Institute for the Wireless Internet of Things
at Northeastern University

EECE5155: Wireless Sensor Networks and the Internet of Things

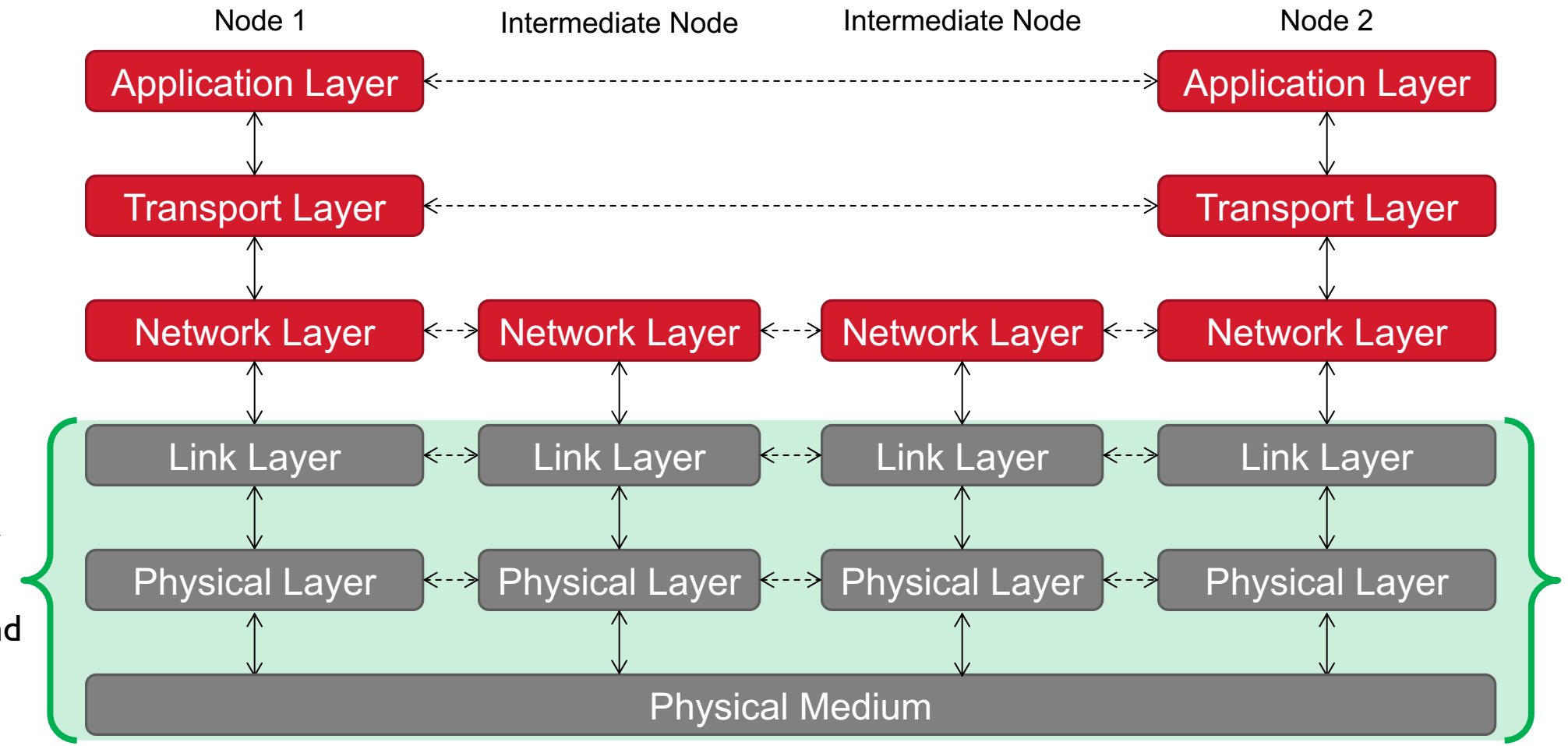
Josep Miquel Jornet
Associate Professor, Department of Electrical and Computer Engineering
Director, Ultrabroadband Nanonetworking Laboratory
Member, Institute for the Wireless Internet of Things
Northeastern University
jmjornet@northeastern.edu
www.unlab.tech

Institute for the Wireless Internet of Things at Northeastern

Standards

The Protocol Stack

Institute for the Wireless Internet of Things at Northeastern



Standards commonly define the physical and link layers

Wireless Technologies for the IoT

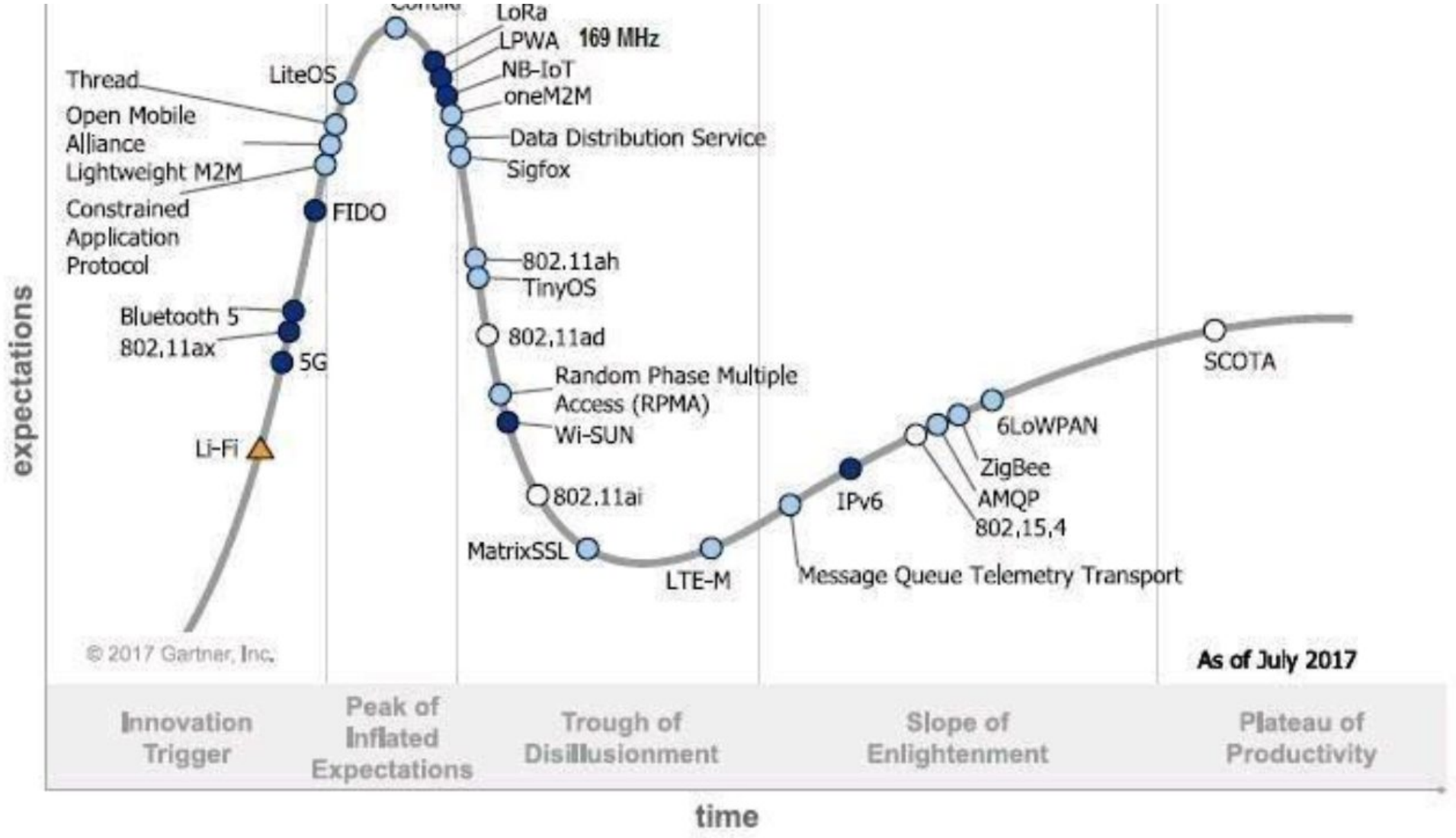
Institute for the Wireless Internet of Things at Northeastern

- There are many technologies to enable the connectivity of "Things" to the Internet:
  - **Physical & link layers:**
    - Radio-frequency Identification (RFID)
      - Passive, Active (DASH7)
    - IEEE 802.15.4 (Low-rate Wireless Personal Area Networks, LR-WPAN)
      - WirelessHART, MiWi, Snap, Thread, (ZigBee?)
    - Z-Wave
    - 1000s of protocols in the field of Wireless Sensor Networks
    - Bluetooth
    - IEEE 802.11 (WLAN)
    - Wide Area Networks (WAN): 3G/4G/5G

Hype Cycle for IoT Standards and Protocols

Institute for the Wireless Internet of Things at Northeastern

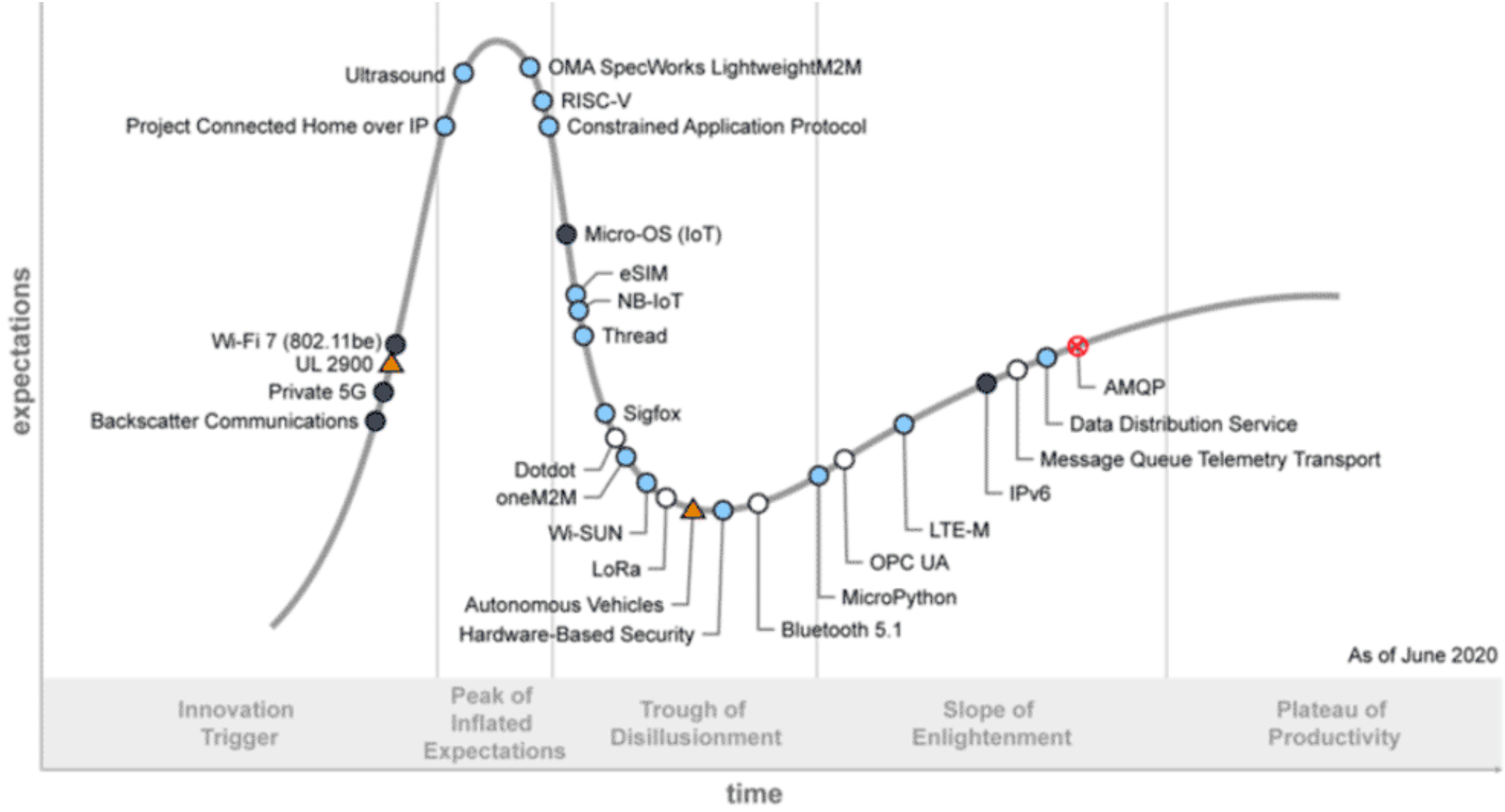
2017



Hype Cycle for IoT Standards and Protocols

Institute for the Wireless Internet of Things at Northeastern

2020



IEEE 802.15.4

Institute for the Wireless Internet of Things at Northeastern

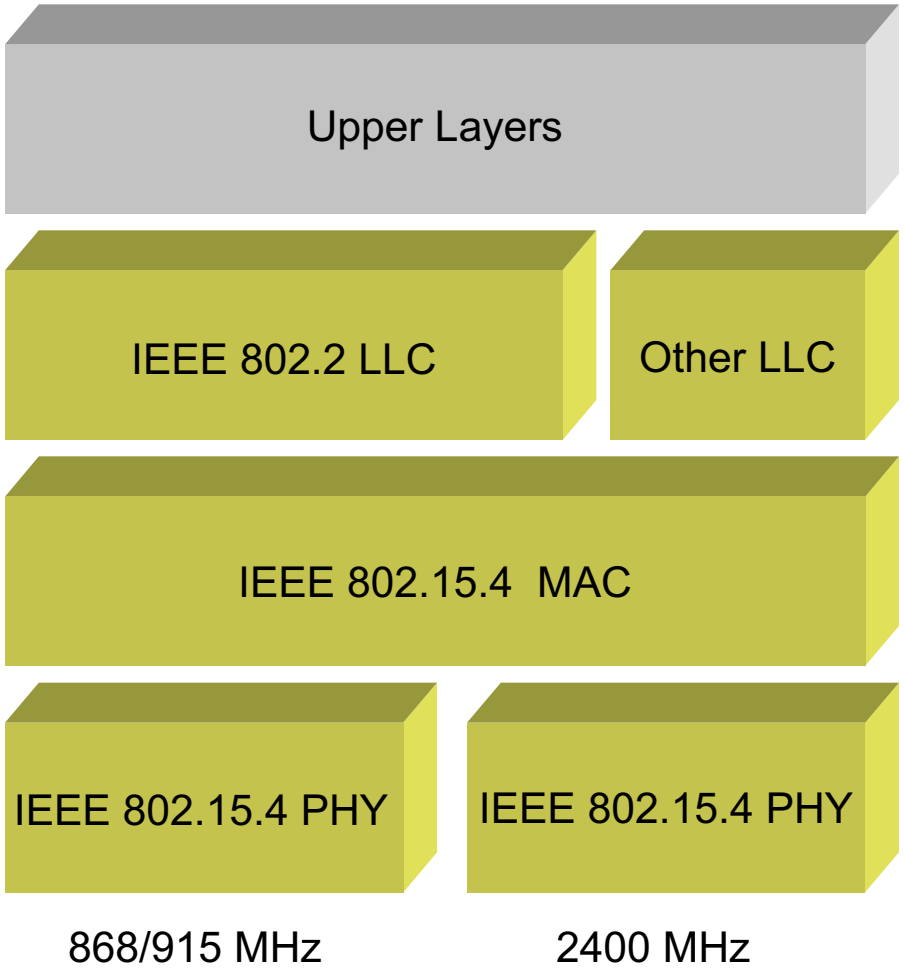
- IEEE = Institute of Electrical and Electronics Engineers
- IEEE 802 = family of IEEE standards for
  - Personal area networks (PAN)
  - Local area networks (LAN)
  - Metropolitan area networks (MAN)
- IEEE 802.15 = working group within the IEEE 802 which specifies wireless PANs or WPANs
- IEEE 802.15.4 = technical standard which defines the operation of low-rate WPANs or LR-WPANs

IEEE 802.15.4: Common Applications

Institute for the Wireless Internet of Things at Northeastern

- Home Networking
- Automotive Networks
- Industrial Networks
- Interactive Toys
- Remote Metering

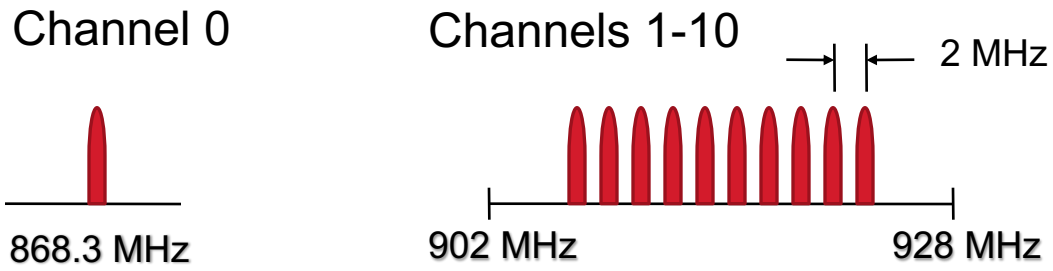
IEEE 802.15.4: Architecture



IEEE 802.15.4 PHY: Frequency Bands

Institute for the Wireless Internet of Things at Northeastern

868MHz / 915MHz



2.4 GHz

Unlicensed Frequency Bands

Institute for the Wireless Internet of Things at Northeastern

- Many wireless communication technologies operate in the Industrial, Scientific and Medical (ISM) bands
  - These frequency bands are unlicensed and hence free to utilize as long as the transmission power is below 1 W (usually <100 mW)
  - Free to use also means **used by many other devices** (e.g., cordless phones, garage door openers, microwave ovens, etc.)
    - Interference is a major problem
- Examples:
  - 902-928 MHz
  - 2.4-2.5 GHz
  - 5.725-5.875 GHz
  - 24-24.250 GHz
  - 57-71 GHz
  - 122-123 GHz

IEEE 802.15.4 PHY: Modulation/Spreading

- **868MHz/915MHz PHY**
  - Data modulation is BPSK with differential encoding
    - Data Rate
      - 868 MHz Band: 20 kb/s (1 bit/symbol, 20 ksymbols/s)
      - 915 MHz Band: 40 kb/s (1 bit/symbol, 40 ksymbols/s)
  - Spreading code is a 15-chip m-sequence
    - Chip modulation is BPSK at
      - 868 MHz Band: 300 kchips/s
      - 915 MHz Band: 600 kchips/s

