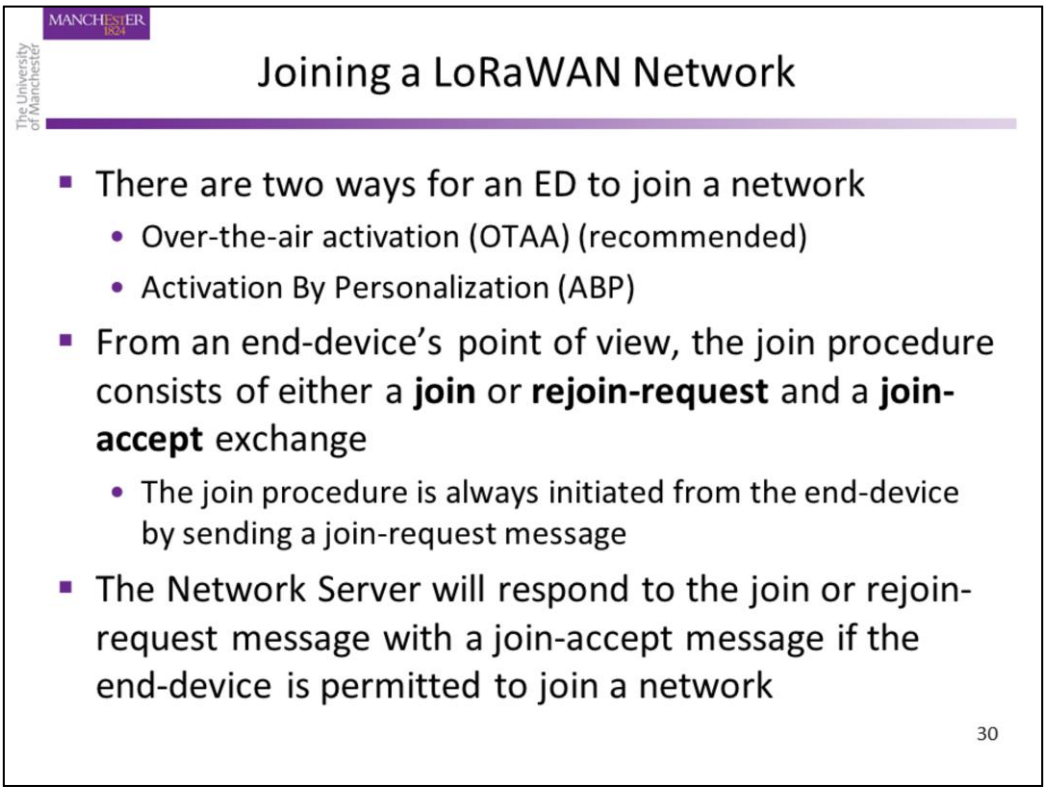


- “NbTrans” is a 4-bit field in the LinkADRReq.
- The device shall stop any further retransmission of an uplink “confirmed” frame if a corresponding downlink acknowledgement frame is received.
- Class A devices shall stop any further retransmission of an uplink “unconfirmed” frame whenever a valid downlink message is received during the RX1 or the RX2 slot window.
- If the network receives more than NbTrans transmissions of the same uplink frame, this may be an indication of a replay attack or a malfunctioning device, and therefore the network shall not process the extra frames.