IEEE 802.15.4 PHY: Modulation/Spreading

Institute for the Wireless Internet of Things at Northeastern

- **2.4 GHz PHY**
  - Data modulation is 16-ary orthogonal modulation
    - 16 symbols are orthogonal set of 32-chip PN codes
    - Data rate: 250 kb/s (4 bits/symbol, 62.5 ksymbols/s)
  - Chip modulation is O-QPSK at 2.0 Mchips/s

IEEE 802.15.4 PHY: Common Parameters

Institute for the Wireless Internet of Things at Northeastern

- **Transmit Power**
  - Capable of at least 0.5 mW
- **Transmit Center Frequency Tolerance**
  - ± 40 ppm
- **Receiver Sensitivity (Packet Error Rate <1%)**
  - <-85 dBm @ 2.4 GHz band
  - <-92 dBm @ 868/915 MHz band
- **Dynamic channel selection**
- **Clear channel assessment**
  - Needed to perform carrier sense

IEEE 802.15.4: MAC Overview

Institute for the Wireless Internet of Things at Northeastern

- Star and peer-to-peer topologies
- Optional frame structure
- Association
- CSMA-CA channel access mechanism
- Packet validation and message rejection
- Optional guaranteed time slots
- Guaranteed packet delivery
- Facilitates low-power operation
- Security

IEEE 802.15.4: Device Classes

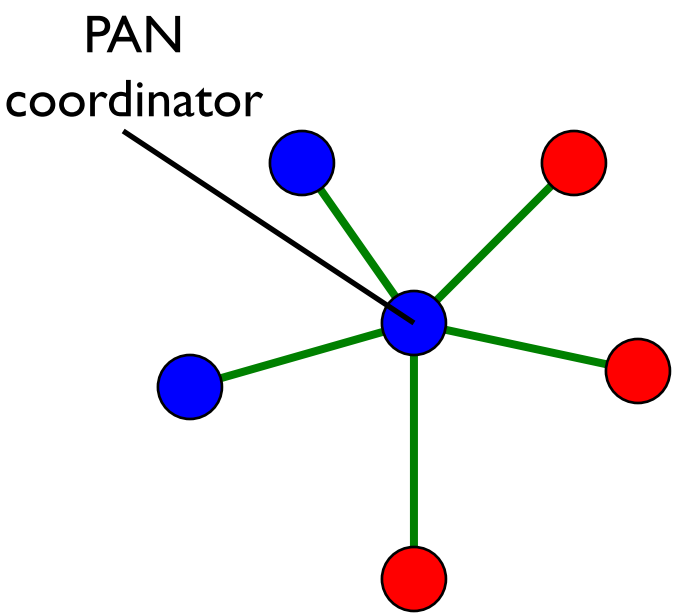
- **Full function device (FFD)**
  - Any topology
  - PAN coordinator capable
  - Talks to any other device
  - Implements complete protocol set
- **Reduced function device (RFD)**
  - Limited to star topology or end-device in a peer-to-peer network
  - Cannot become a PAN coordinator
  - Very simple implementation
  - Reduced protocol set

IEEE 802.15.4: Some definitions

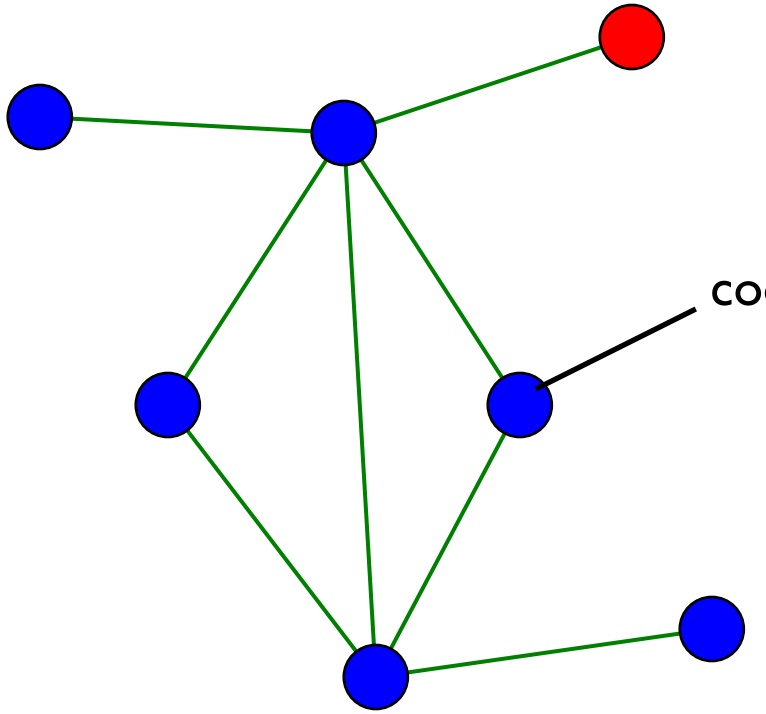
Institute for the Wireless Internet of Things at Northeastern

- **Network Device:** An RFD or FFD implementation containing an IEEE 802.15.4 medium access control and physical interface to the wireless medium.
- **Coordinator:** An FFD with network device functionality that provides coordination and other services to the network.
- **PAN Coordinator:** A coordinator that is the principal controller of the PAN. A network has exactly one PAN coordinator.

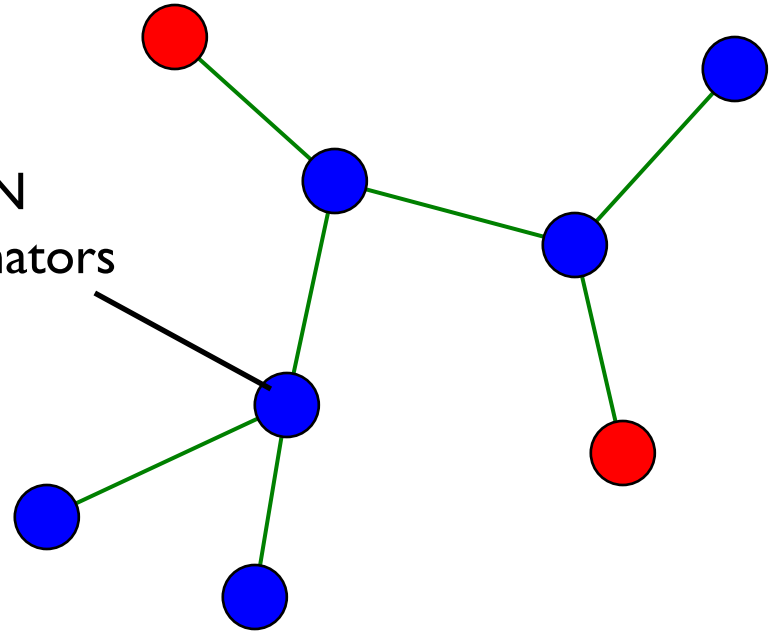
Topologies



Master/slave



Point to point



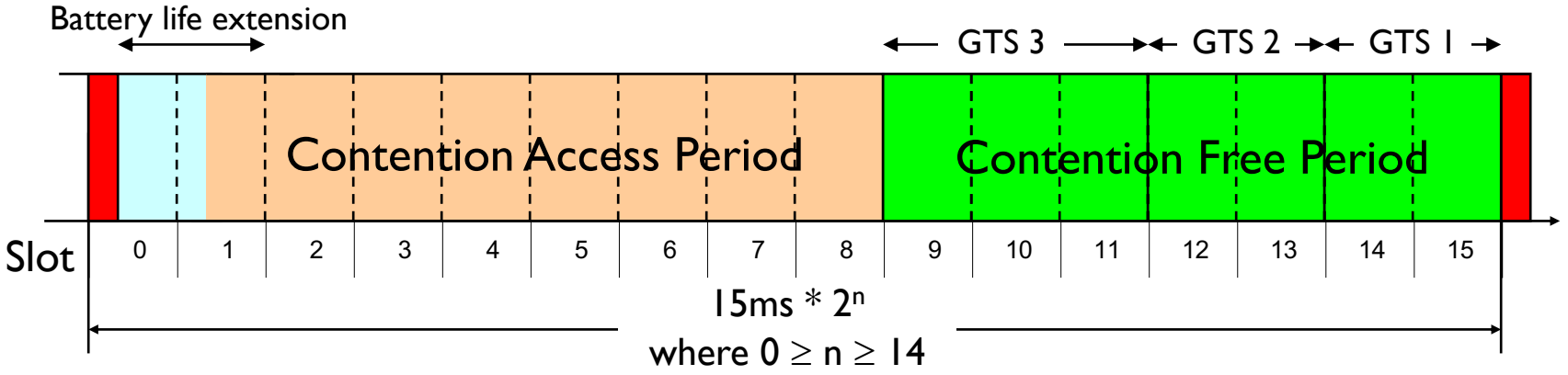
Cluster tree

FFD

RFD

Communications flow

IEEE 802.15.4: Optional Superframe Structure



Network beacon		Transmitted by PAN coordinator. Contains network information, frame structure and notification of pending node messages.
Beacon extension period		Space reserved for beacon growth due to pending node messages
Contention period		Access by any node using CSMA-CA
Guaranteed Time Slot		Reserved for nodes requiring guaranteed bandwidth

IEEE 802.15.4: General Frame Format

Institute for the Wireless Internet of Things at Northeastern

Octets:2	1	0/2	0/2/8	0/2	0/2/8	variable	2
Frame control	Sequence number	Destination PAN identifier	Destination address	Source PAN identifier	Source address	Frame payload	Frame check sequence
		Addressing fields					
MAC header						MAC payload	MAC footer

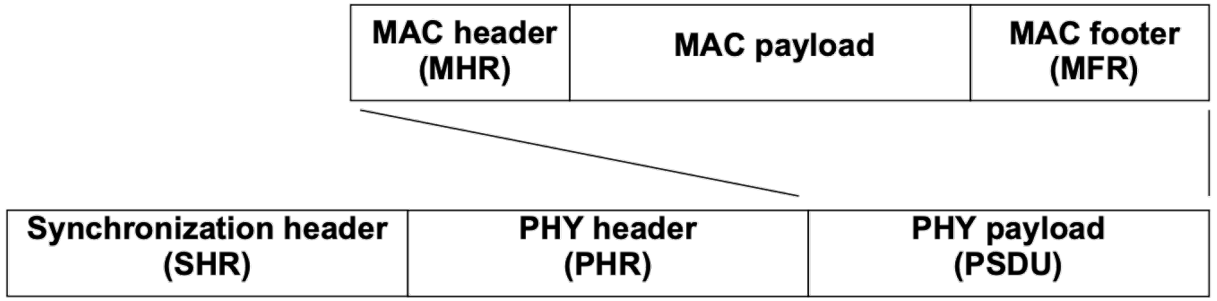
Bits: 0-2	3	4	5	6	7-9	10-11	12-13	14-15
Frame type	Sequrity enabled	Frame pending	Ack. Req.	Intra PAN	Reserved	Dest. addressing mode	Reserved	Source addressing mode

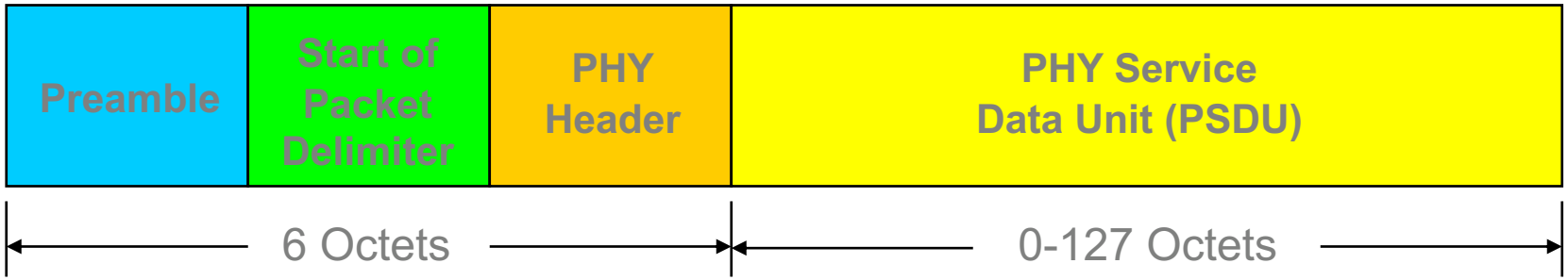
Frame control field

IEEE 802.15.4: PHY Frame Structure

Institute for the Wireless Internet of Things at Northeastern

- **PHY Fields**
  - Preamble (32 bits): For synchronization
  - Start of Packet Delimiter (8 bits)
  - PHY Header (8 bits): Indicates PSDU length
  - PSDU (0 to 1,016 bits): Information coming from the link layer





Differences between IEEE 802.15.4, ZigBee and Thread

Institute for the Wireless Internet of Things at Northeastern

- IEEE 802.15.4
  - PHYsical Layer (PHY)
    - Radio portion, transmitter and receiver
  - Media Access Control (MAC) Layer
    - Radio controller, get data to the next device
- ZigBee & Thread (more later)
  - Network Layer
  - Application Support Layer

Differences between ZigBee and Z-Wave

- ZigBee and Z-Wave target the same application space
- Both of them support start and peer-to-peer (mesh) topologies
- Z-Wave supports only the 900 MHz band
  - ZigBee supports both, 900 MHz and 2.4 GHz
- Z-Wave is a proprietary solution (current owner: Silicon Labs)
  - ZigBee is an open standard

- Commercial examples of these technologies:
  - **Samsung SmartThings:** works with both
  - **Philips Hue:** works only with ZigBee
  - Many third-party sensors for smart-home

What Does Everyone Else Use?

Institute for the Wireless Internet of Things at Northeastern

- Amazon Echo?
- Google Nest?
- Smart Doorbells?
- Many light bulbs?
- Many plugs?

Our good friends Bluetooth and WiFi!!!

Bluetooth

Institute for the Wireless Internet of Things at Northeastern

- **Objective:**
  - **Original:** to replace cables used to connect small devices such as cellphones, mouse, keyboard, audio headset, microphone, etc.
  - **Today:** wirelessly connect any type of nearby devices

- **Versions:**
  - Bluetooth 1 (1999) – IEEE 802.15.1
  - Bluetooth 2 (2004)
  - Bluetooth 3 (2009)
  - Bluetooth 4 (2010)
  - Bluetooth 5 (2016)

- Developed by the Bluetooth Special Interest Group (SIG)
  - Composed by **Ericsson, IBM, Intel, Nokia, Toshiba**, Microsoft, Lenovo, Apple
  - Only Bluetooth 1.0 was an IEEE Standard

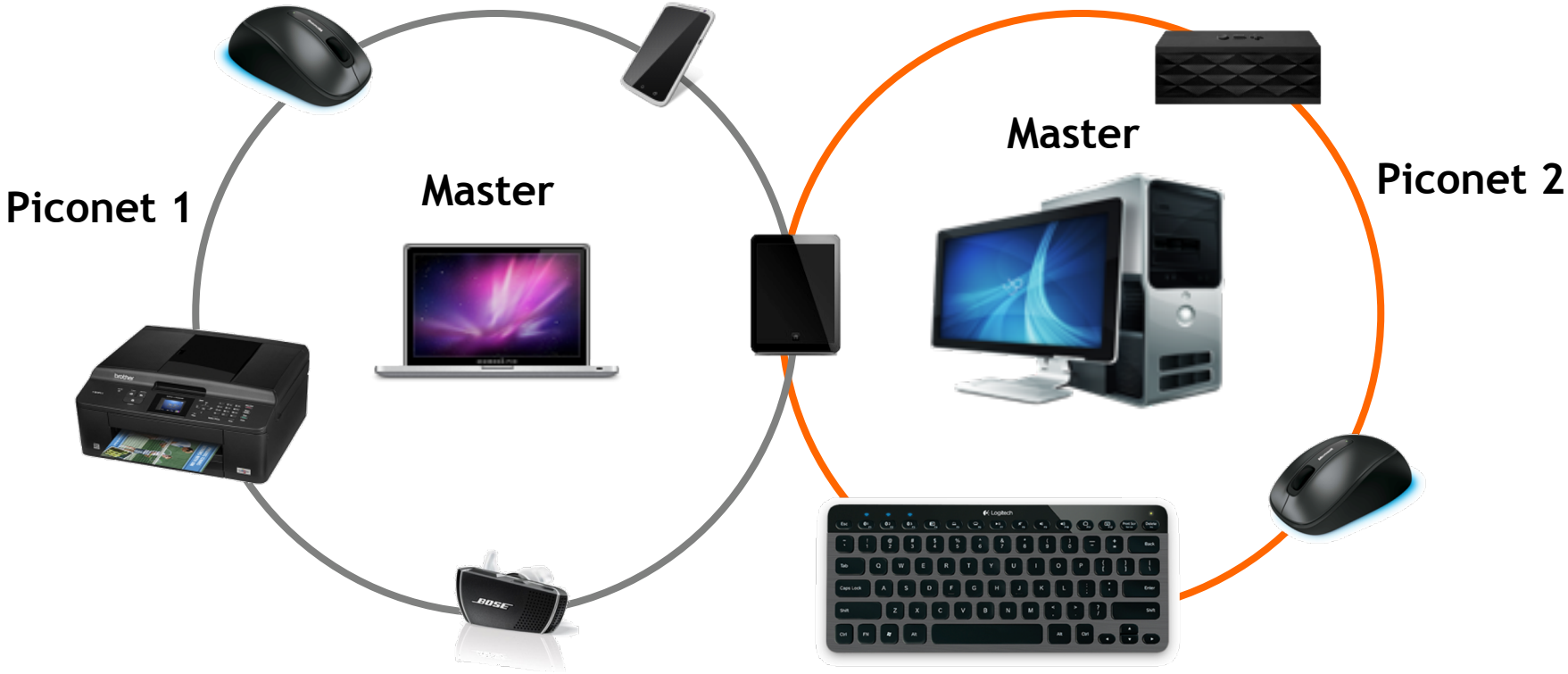
Bluetooth Architecture

Institute for the Wireless Internet of Things at Northeastern

- **Piconet**:
  - Composed by a **master node** and up to **seven active slave nodes** within a distance of up to 10 m
    - There can be up to **255 parked nodes**
      - These are switched by the master to a low-power state to reduce the drain on their batteries
      - They cannot do anything except respond to an activation or beacon signal from the master
  - Operates under a **centralized TDMA system**, with the master controlling the clock and determining which device gets to communicate in which time slot
  - **Direct slave-slave communication is not possible**

- **Scatternet:**
  - An interconnected collection of piconets
  - Enabled by a **bridge node** that takes part in multiple piconets

Bluetooth Architecture



Bluetooth Applications

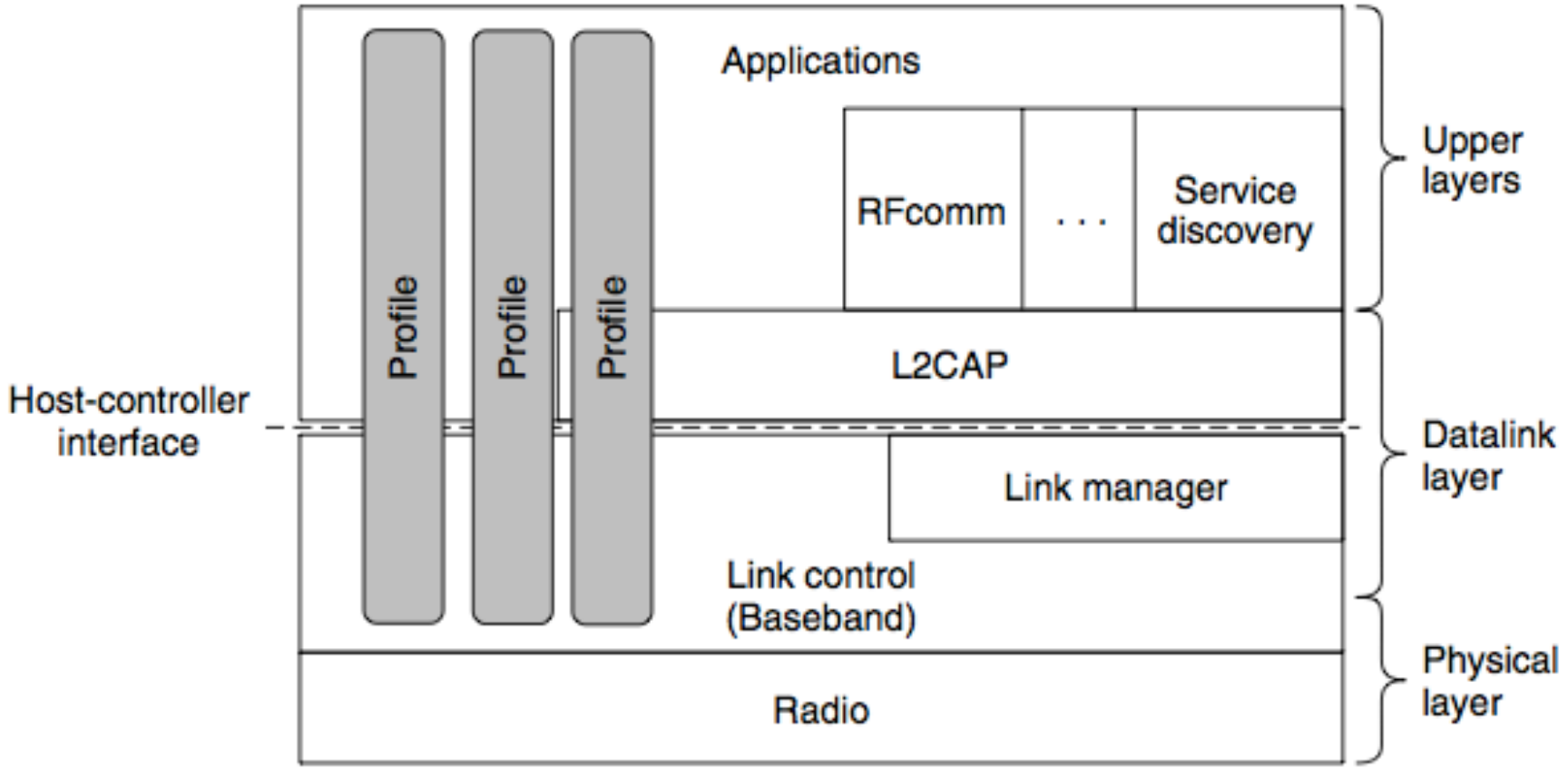
Institute for the Wireless Internet of Things at Northeastern

- Contrary to the other standards we have seen, Bluetooth defines the applications to be supported

- These are called **profiles**, there are 34 as of today:
  - Headset profile
  - Hands-free profile
  - Advanced Audio Distribution profile (A2DP)
  - Human Interface Device profile (e.g., mouse, keyboard)
  - File Transfer profile
  - Object Exchange (OBEX) profile
  - SIM Access profile
  - …

Bluetooth Protocol Stack

- Does not follow the OSI model or the TCP/IP model



Bluetooth Radio Layer

Institute for the Wireless Internet of Things at Northeastern

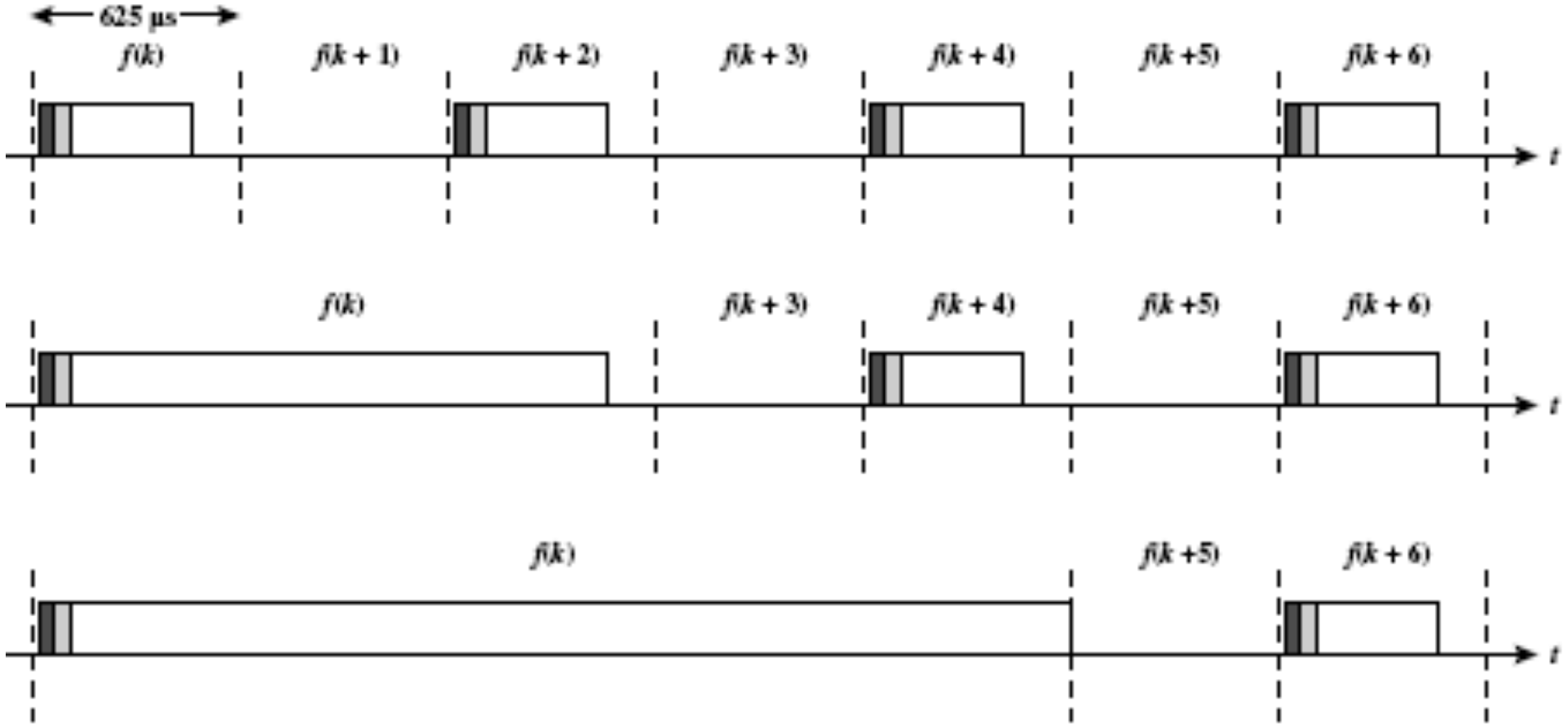
- **Frequency:** 2.4 GHz
- **Bandwidth:** 79 channels, each 1 MHz wide
- **Modulation:**
  - Adaptive Frequency Hopping
    - Up to 1600 hops/s over slots with a dwell time of 625 μs
    - All the nodes in a piconet hop frequencies simultaneously, following the slot timing and pseudorandom hop sequence dictated by the master
  - On top,
    - Originally: Frequency Shift Keying, 1 Mbps
    - Later: Enhanced data rates with Phase Shift Keying, up to 3 Mbps
    - Up to 24 Mbps through the 802.11 Protocol Adaptation Layer (PAL)

Bluetooth Link Layer

- **Medium Access Control:**
  - The master in each piconet defines a series of 625-μs-long time slots:
    - The master's transmissions start in the even slots
    - The slaves' transmissions start in the odd ones
    - Similar to traditional time division multiplexing, with the master getting half the slots and the slaves sharing the other half

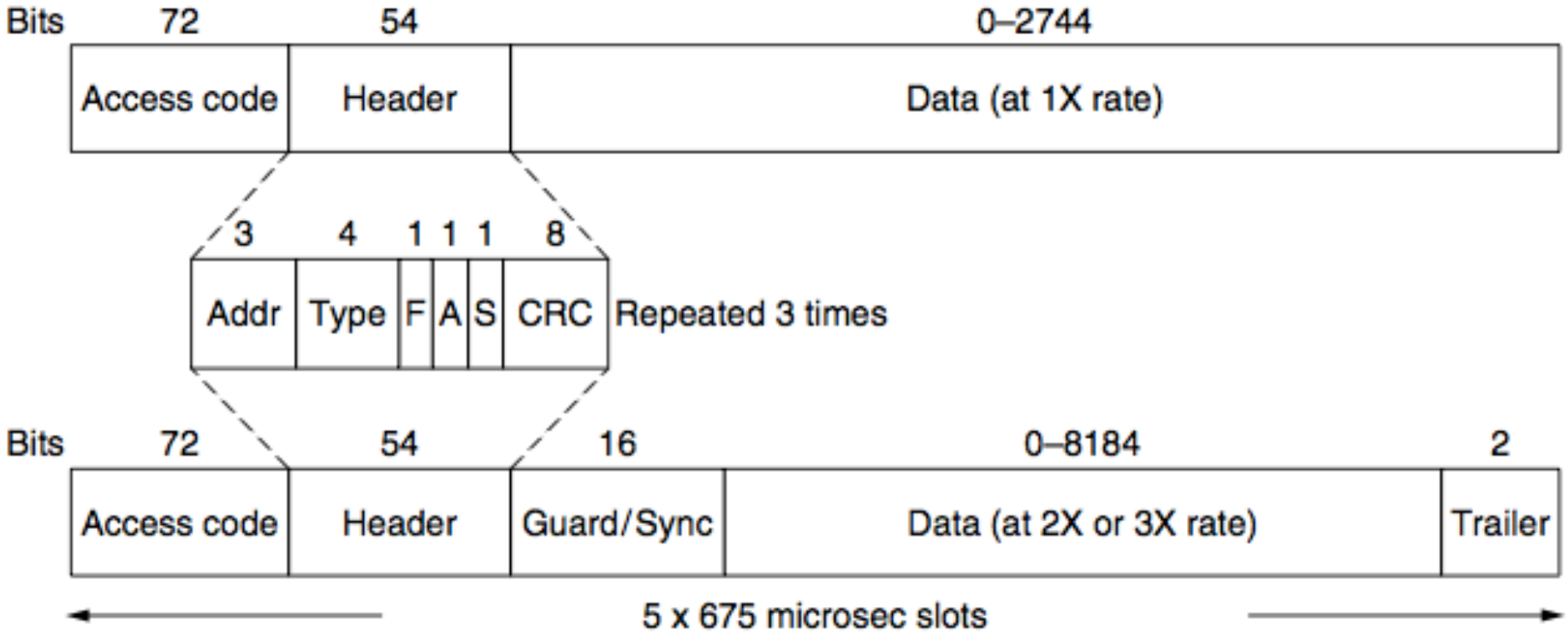
- **Framing:**
  - Frames can be 1, 3, or 5 slots long
  - Each frame has an overhead of 126 bits for an access code and header
  - The payload of the frame can be encrypted for confidentiality with a key that is chosen when the master and slave connect
  - Hops only happen between frames, not during a frame

Multi-slot Frames



Bluetooth Frame Structure

- A frame can occupy up to 5 time slots
- Two different types of frame:



Bluetooth Frame Structure

Institute for the Wireless Internet of Things at Northeastern

- *Access Code:* identifies the master node
- *Header:* repeated 3 times!
  - *Address*: identifies the slave node
  - *Type*: ACL, SCO, poll, null
  - *Flow bit*: set by the slave to tell its buffer is full and cannot accept more data
  - *Acknowledgement bit*: piggybacks an ACK (no need for a separate ACK)
  - *Sequence bit*: used to detect retransmissions (stop-and-wait retransmissions, so at most 1 bit needed)
  - *Checksum*: for the header only
- *Data:*
  - Depends on the type of link…
  - Simple case: SCO
    - Up to 240 bits
    - In case strong protection is needed, only 80 bits repeated 3 times

Bluetooth Link Layer

- Link Manager Protocol:
  - Utilized to set up the links between a master and its slaves
  - Links are established by means of a **pairing procedure**:
    - Originally: 4-digit PIN number (usually 0000 or 1234…)
    - **Secure simply pairing:** requires users to confirm that both devices are displaying the same passkey, or to observe the passkey on one device and enter it into the second device

Bluetooth Link Layer

- Two main types of links exist:
  1. **Synchronous Connection Oriented (SCO) link:**
     - For real time data (e.g., voice)
     - A slave may have up to three SCO links with its master
     - Frames sent over them are never retransmitted
       → Forward error correction can be used to increase reliability
  2. **Asynchronous Connection Less (ACL) link:**
     - Used for packet-switched data that is available at irregular intervals
     - Traffic is delivered on a best-effort basis
       →No guarantees are given
       →Frames can be lost and may have to be retransmitted

Logical Link Control Adaptation Protocol(L2CAP)

- Only used with ACL links

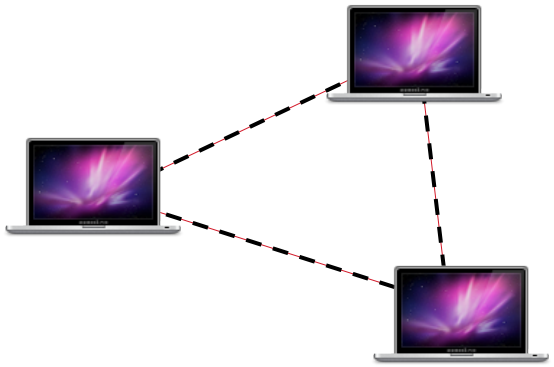
- Has four main functions:
  1. It accepts packets of up to 64 KB from the upper layers and **breaks them into frames for transmission**:
     - The frames are reassembled into packets at the destination
  2. It handles the **multiplexing and demultiplexing of multiple packet sources**:
     - When a packet has been reassembled, the L2CAP layer determines which upper-layer protocol to hand it to
  3. It handles **error control and retransmission**:
     - It detects errors and resends packets that were not acknowledged
  4. It enforces quality of service requirements between multiple links

IEEE 802.11 (Wi-Fi)

- Two operating modes:
  - **Infrastructure Mode:**
    - Each node is associated to an **Access Point (AP)**, through which all the frames are sent
    - Many APs can be connected together, usually through a wired network, to create an extended 802.11 network (e.g., NUwave.)
  - **Ad hoc Mode:**
    - Nodes communicate directly with each other, there is no AP involved

Infrastructure Mode

Ad hoc Mode



IEEE 802.11 Protocol Stack

Institute for the Wireless Internet of Things at Northeastern

Logical Link Sub-layer Medium Access Control Sub-layer								
802.11 (Legacy)	802.11a	802.11b	802.11g	802.11n	802.11ad	802.11ac (WiFi 5)	802.11ah	802.11ax (WiFi 6)
Frequency hopping, Spread Spectrum	OFDM with 48+4 carriers	Spread Spectrum + QPSK, CCK	OFDM with 48+4 carriers	MIMO + OFDM	256 QAM	Downlink MU-MIMO OFDM 256QAM	MU-MIMO OFDM 256QAM	DL &UL MU-MIMO OFDMA 1024 QAM
2.4 GHz and infrared	5 GHz	2.4 GHz	2.4/5 GHz	2.4/5 GHz	60 GHz	2.4/5 GHz	0.9 GHz	2.4/5 GHz
22 MHz	20 MHz	22 MHz	20 MHz	20/40 MHz	+2 GHz	20/40/80/ 160 MHz	1/2/4/8/ 16 MHz	20/40/80/ 160 MHz
1-2 Mbps	6 to 54 Mbps	1, 2, 5.5 and 11 Mbps	6-54 Mbps	Up to 150 Mbps/ stream, up to 4 streams	Up to 7 Gbps	Up to 866 Mbps/ stream, up to 4 streams	Up to 86 Mbps/ stream, up to 3 streams	Up to 1201 Mbps/ stream, up to 8 streams
1997-1999	1999	1999	2003	2009	2012	2013	2016	2020

Physical Layer

- All the variations operate in an ISM band (900 MHz, 2.4 GHz, 5 GHz, 60 GHz)