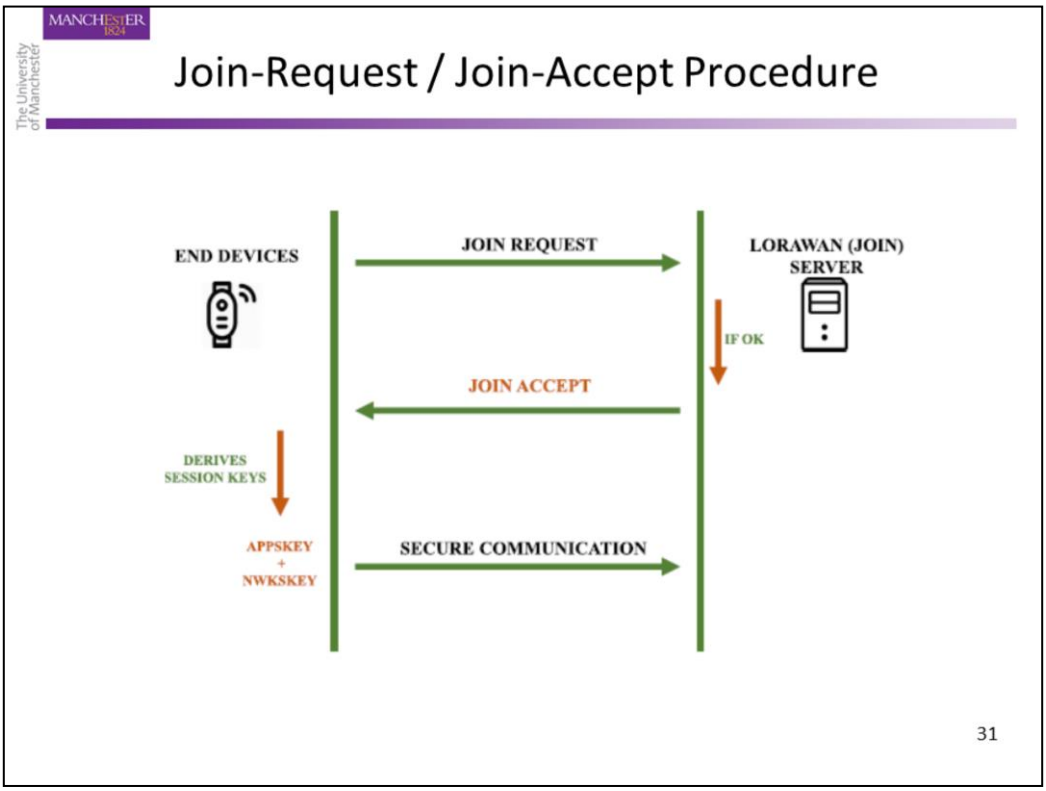


- The encryption scheme used is based on the generic algorithm described in IEEE 802.15.4/2006 Annex B [IEEE802154] using AES with a key length of 128 bits.
- Both the NwkKey and AppKey should be stored in a way that prevents extraction and re-use by malicious actors.
- The **DevAddr** (End-device address) consists of 32 bits and identifies the end-device within the current network. The DevAddr is allocated by the Network Server of the end-device.
- The **FNwkSIntKey** (Forwarding Network session integrity key) is a network session key specific for the end-device. It is used by the end device to calculate the MIC or part of the MIC (message integrity code) of all uplink data messages to ensure data integrity.
- The **SNwkSIntKey** (Serving Network session integrity key) is a network session key specific for the end-device and is used by the end-device to verify the MIC (message integrity code) of all downlink data messages to ensure data integrity and to compute half of the uplink messages MIC.