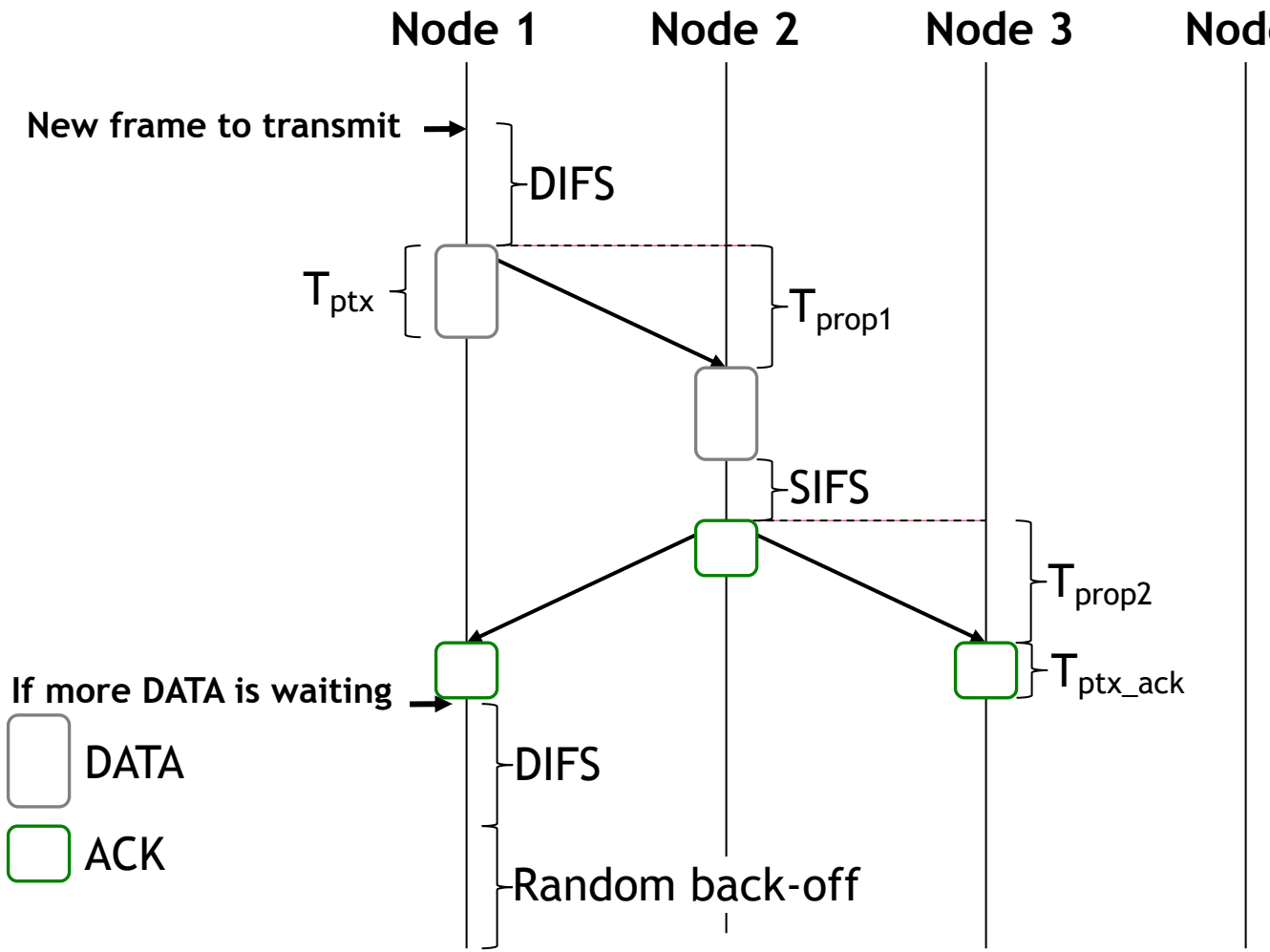
- All the variations support transmission at different data-rates or **rate-adaption**:
  - The rate is negotiated based on the current channel conditions

Medium Access Control

Institute for the Wireless Internet of Things at Northeastern

- Two operation modes:
  - **Distributed Coordination Function:** CSMA/CA with optional RTS/CTS
    - Most common mode
  - **Point Coordination Function:** the AP acts as a centralized polling coordinator
    - Rarely used…

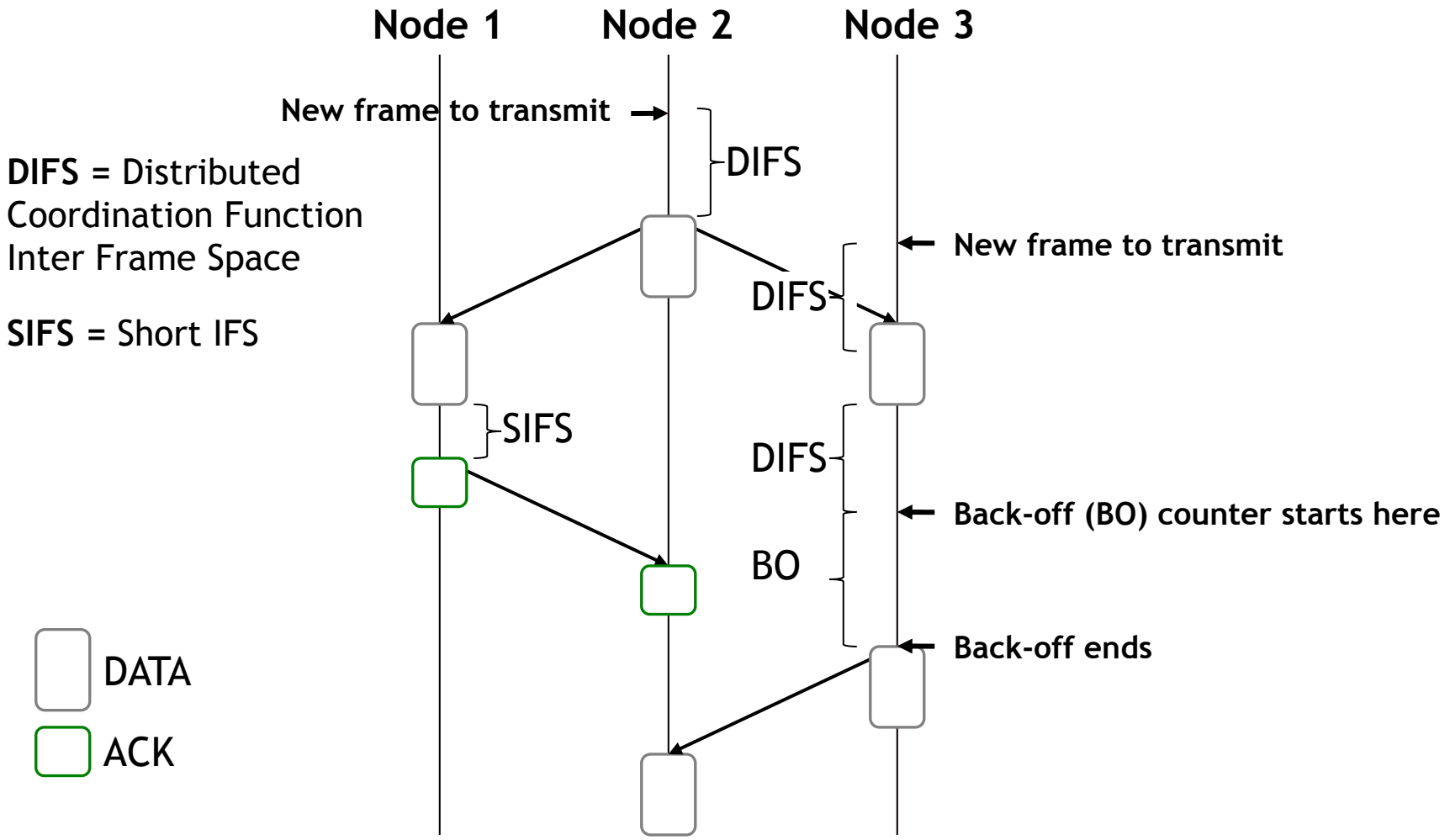
Distributed Coordination Function (without RTS/CTS)



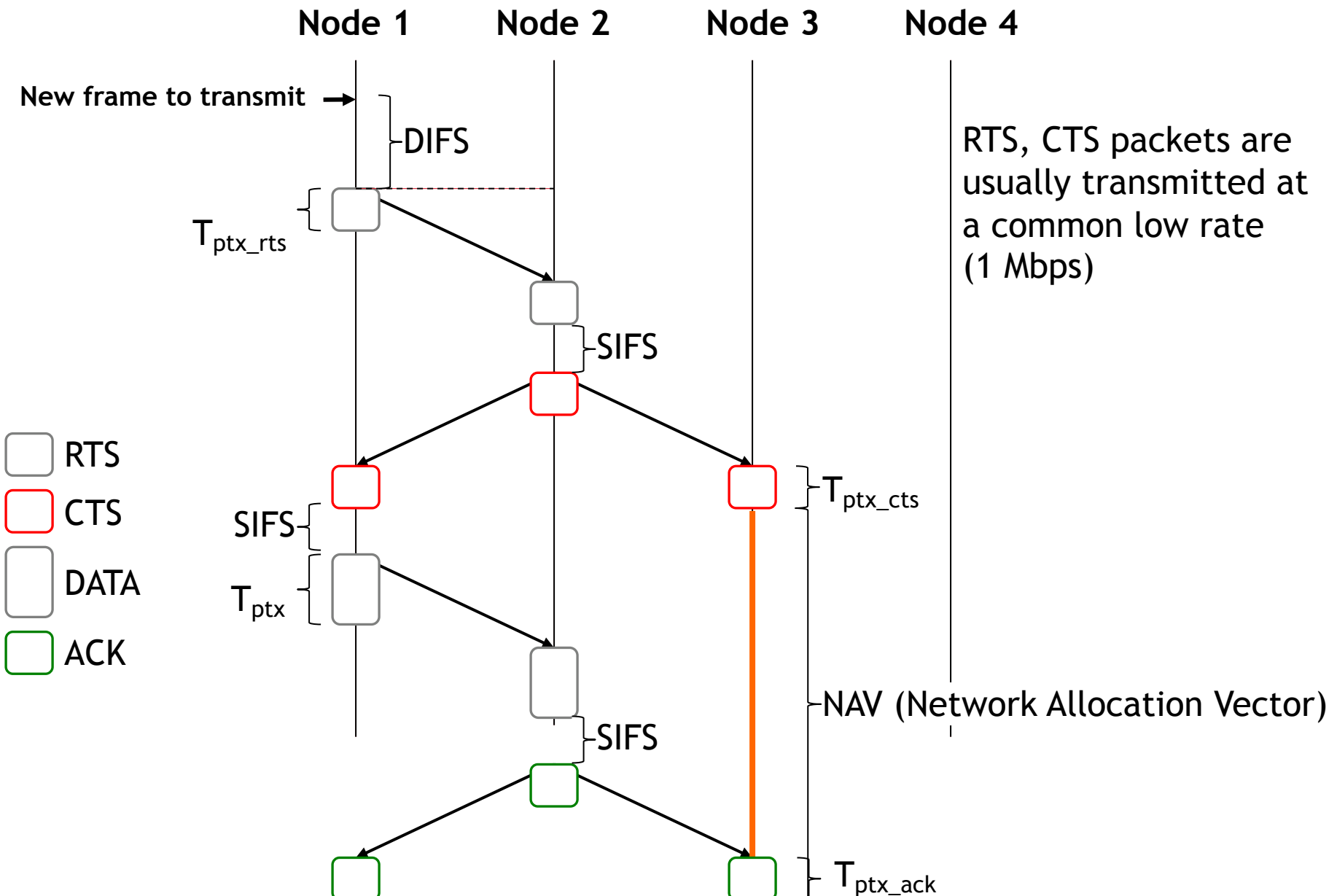
DIFS = Distributed Coordination Function Inter Frame Space

SIFS = Short IFS

Distributed Coordination Function (without RTS/CTS)

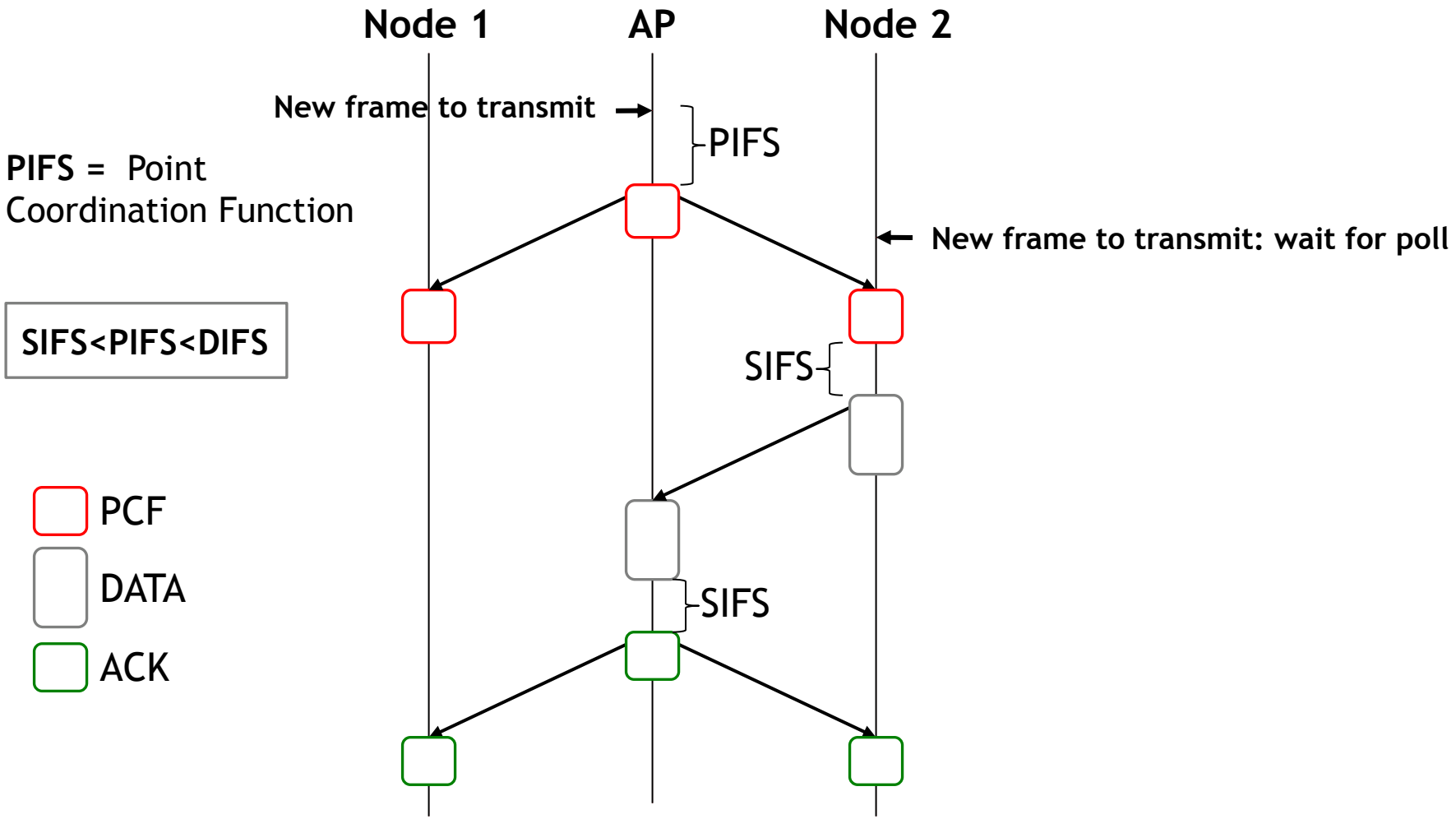


Distributed Coordination Function (with RTS/CTS)



RTS, CTS packets are usually transmitted at a common low rate (1 Mbps)

Point Coordination Function



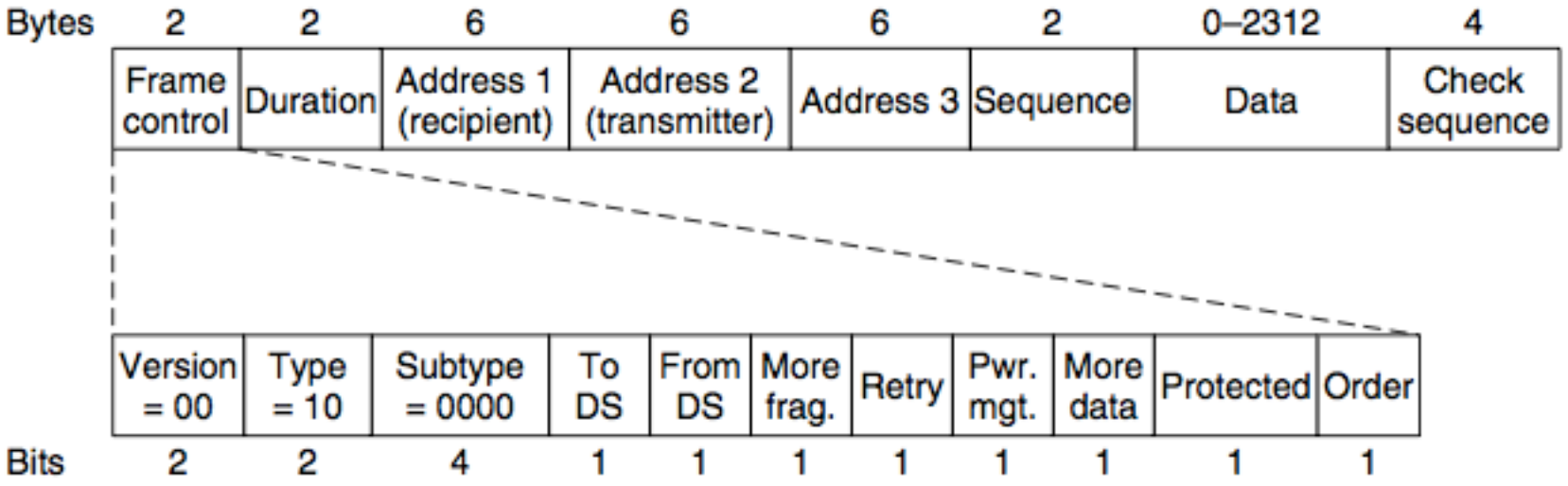
Additional Functionalities

Institute for the Wireless Internet of Things at Northeastern

- **Fragmentation:**
  - Short frames are more likely to be received properly
    - Frames can be split into smaller frames, each with its own checksum
    - Stop-and-wait flow control is used for each sub-frame
- **Energy Savings:**
  - **Power-save Mode:** Nodes that have nothing to send or to receive can go to sleep
    - The AP buffers the traffic for them
  - The AP sends periodical **beacon frames** with information about the AP, security, and also if there is buffered traffic for different nodes (using a bit-map structure)
    - The awaken node can poll the AP for the data, and then continue sleeping
- **Traffic Prioritization:**
  - **Arbitration Inter Frame Space (AIFS):** different waiting times can be defined to give different priorities to different types of traffic
    - **SIFS<AIFS1<DIFS<AIFS2<EIFS**
    - **Extended Inter Frame Spacing (EIFS):** only by a station that has just received a bad or unknown frame

Frame Structure

Institute for the Wireless Internet of Things at Northeastern



Frame Structure

Institute for the Wireless Internet of Things at Northeastern

- Frame control:
  - *Protocol version* (only 00 for the time being)
  - *Type* (data, control, or management)
  - *Subtype* fields (e.g., RTS or CTS)
  - *To DS* and *From DS* (to or from the network after the AP)
  - *More fragments* → More fragments will follow
  - *Retry* → Retransmission
  - *Power management* → The sender is going into power-save mode
  - *More data* → The sender has additional frames for the receiver
  - *Protected Frame* → The frame body has been encrypted for security
  - *Order* → Tells the receiver that the higher layer expects the sequence of frames to arrive strictly in order