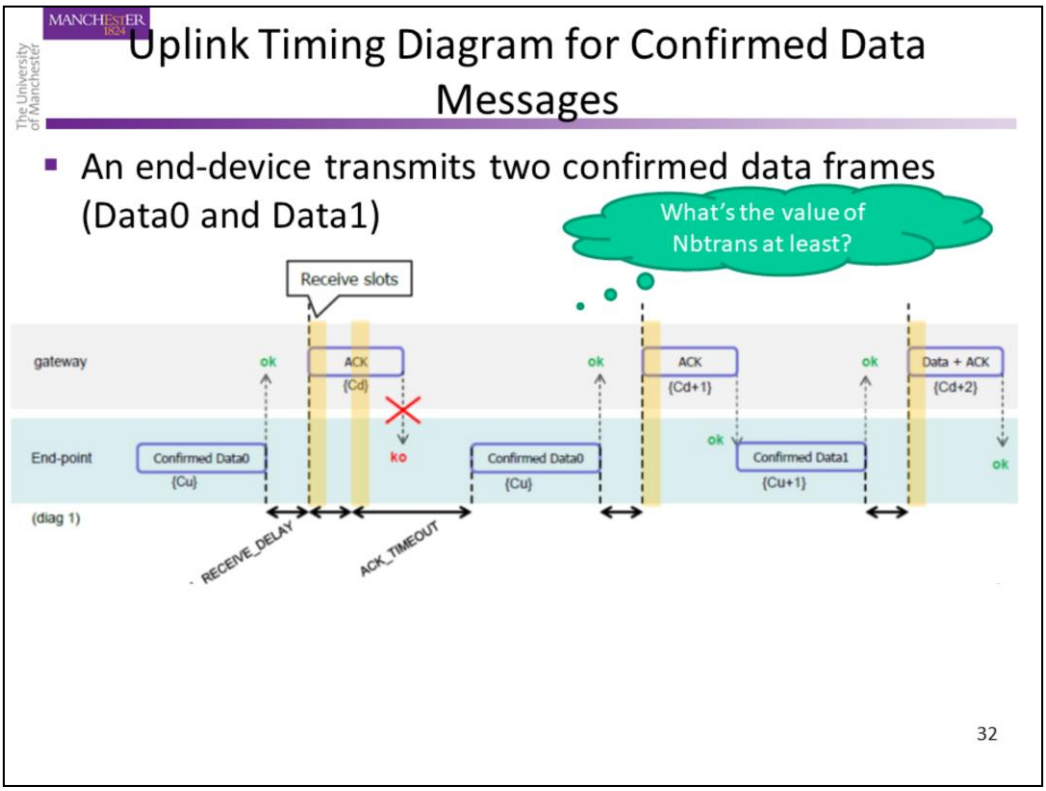
- The **NwkSEncKey** (Network session encryption key) is a network session key specific to the end-device and is used to encrypt & decrypt uplink & downlink MAC commands transmitted as payload.
- The **AppSKey** (Application session key) is an application session key specific for the end-device. It is used by both the application server and the end-device to encrypt and decrypt the payload field of application-specific data messages. Application payloads are end-to-end encrypted between the end-device and the application server.
- Upon completion of either the OTAA or ABP procedure, a new security session context has been established between the NS/AS and the end-device. Keys and the end-device address are fixed for the duration of a session (FNwkSIntKey, SNwkSIntKey, AppSKey, DevAddr).



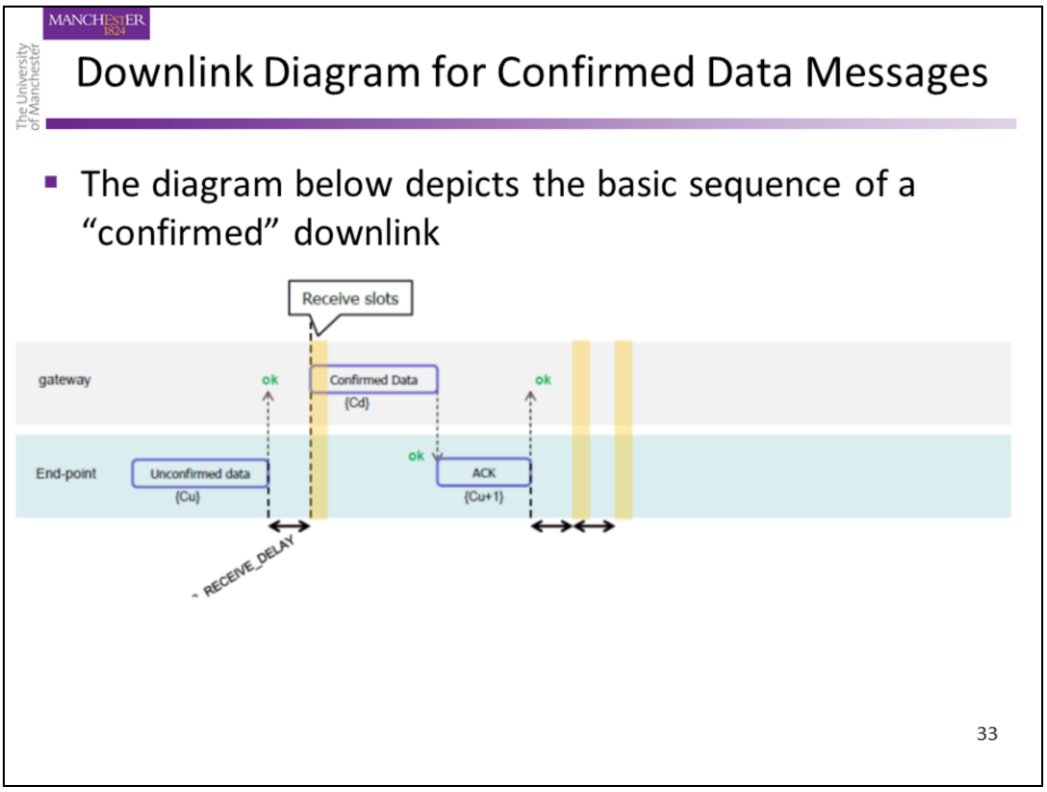
- In either case, a join-accept procedure should be followed
  - The join procedure requires the ED to be personalized with the following information before it starts the join procedure: a DevEUI, JoinEUI, NwkKey and AppKey.



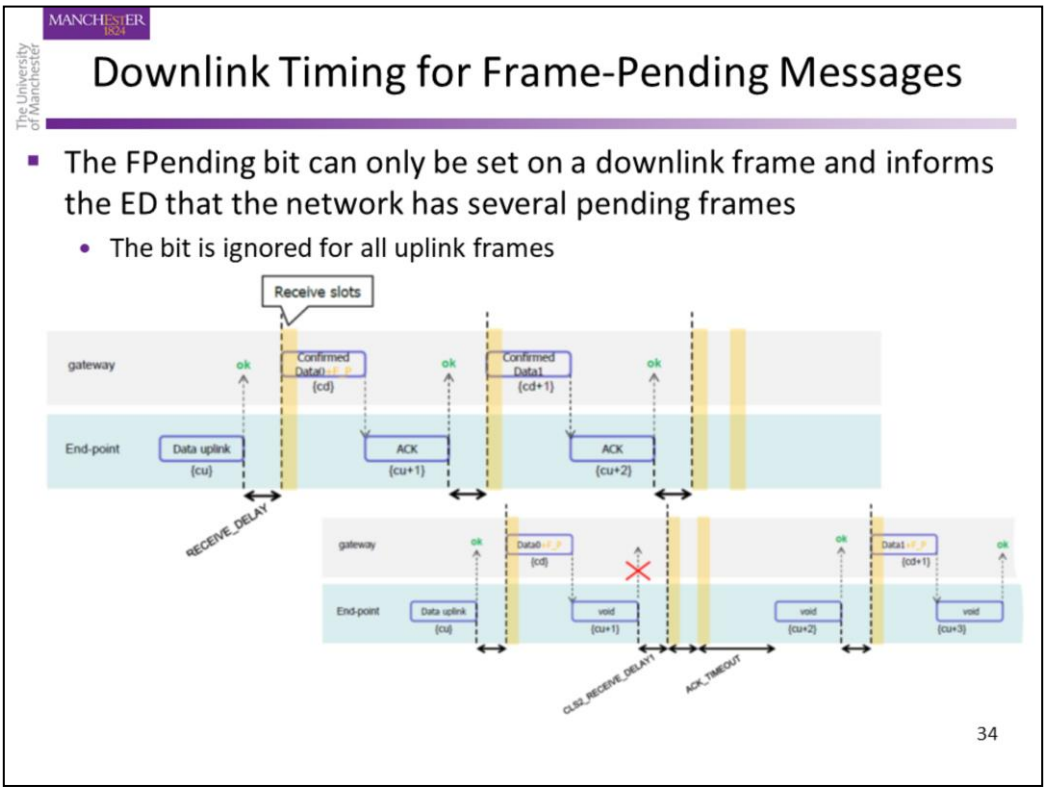
- The join-accept message contains among other information, a network identifier (NetID) (which network was joined), an end-device address (DevAddr), a (DLSettings) field providing some of the downlink parameters, the delay between TX and RX (RxDelay) and an optional list of network parameters (CFList) for the network the end-device is joining.
- Once activated a device may periodically transmit a Rejoin-request message on top of its normal application related traffic. This Rejoin-request message periodically gives the backend the opportunity to initialize a new session context for the end-device. For this purpose, the network replies with a Join-Accept message. This may be used to hand-over a device between two networks or to rekey and/or change DevAddr of a device on a given network.