Frame Structure

Institute for the Wireless Internet of Things at Northeastern

- *Duration* field: How long the frame and its acknowledgement will occupy the channel (NAV)
- Address 1, 2, 3: receiver, transmitter, final destination
- *Sequence*: frame number so that duplicate frames can be detected
- *Data*: The payload, up to 2312 bytes
- *Frame check sequence*: The same 32-bit CRC

Services

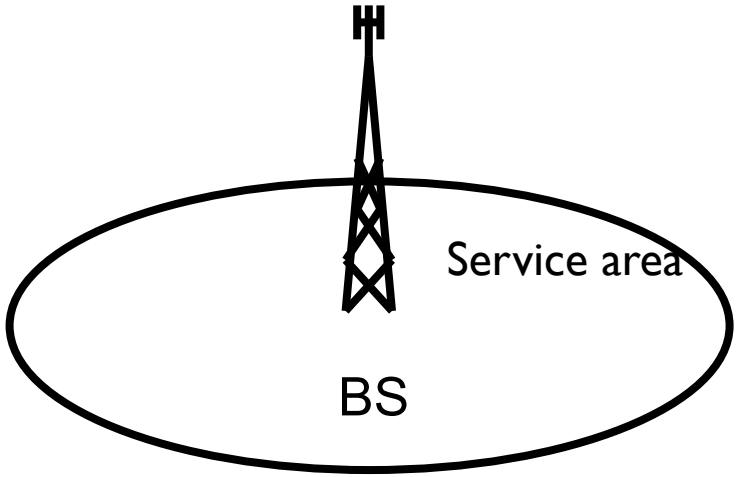
- Defined by the standard:
  - *Association*: to connect to an AP
  - *Reassociation*: to connect to another AP in the same network
  - *Disassociate*: to disconnect from the AP
  - *Authenticate*: different types of security
    - WEP (**Wired Equivalent Privacy**): shared password, very easy to break
    - WPA2 (**WiFi Protected Access 2**):
      - The AP can talk to an authentication server that has a username and password database to determine if the station is allowed to access the network
      - Alternatively a pre-shared key may be configured

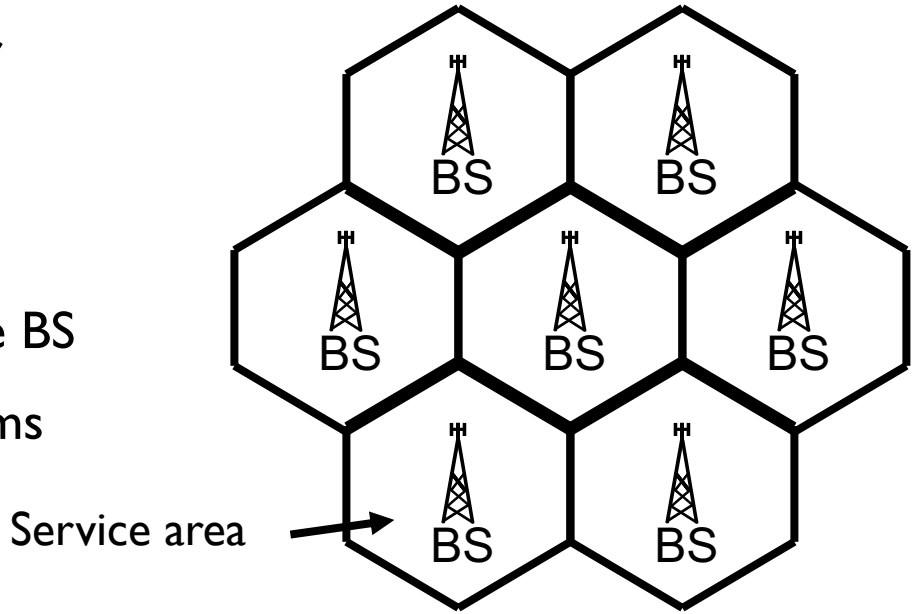
IEEE 802.11 ah

- This version was developed with IoT in mind:
  - 802.11ah runs at 900 MHz band → Longer distance
  - 802.11ah is 802.11ac down by 10x
    - It uses OFDM with 1/2/4/8/16 MHz channels
    - All clocks, all timings, are 10x longer
  - MAC is more efficient by reducing header side, aggregating acks, null data packets (no MAC content, only PHY, used for ACKs), speed frame exchanges (multi-frame transmissions – sliding window)
  - Relays are used to allow connectivity outside the coverage area
  - Saves energy by allowing stations and AP to sleep longer
  - Slow adoption by industry
    - No products by major companies → Everything seems to stick to IEEE 802.11n/ac

Mobile Cellular Networks

- A mobile cellular network is a wireless network distributed over land areas called cells (total area is divided into cells)
- Cells together provide radio coverage over a wide geographic area
- Users can move around this geographical area moving from one cell to another
- Each cell is served by a Base Station (BS), which is in the center
- We refer to users as Mobile Stations (MSs)
- A cell is defined as an area covered by a BS wherein the use of radio communication resources by the MSs is controlled by the BS
  - Constitute the design of the heart of mobile cellular systems
  - MSs in that area are connected and served by the BS





Evolution of Cellular Networks

Institute for the Wireless Internet of Things at Northeastern

Feature	NMT	GSM	IS-95 (CDMA one)	IS-200 (CDMA 2000)	UMTS (3GSM)	LTE	5G NR
Technology	FDMA	TDMA and FDMA	CDMA	CDMA	W-CDMA	OFDMA	OFDMA
Generation	1G	2G	2G	3G	3G	4G	5G
Modulation and Coding	Analog	Digital	Digital	Digital	Digital	Digital	Digital
Year of First Use	1981	1991	1995	2000 / 2002	2001	2009	2018
Focus	Mobile telephony	Digital Voice, SMS	Digital Voice, SMS	Audio, video, data	Audio, video, data	Massive data, streaming	Massive data, streaming
Channel Bandwidth	30 KHz	0.2 MHz	1.25 MHz	1.25 MHz	5 MHz	Up to 20 MHz	Up to 800 MHz
Peak data-rate	2 kbps	64 kbps	Up to 115 kbps	Up to 3Mbit/s	Up to 42Mbit/s for HSPA+	Up to 1 Gbps	Up to 20 Gbps

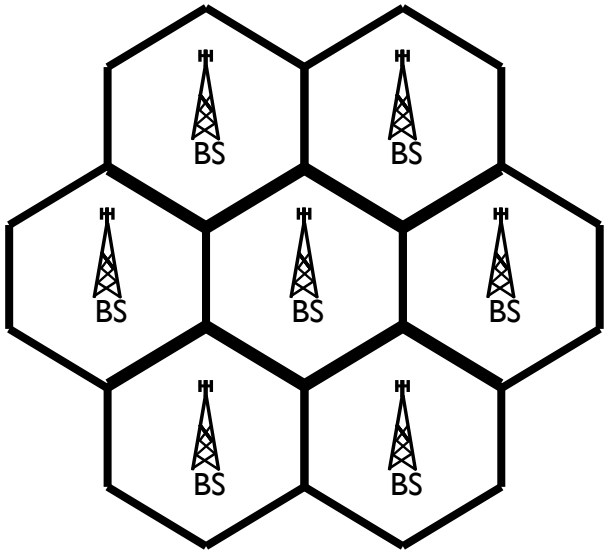
Since 1998, the 3rd Generation Partnership Project (3GPP) has been leading the development of maintenance of cellular standards. Different standards correspond to different "releases" (e.g., LTE was first introduced in Release 8, 5GNR in release 15).

Cellular vs WiFi Technologies

Institute for the Wireless Internet of Things at Northeastern

Cellular

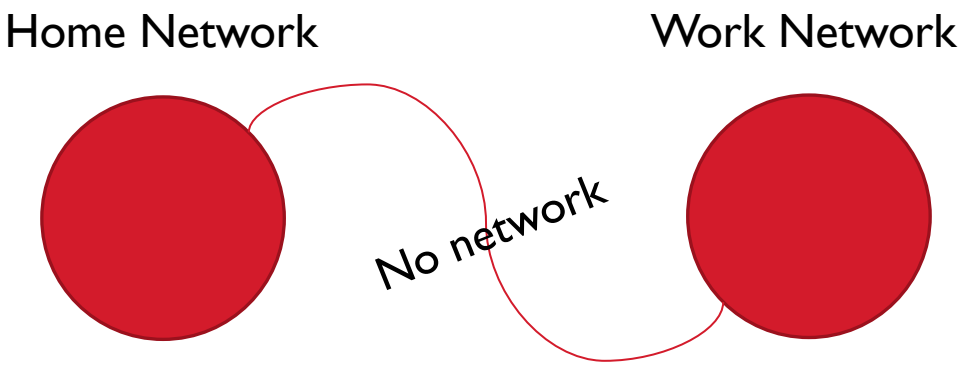
Full area coverage, connection through internet through cellular provider



There is a lot of complexity in orchestrating a network that can cover an entire country with reliable service:

- More complicated hardware, more complicated communication and networking solutions
- Devices are more expensive, service is more expensive

WiFi



Best-effort network, with relatively low-cost devices, low-complexity hardware, low complexity communication and networking protocols

About Cellular Networks

Institute for the Wireless Internet of Things at Northeastern

- Do you want to learn more about cellular networks?
  - **EECE 5576 Wireless Communication Systems:**
    - From fundamentals of the design of cellular networks to standards

Cellular Networks and the IoT

Institute for the Wireless Internet of Things at Northeastern

- While originally cellular networks might not be well aligned with the IoT
  - Solutions are not low-complexity
  - Hardware is not low-cost
  - Service is not low-cost
    - Who is going to pay for a "data plan" for each *Thing*?
- Of course, having global coverage without the need of installing new infrastructure (e.g., access points) is a huge advantage.
  - … they are not going to miss the huge business opportunity that the IoT is!

3GPP

- LTE Cat-M1, LTE-M
  - 'LTE-Light'
  - Smaller front-end (1.4 MHz), half-duplex, 1 antenna → This is much simpler than LTE on your phone!
  - Cheaper chipset
  - Power Saving Mode and Extended Discontinuous Reception

- LTE Cat-M2, NB-IoT
  - Not LTE
  - 200 kHz bands: stand-alone, guard-band, in-band

3GPP

Institute for the Wireless Internet of Things at Northeastern

	LTE Cat 1	LTE Cat 0	LTE Cat M1 (LTE-M)	LTE Cat M2 (NB-IoT)	EC-GSM-IoT
3GPP Release	Release 8	Release 12	Release 13	Release 13	Release 13
Downlink Peak Rate	10 Mbit/s	1 Mbit/s	1 Mbit/s	250 kbit/s	474 kbit/s (EDGE)2 Mbit/s (EGPRS2B)
Uplink Peak Rate	5 Mbit/s	1 Mbit/s	1 Mbit/s	250 kbit/s (multi-tone)20 kbit/s (single-tone)	474 kbit/s (EDGE)2 Mbit/s (EGPRS2B)
Latency	50-100ms	not deployed	10ms-15ms	1.6s-10s	700ms-2s
Number of Antennas	2	1	1	1	1-2
Duplex Mode	Full Duplex	Full or Half Duplex	Full or Half Duplex	Half Duplex	Half Duplex
Device Receive Bandwidth	1.08 - 18 MHz	1.08 - 18 MHz	1.08 MHz	180 kHz	200 kHz
Receiver Chains	2 (MIMO)	1 (SISO)	1 (SISO)	1 (SISO)	1-2
Device Transmit Power	23 dBm	23 dBm	20 / 23 dBm	20 / 23 dBm	23 / 33 dBm

Let's look at all these technologies in retrospective

Technology Classification

Institute for the Wireless Internet of Things at Northeastern

- **"Classical Technologies", Group 1:**
  - RFID
  - IEEE 802.15.4
  - Z-Wave
  - Bluetooth
  - IEEE 802.11
- **Pros:**
  - Low cost to operate (rely on unlicensed spectrum)
  - Low power & low energy consumption
  - Low cost to manufacture
- **Cons:**
  - Limited communication distance: tens to hundreds of meters only…
  - Need for "local" coordinator: tag reader, hub, cellphone, tablet, access point, ...

Technology Classification

Institute for the Wireless Internet of Things at Northeastern

- "**Classical Technologies," Group 2:**
  - Wide Area Networks: 3G/4G/5G
- **Pros:**
  - Long communication range: a single base-station can provide coverage over distances of up to several kilometers
- **Cons:**
  - High cost of the devices: need to run complex communication protocols
    - Think of the cost of a smartphone…
  - High cost of operation: required licensed spectrum
    - Who is going to pay the monthly bill for *billions of things?*

Is there anything better?

Low-Power Wide Area Networks (LPWAN)

- Combine the advantages of low-cost, low-energy PAN/LAN technology with the coverage distance of commercial WANs
- **Different players, common properties:**
  - Network infrastructure in the form of base-stations
  - Utilize very simple physical and link layer communication solutions
    - Similar to those of Bluetooth or primitive versions of Wi-Fi
  - Low data-rates (up to a few kilobits-per-second or kbps)
    - This is not a major concern for the majority of IoT applications
  - Can operate over:
    - Unlicensed spectrum (e.g., ISM bands, like WPAN, WLAN, etc.)
    - Licensed spectrum (e.g., cellular frequency bands)

LPWAN Technologies

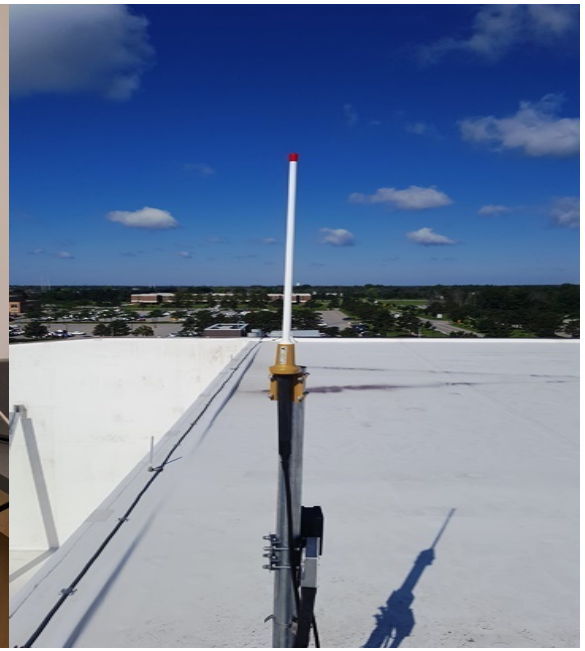
Institute for the Wireless Internet of Things at Northeastern

…

How Do LPWAN Stations Look Like?

Institute for the Wireless Internet of Things at Northeastern

Indoor Gateway



Outdoor Gateway

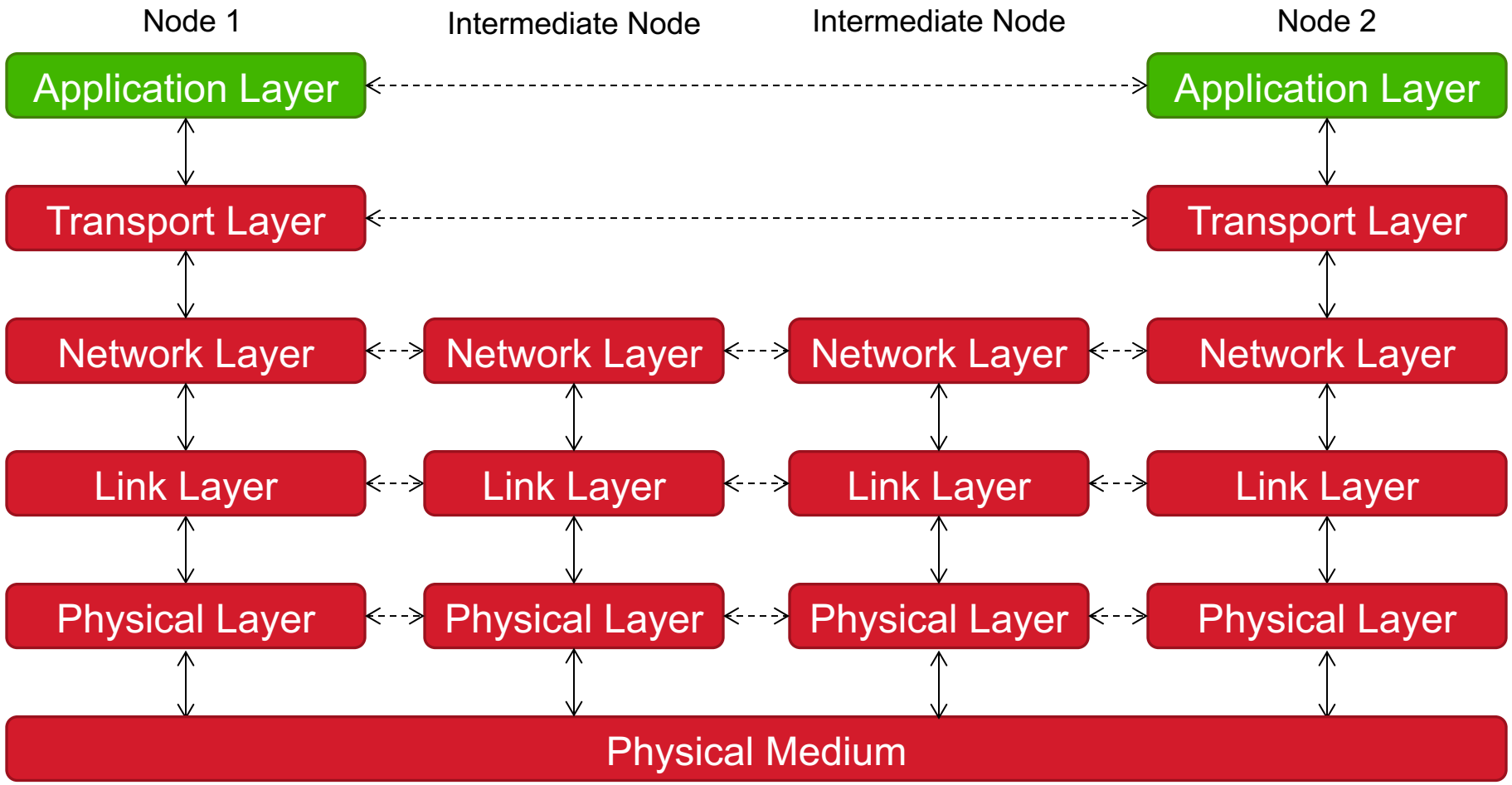
LoRaWAN

Institute for the Wireless Internet of Things at Northeastern

- A proprietary LPWAN standard, defined by the LoRa Alliance and formalized in the LoRaWAN Specification
- Defines both the physical and the link layers:
  - **Physical Layer:**
    - Relies on Long Range (LoRa) modulation or Frequency Shift Keying (FSK) modulation
    - Operates in ISM radio bands
  - **Link Layer:**
    - Designed to allow low-powered devices to communicate with Internet-connected applications over long-range wireless connections
- **Data-rates:** adjustable, up to 50 kilo-bits-per-second (Kbps)
- **Distance:** up to a few kilometers (changes drastically between urban, suburban and rural scenarios)

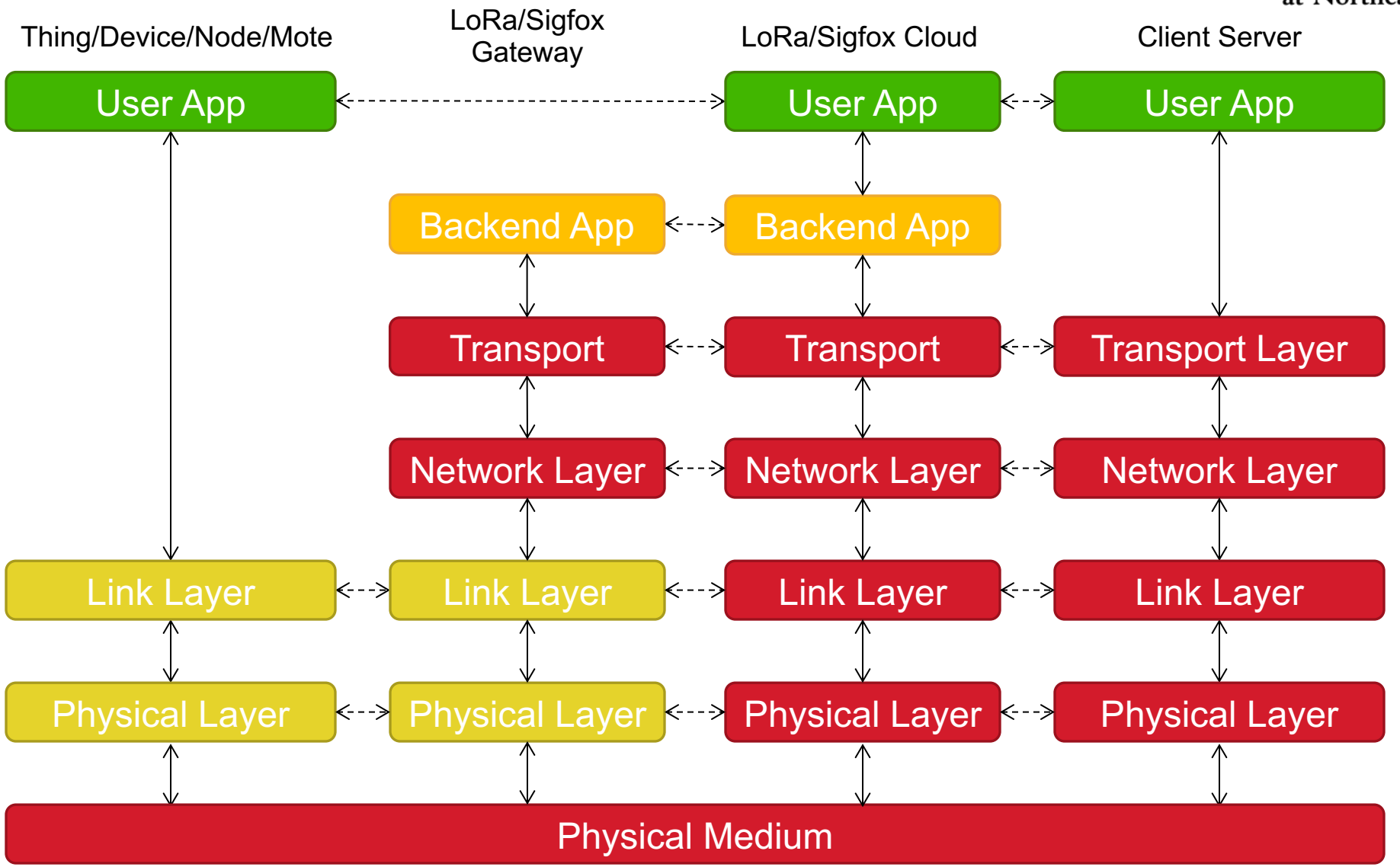
OSI Model – Protocol Stack

Institute for the Wireless Internet of Things at Northeastern



Protocol Stack

Institute for the Wireless Internet of Things at Northeastern



Physical Medium: Frequency Bands

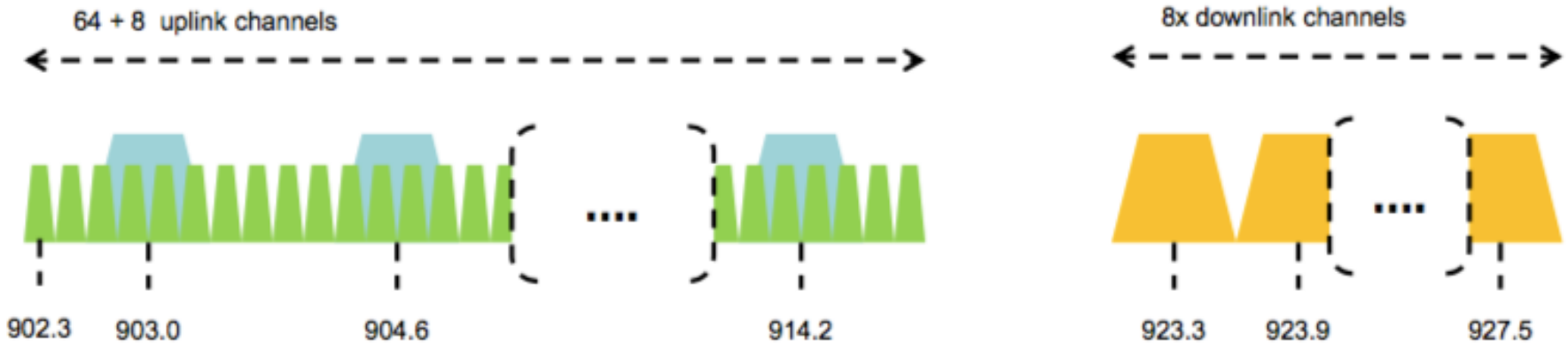
Institute for the Wireless Internet of Things at Northeastern

- **Unlicensed spectrum:**
  - **United States of America:** 902-928 MHz
  - **European Union:** 863-870 MHz
  - **Australia:** 915-928 MHz
  - **China:** 779-787 MHz

Channelization (USA)

Institute for the Wireless Internet of Things at Northeastern

- **Upstream:**
  - 64 channels numbered 0 to 63 utilizing LoRa 125 kHz bandwidth varying from Data Rate (DR) 0 to DR3, using coding rate 4/5, starting at 902.3 MHz and incrementing linearly by 200 kHz to 914.9 MHz
  - 8 channels numbered 64 to 71 utilizing LoRa 500 kHz BW at DR4 starting at 903.0 MHz and incrementing linearly by 1.6 MHz to 914.2 MHz
- **Downstream:**
  - 8 channels numbered 0 to 7 utilizing LoRa 500 kHz BW at DR8 to DR13 starting at 923.3 MHz and incrementing linearly by 600 kHz to 927.5 MHz



Power and Time Limits (USA)

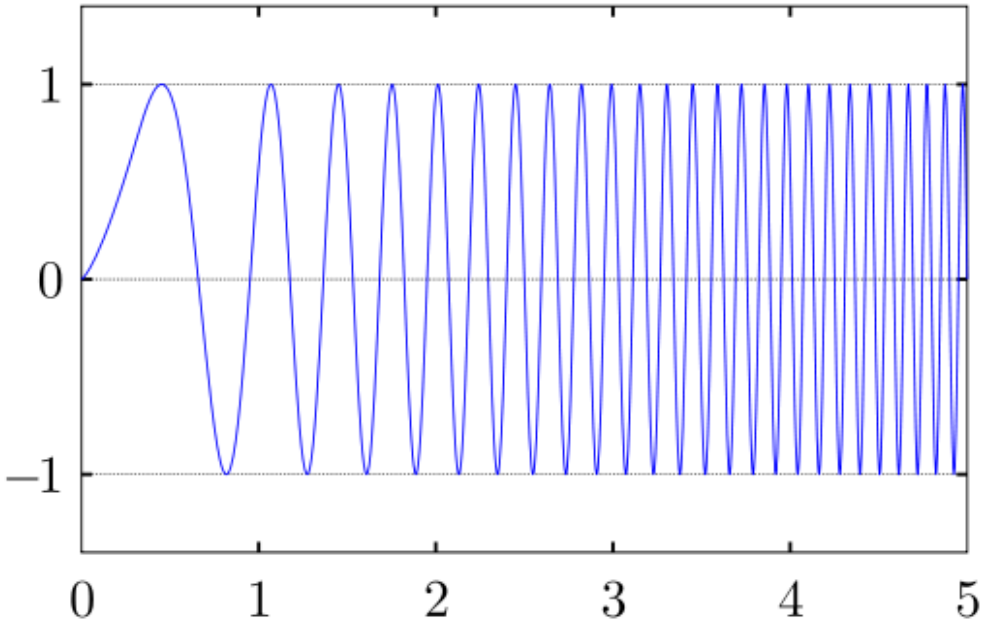
Institute for the Wireless Internet of Things at Northeastern

- **Default radiated power:** 20 dBm
  - Devices, when transmitting with 125 kHz bandwidth, may use a maximum of +30 dBm
  - Devices, when transmitting with 500 kHz bandwidth, may use a maximum of +26 dBm

- **Transmissions shall never last more than 400 ms.**

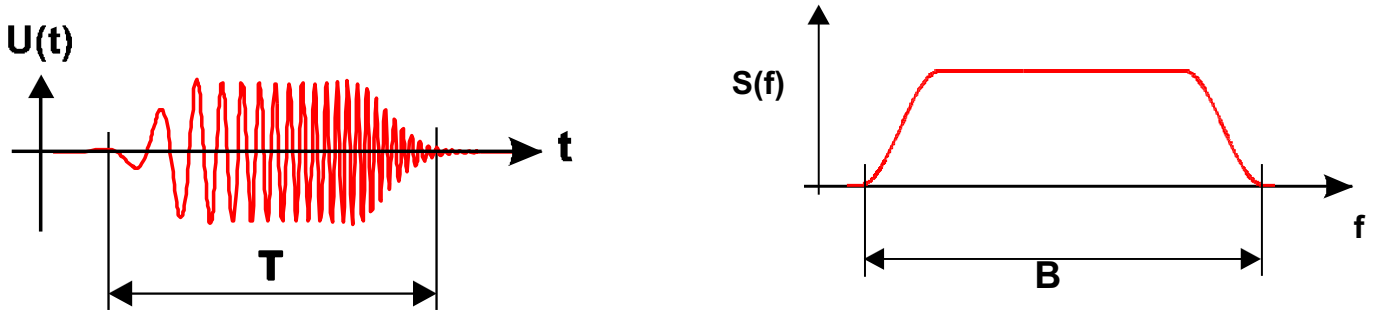
Physical Layer: LoRa (USA)

- LoRa (i.e., Long Range) is a **chirp spread spectrum (CSS)** modulation scheme
  - **Chirp:** Compressed High Intensity Radar Pulse
    - Used by whales and dolphins
    - Patented for radar applications in 1944



Characteristics of Chirp Pulses

- A chirp pulse is a frequency modulated pulse:
  - Within the chirp duration (T), the **frequency is changing in a monotonic manner**
    - From a lower value to a higher one ("Up-Chirp")
    - From a higher value to a lower one ("Down-Chirp")
  - The difference between these two frequencies is a good approximation for the bandwidth B of the chirp pulse



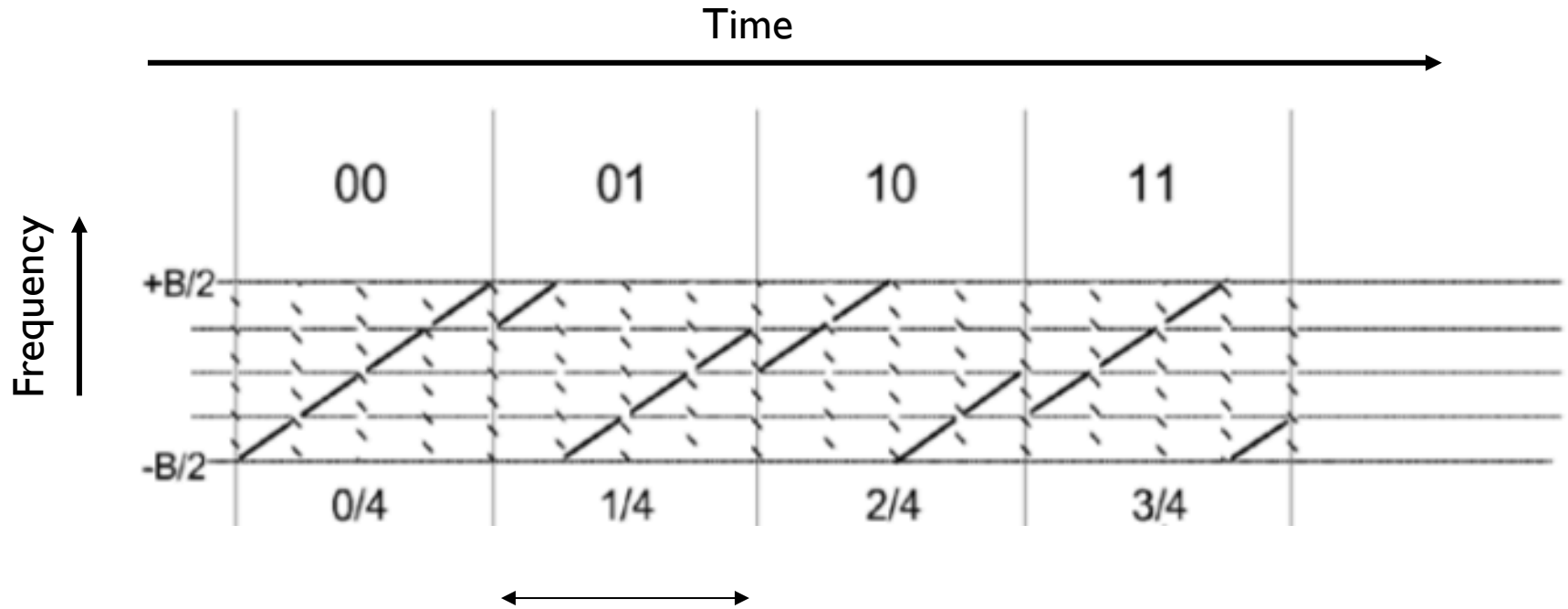
Up-chirp in time and frequency domains (roll-off factor 0.25)

Advantages of CSS

Institute for the Wireless Internet of Things at Northeastern

- **Frequency spreading:**
  - Information theory tells us that CSS benefits when the bandwidth B of the chirp pulse is much higher than the data rate R: B >> R
- **Time spreading:**
  - The data rate can scale independently of the BT product
  - The duration T of the chirp pulse can be chosen freely
  - A signal with a very high BT product can be achieved, which transforms into a very robust signal in the channel
- **Excellent range – data rate scalability:**
  - Preferred for systems where range and/or data rate requirement varies rapidly
  - Especially promising for wideband systems where available frequency bandwidth B is much higher than the data rate R

LoRa Modulation

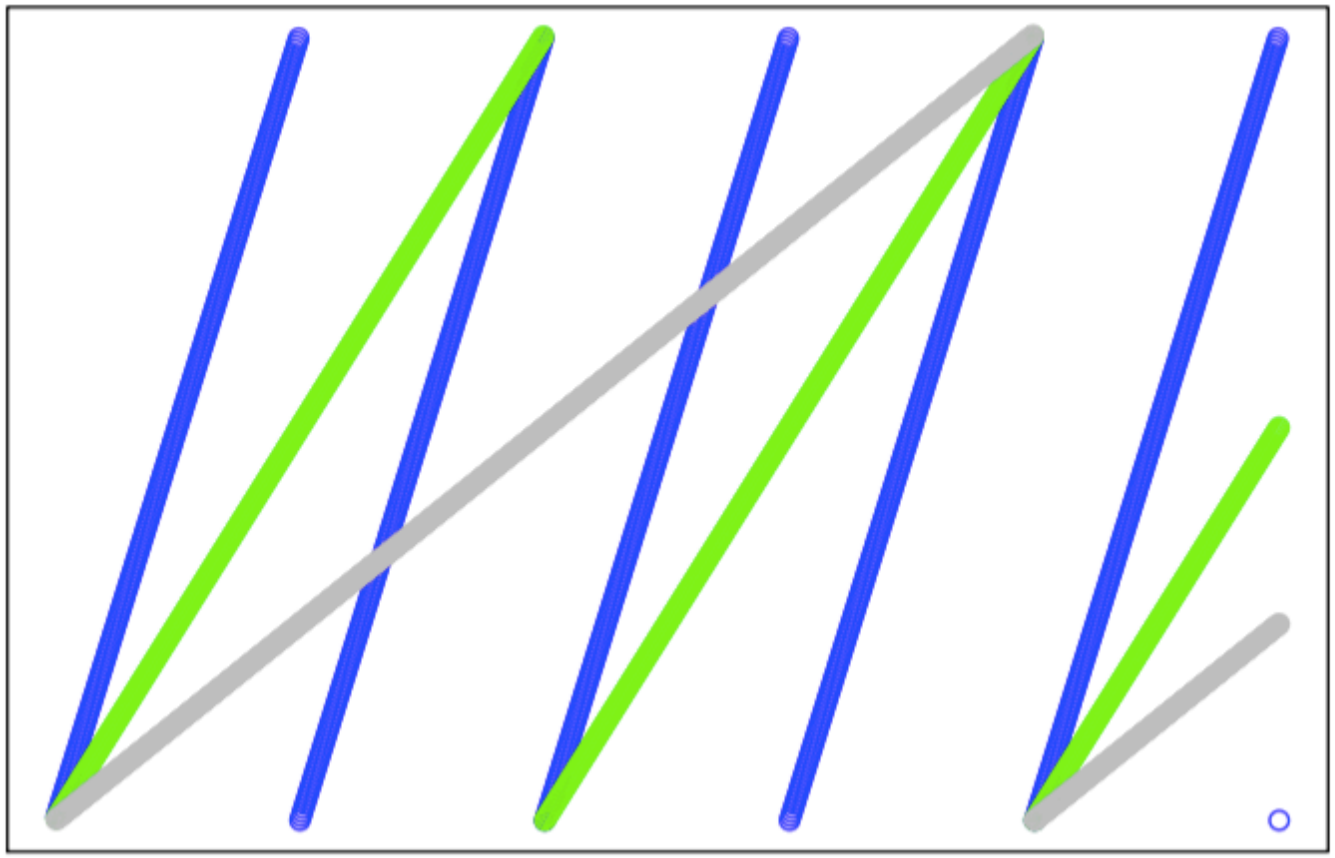


Symbol Time
$T_s=2^{SF}/B$
SF=Spreading factor

From the patent
EP2449690 (B1)