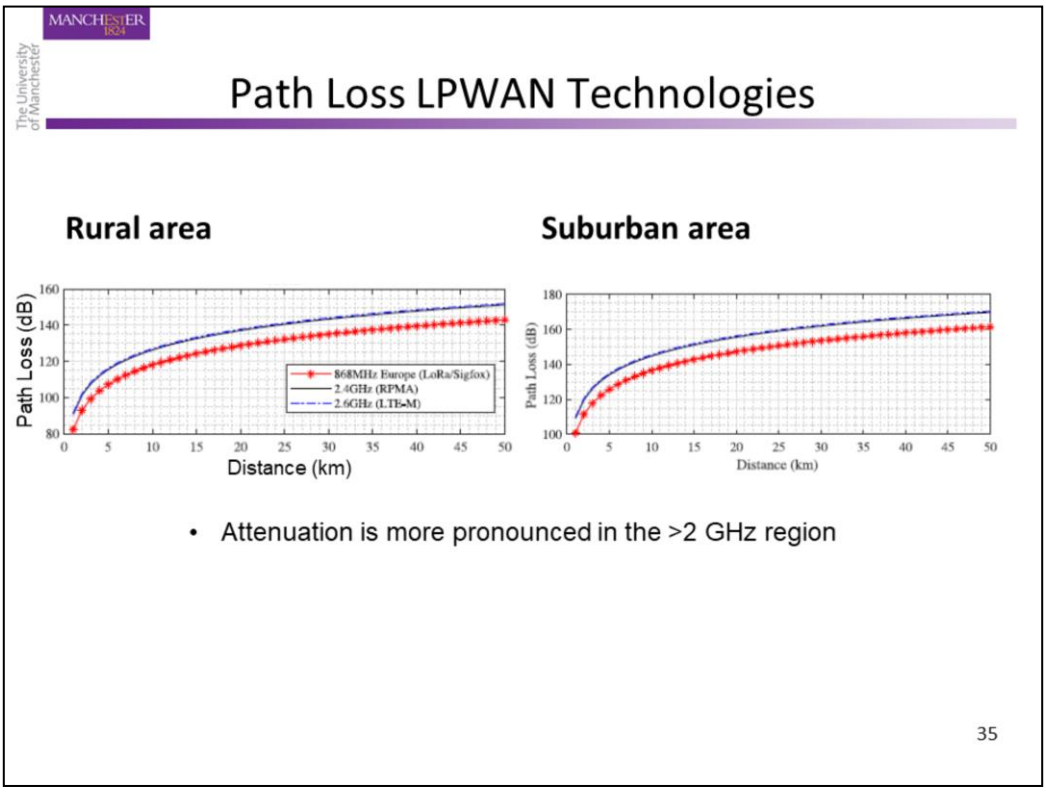
- If an end-device does not receive a frame with the ACK bit set in one of the two receive windows immediately following the uplink transmission it may resend the same frame with the same payload and frame counter again at least ACK_TIMEOUT seconds after the second reception window. This resend must be done on another channel (if supported by the gateway) and must obey the duty cycle limitation as any other normal transmission.



- Upon reception of a data frame requiring an acknowledgement, the ED transmits a frame with the ACK bit set at its own discretion. This frame might also contain piggybacked data or MAC commands as its payload. This ACK uplink is treated like any standard uplink, and as such is transmitted on a random channel that might or might not be different from channel A.



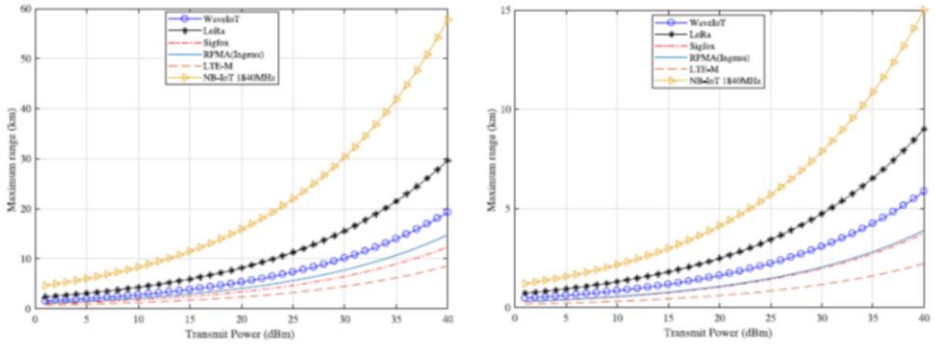
- If a frame with the FPending bit set requires an acknowledgement, the end-device shall do so as described before. If no acknowledgment is required, the end-device may send an empty data message to open additional receive windows at its own discretion, or wait until it has some data to transmit itself and open receive windows as usual.