Spreading Factor (SF)

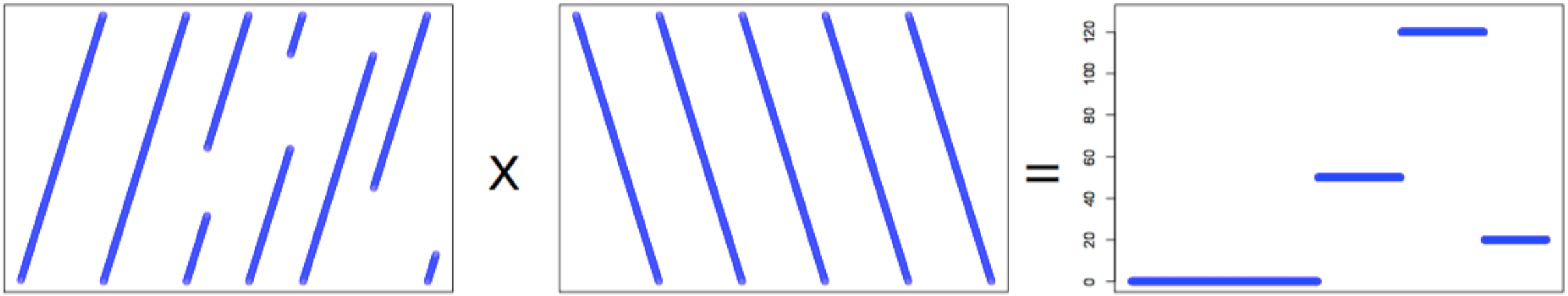
Institute for the Wireless Internet of Things at Northeastern



The spreading determines how quickly the frequency is changed and, thus, the symbol time

LoRa Demodulation

Institute for the Wireless Internet of Things at Northeastern



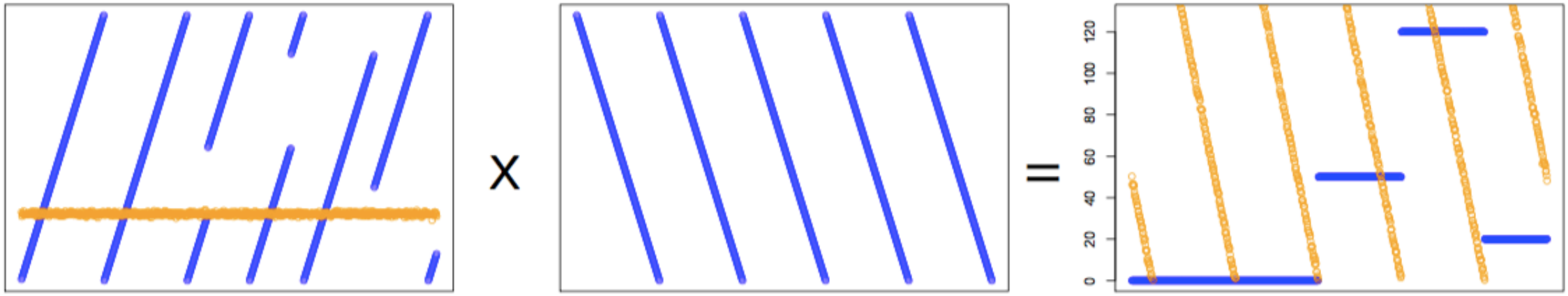
Received Lora signal

Inverse chirp

Decoded symbols

Lora Demodulation with Interference

Institute for the Wireless Internet of Things at Northeastern



Received Lora signal
Narrowband interferer

Inverse chirp

Decoded symbols

Data Rates

Institute for the Wireless Internet of Things at Northeastern

Symbol Rate:

$$R_s = \frac{B}{2^{SF}}$$

SF bits per symbol

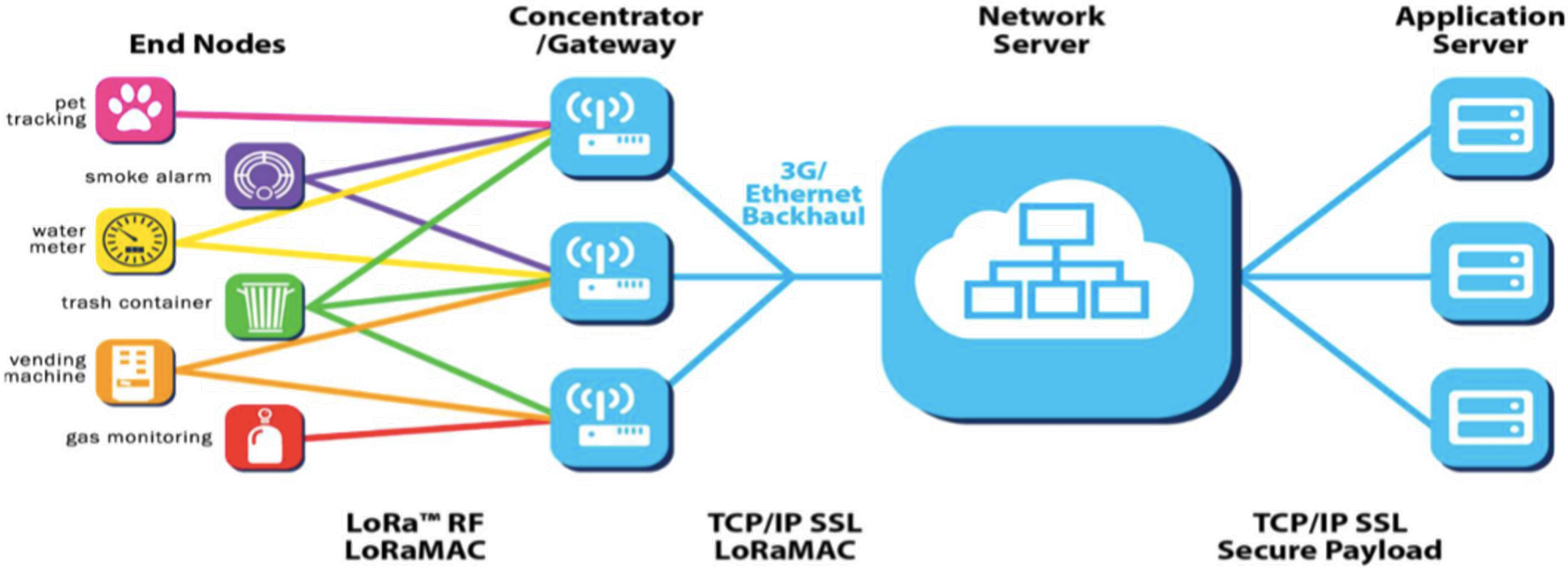
Bit rate:

$$R_b = SF\,\frac{B}{2^{SF}}$$

Data Rate	Configuration	Effective Bit Rate (bps)
0	LoRa: SF10 / 125 kHz	980
1	LoRa: SF9 / 125 kHz	1760
2	LoRa: SF8 / 125 kHz	3125
3	LoRa: SF7 / 125 kHz	5470
4	LoRa: SF8 / 500 kHz	12500
5:7	Future Use	
8	LoRa: SF12 / 500 kHz	980
9	LoRa: SF11 / 500 kHz	1760
10	LoRa: SF10 / 500 kHz	3900
11	LoRa: SF9 / 500 kHz	7000
12	LoRa: SF8 / 500 kHz	12500
13	LoRa: SF7 / 500 kHz	21900
14:15	Future Use	

Link Layer: LoRaWAN

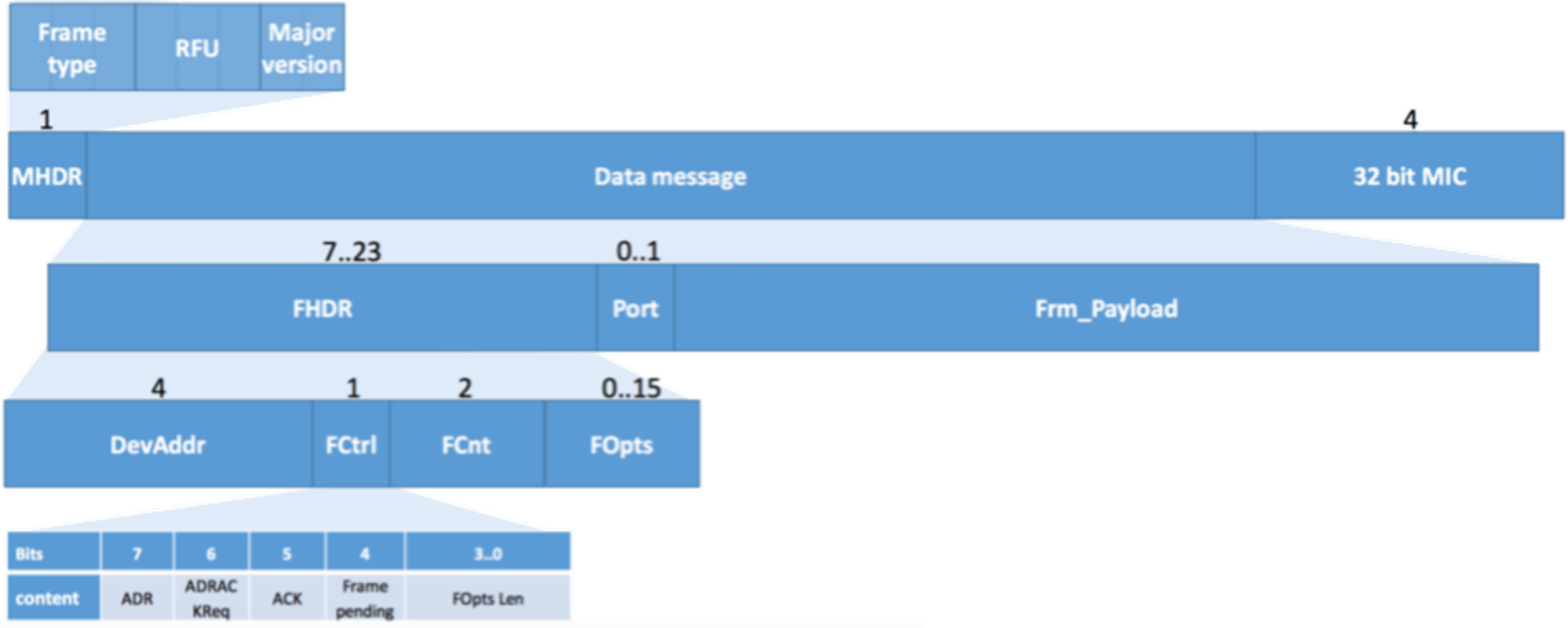
Institute for the Wireless Internet of Things at Northeastern



Frame Format

Institute for the Wireless Internet of Things at Northeastern

Frame type value $B_7\ b_6\ b_5$	Description
000	Join Request
001	Join Accept
010	Unconfirmed Data
011	Confirmed Data
011…110	Reserved for future use
111	Proprietary



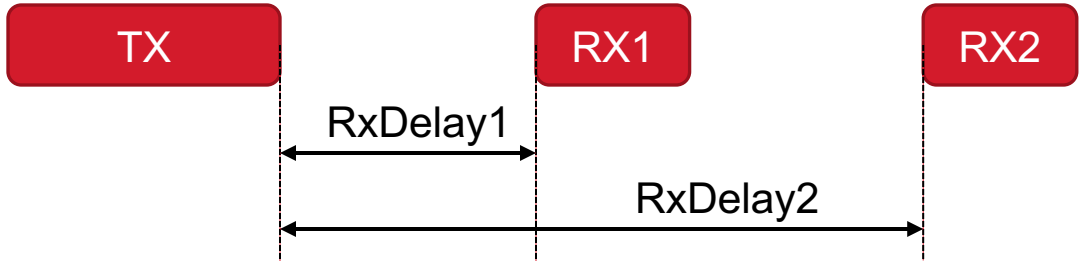
LoRaWAN Device Classes

Institute for the Wireless Internet of Things at Northeastern

- Three classes of devices have been defined, to address specific application requirements:
  - **Class A:** Each device's uplink transmission is followed by two short downlink receive windows.
  - **Class B:** In addition to the Class A functionality, Class B devices open extra receive windows at scheduled times.
  - **Class C:** These devices have a continuous open receive widow, except when transmitting.

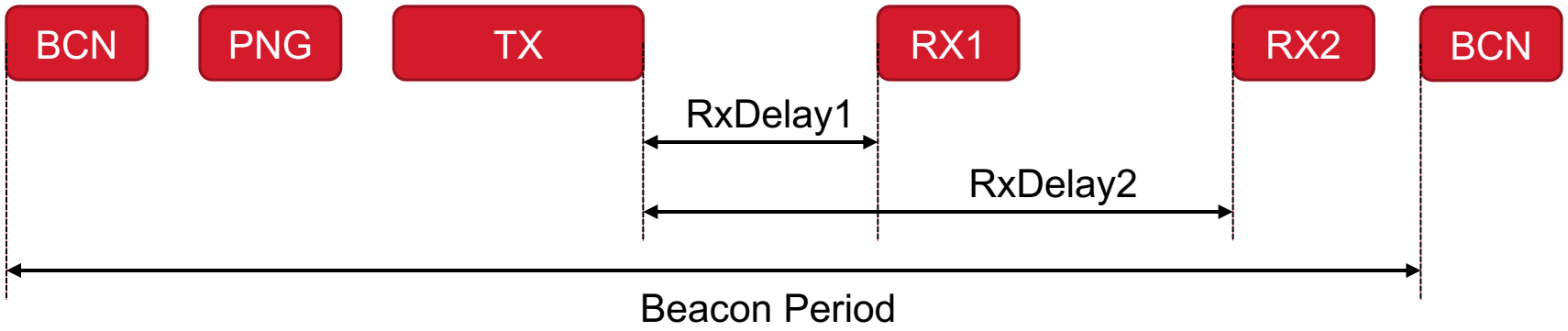
Class A

- Bidirectional communications
- Unicast messages
- Small payloads, long intervals
- End-device initiates communication (uplink))
- Server communicates with end-device (downlink) during predetermined response windows



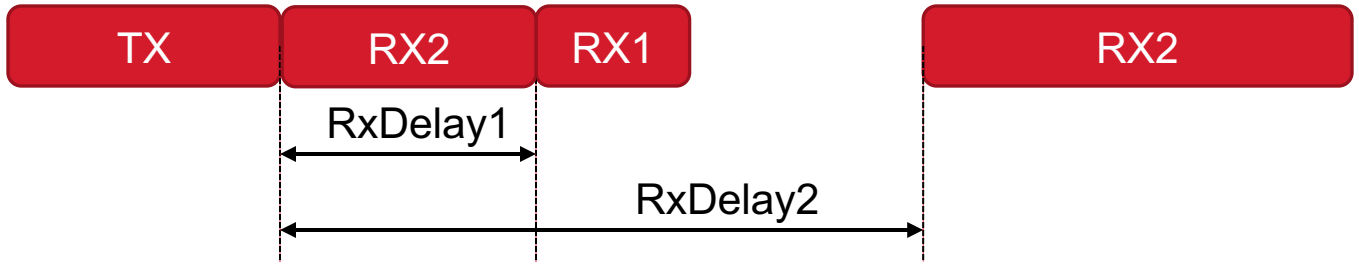
Class B

- Bidirectional with scheduled receive slots
- Unicast and Multicast messages
- Small payloads, long intervals
- Periodic beacon from gateway
- Extra receive window (ping slot)
- Server can initiated transmission at fixed intervals



Class C

- Bidirectional communications
- Unicast and Multicast messages
- Small payloads
- Server can initiate transmission at any time
- End - device is constantly receiving



LoRaWAN Security

Institute for the Wireless Internet of Things at Northeastern

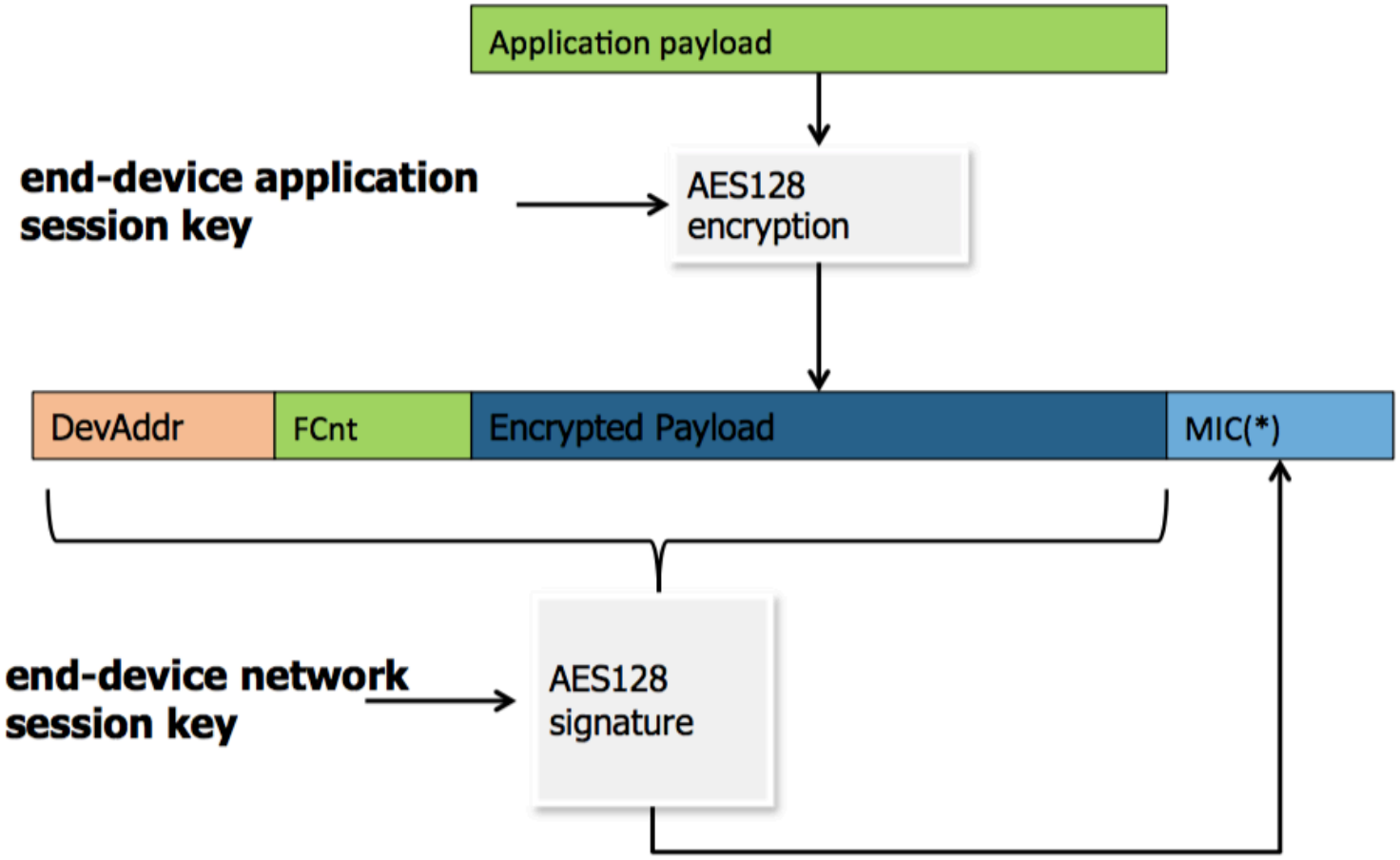
- Two layers of security:
  - Network (nwkSkey):
    - Unique per end-device, Shared between End-device and Network Server
  - Application (appSkey)
    - Unique per end-device, Shared between End-device and Application Server