- Source: A. Ikpehai *et al.,* "Low-Power Wide Area Network Technologies for Internet-of-Things: A Comparative Review," *IEEE Internet of Things Journal*, Vol. 6, No2, pp. 2225-2240, April 2019.
- The 868 MHz technologies require significantly taller masts or towers. If that is considered against the fact that many ISM radio equipment (e.g., Wi-Fi and ZigBee) also share the 2.4 GHz band, then the system designers and implementation engineers need to consider the delicate balance between network reliability, cost, and efficiency in the choice of radio technology.
- Although more bandwidth is available in 2.4 and 2.6 GHz compared to 868 MHz, however, the graphs show that at every distance, the 2.x GHz technologies (RPMA, LTE-M) incur at least 9 dB additional path loss which suggests that they are less able to overcome the effects of obstacles.

Maximum Range

Rural area **Suburban area**



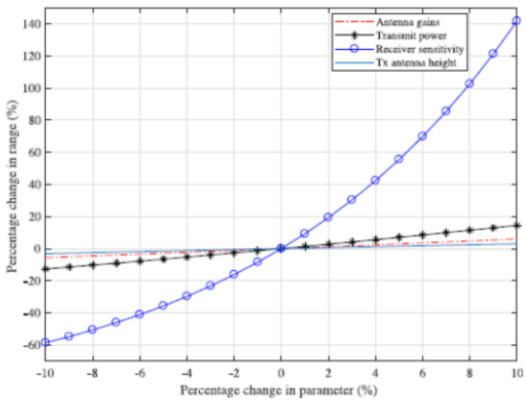
- NB-IoT provides the widest coverage out of the six technologies considered

36

- Source: A. Ikpehai *et al.,* "Low-Power Wide Area Network Technologies for Internet-of-Things: A Comparative Review," *IEEE Internet of Things Journal*, Vol. 6, No2, pp. 2225-2240, April 2019.

LoRa Parameter Sensitivity

- Transmit power, antenna gain, receiver sensitivity, and the height of gateway antenna are varied within ±10% successively
- Receiver sensitivity and transmitting power mostly affect the coverage of the device

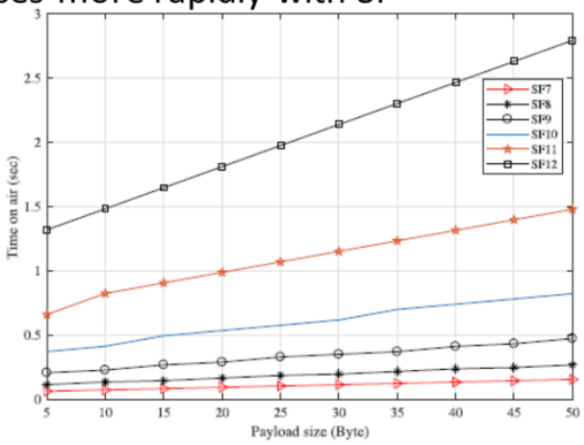


37

- Source: A. Ikpehai *et al.,* "Low-Power Wide Area Network Technologies for Internet-of-Things: A Comparative Review," *IEEE Internet of Things Journal*, Vol. 6, No2, pp. 2225-2240, April 2019.

Spreading Factor (SF) *versus* ToA

- The impact of SF is higher than that of the payload, which implies that for a given payload, the ToA increases more rapidly with SF



38

- Source: A. Ikpehai *et al.,* "Low-Power Wide Area Network Technologies for Internet-of-Things: A Comparative Review," *IEEE Internet of Things Journal*, Vol. 6, No2, pp. 2225-2240, April 2019.