- AES 128 (128 bit key length)

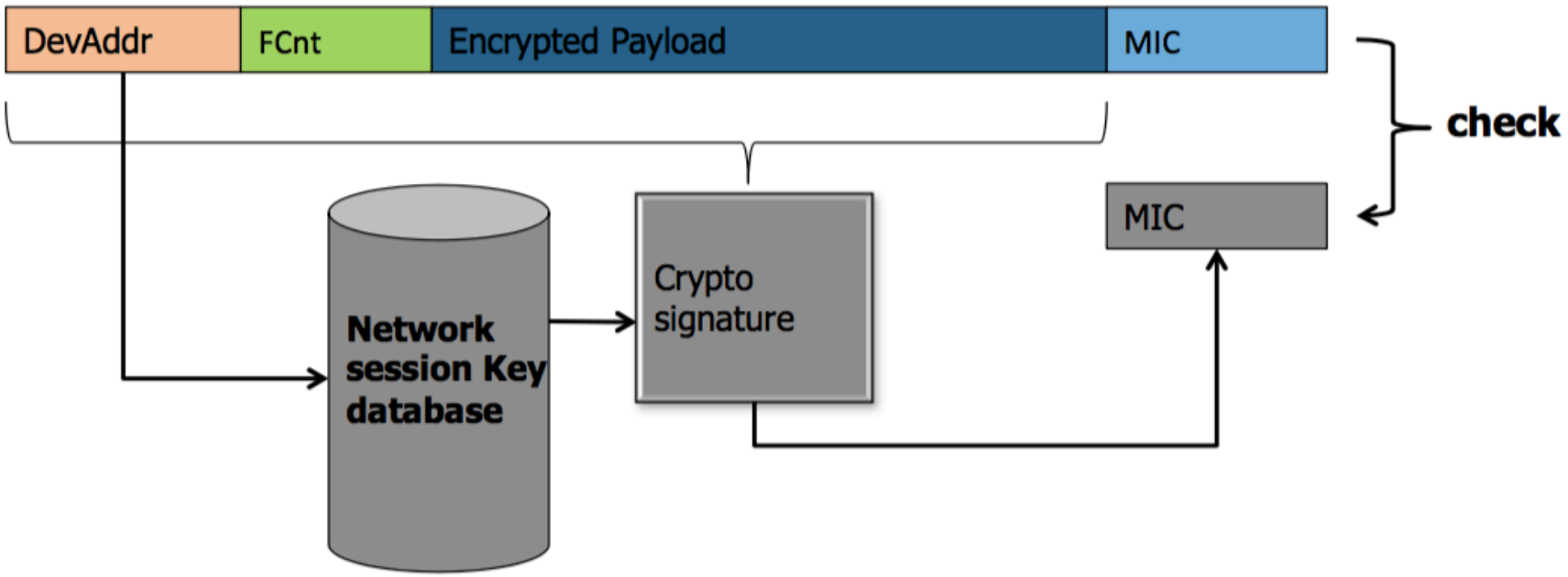
- The network security authenticates the node in the network
  - Message Integrity Check (MIC)

- The application layer of security ensures the network operator does not have access to the application data
  - Sensitive data can optionally be encrypted on top of this with a stronger algorithm

LoRaWAN Security



LoRaWAN Security



LoRaWAN Security

- Activation by Personalization or Over The Air (OTAA)
  - **Activation By Personalization (ABP)**
    - Fixed device addresses and security keys
    - Shared keys stored at production time
    - Locked to a specific network
    - Simple
    - Vulnerable to replay attacks (after a reset)
  - **Over The Air Activation**
    - Based on Globally Unique Identifier
    - New security session keys can be generated from a shared secret
    - Over the air message handshaking
    - Enables roaming

OTAA: Join Process

- Device is provisioned with:
  - **DevEUI** (64 bits): Globally unique end-device identifier
  - **AppEUI** (64 bits): Application identifier
  - **AppKey** (128 bits): Authentication with application key
- Device sends join request message:

Size (bytes)	8	8	2
Join Request	AppEUI	DevEUI	DevNonce

- Network server calculates the session keys:
  - NwkSKey = aes128_encrypt(AppKey, 0x01 | AppNonce | NetID | DevNonce | pad16)
  - AppSKey = aes128_encrypt(AppKey, 0x02 | AppNonce | NetID | DevNonce | pad16)
- Network server sends joi

Size (bytes)	3	3	4	1	1	(16) Optional
Join Accept	AppNonce	NetID	DevAddr	DLSettings	RxDelay	CFList

OTAA: Join Process

- End-device receives Join Accept from application server
- End-device authenticates Join Accept
- End-device decrypts Join Accept
- End-device extracts and stores Device Address (DevAddr)
- End-device derives:
  - NwkSKey = aes128_encrypt(AppKey, 0x01 | AppNonce | NetID | DevNonce | pad16)
  - AppSKey = aes128_encrypt(AppKey, 0x02 | AppNonce | NetID | DevNonce | pad16)

ABP

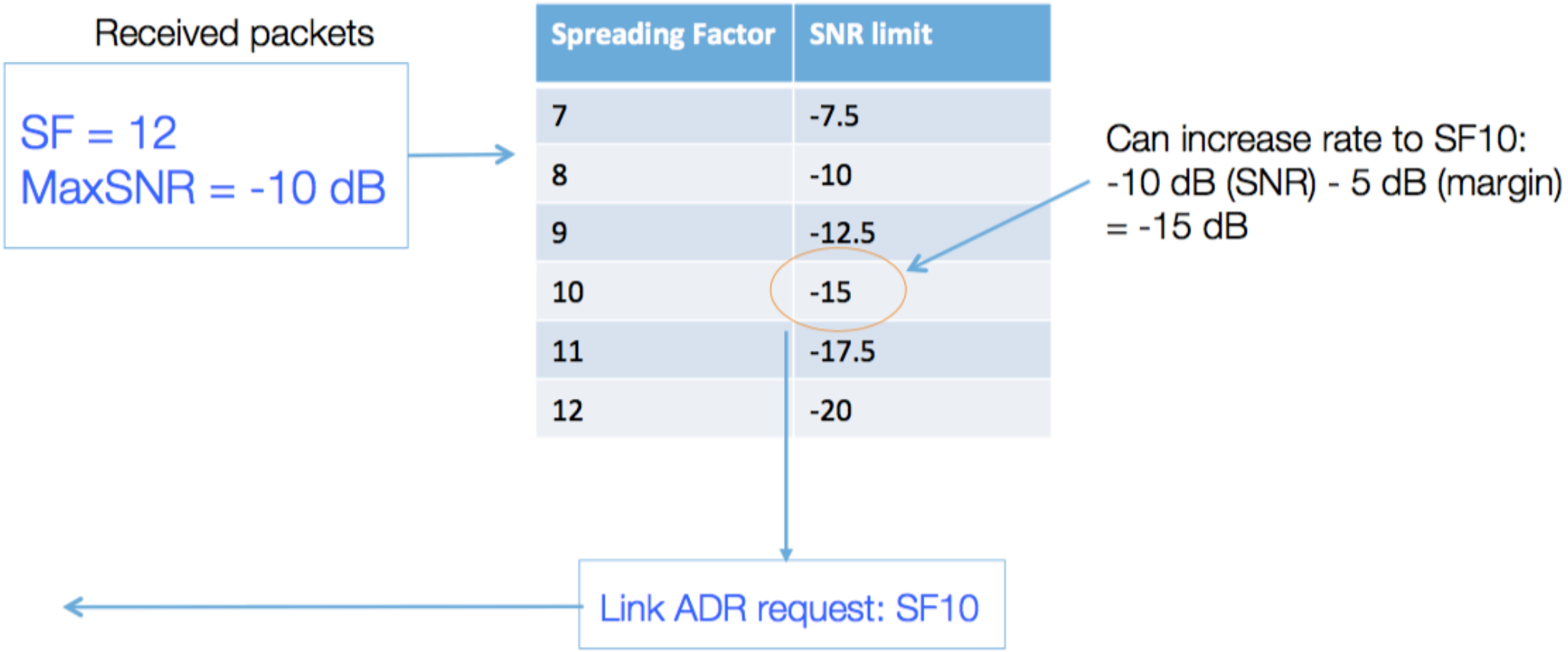
- The following information is configured at production time:
  - Device Address (DevAddr)
  - Network Session Key (NwkSKey)
  - Application Session Key (AppSKey)
- No over the air handshaking
- Device is ready to communicate on the network without any additional procedure

LoRaWAN Scalability

Institute for the Wireless Internet of Things at Northeastern

- Gateways listen on 8 frequencies
- All SF per frequency
  - Can receive concurrently two different SF on the same frequency
- In case of collision, packet with strongest signal gets decoded
- Two dedicated high-speed channels (10 kbps and 50 kbps)
- Adaptive Data Rate (ADR), see next slide
- In case of congestion, scale by adding gateways
  - Nodes get closer to the gateway
  - Due to ADR, spreading factors will be reduced
  - More capacity: multiplicative!

Adaptive Data Rate (ADR)



Sigfox

- As LoRaWAN defines mostly the link layer and the physical layer
- Operates in the same ISM band as LoRaWAN
- Key difference:
  - **Ultranarrowband communication:**
    - 100 Hz channels (randomly placed) within the 200 kHz band
  - **Uplink:** 100 bits-per-second (bps)
    - Differential BPSK modulation
  - **Downlink:** 600 bps
    - Gaussian Frequency Shift Keying (GFSK)
- 12 bytes packets, 3x repetition
- Gateways and servers managed by Sigfox

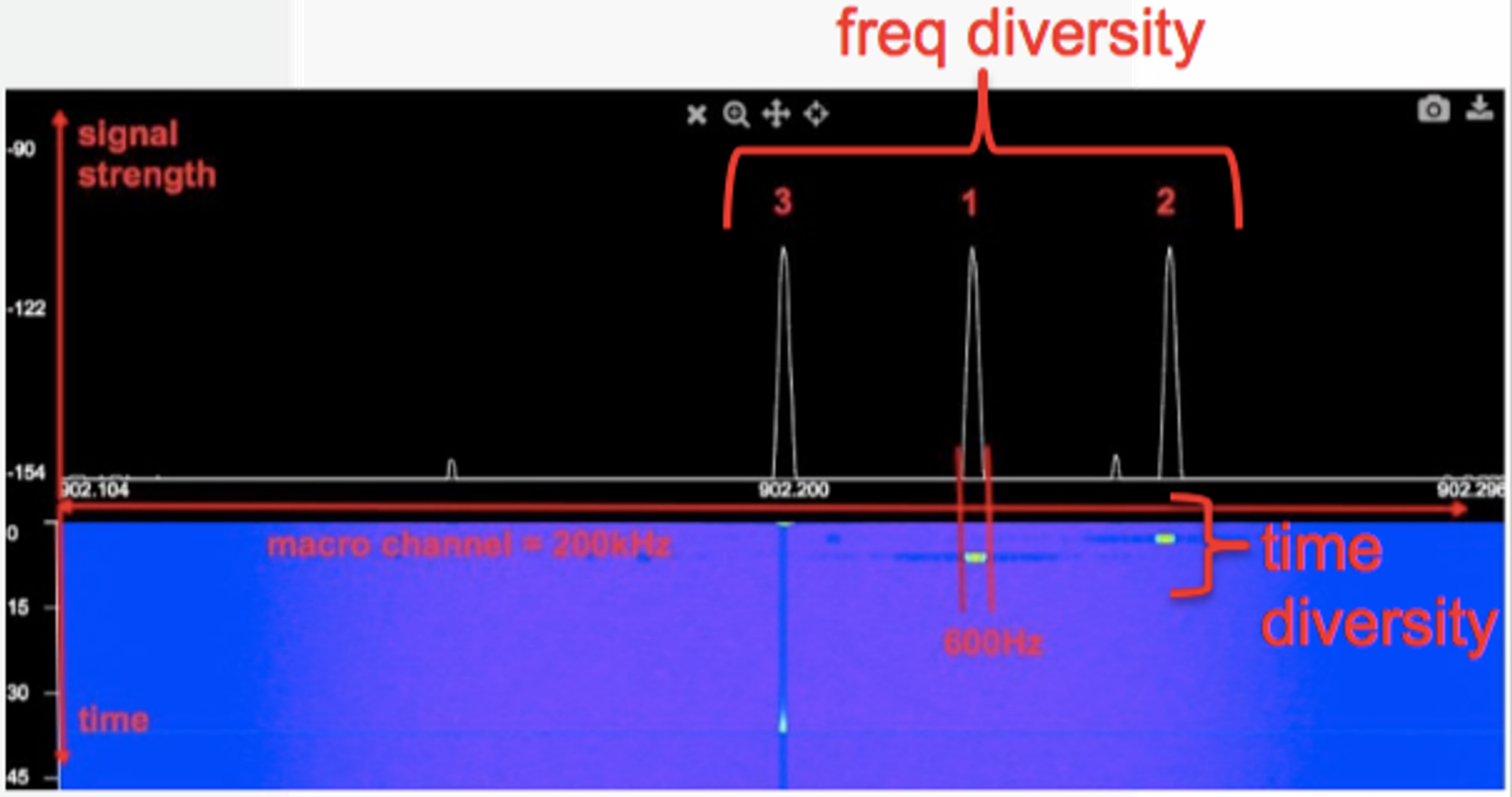
Sigfox Physical Layer

Institute for the Wireless Internet of Things at Northeastern

DIVERSITY

Each message sent over 3 radio frames

- Time diversity
- Frequency diversity

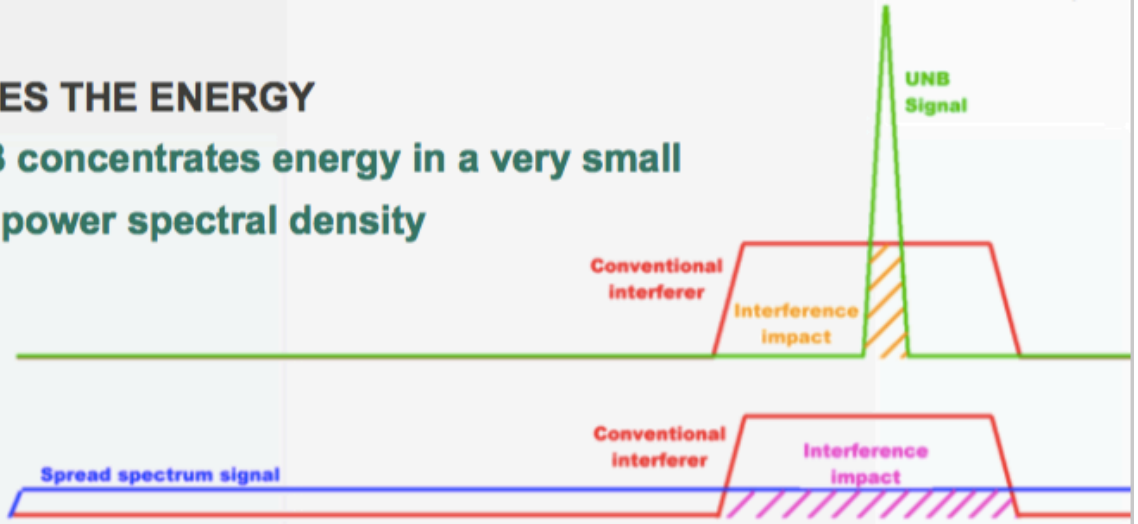


Sigfox Physical Layer

Institute for the Wireless Internet of Things at Northeastern

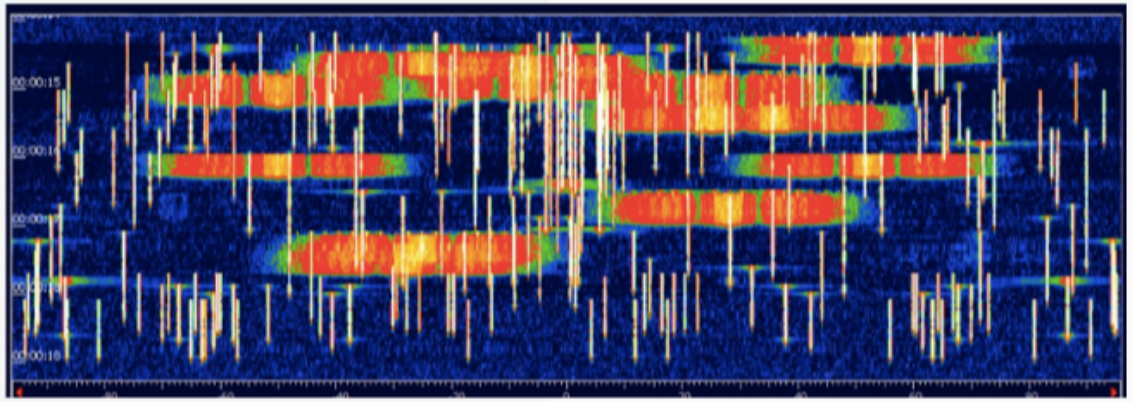
UNB CONCENTRATES THE ENERGY

At equal power UNB concentrates energy in a very small bandwidth = higher power spectral density



UNB REDUCES CHANCES OF COLLISION WITH INTERFERER

Small bandwidth reduces probability of collision with high power interferer



UNB vs CSS

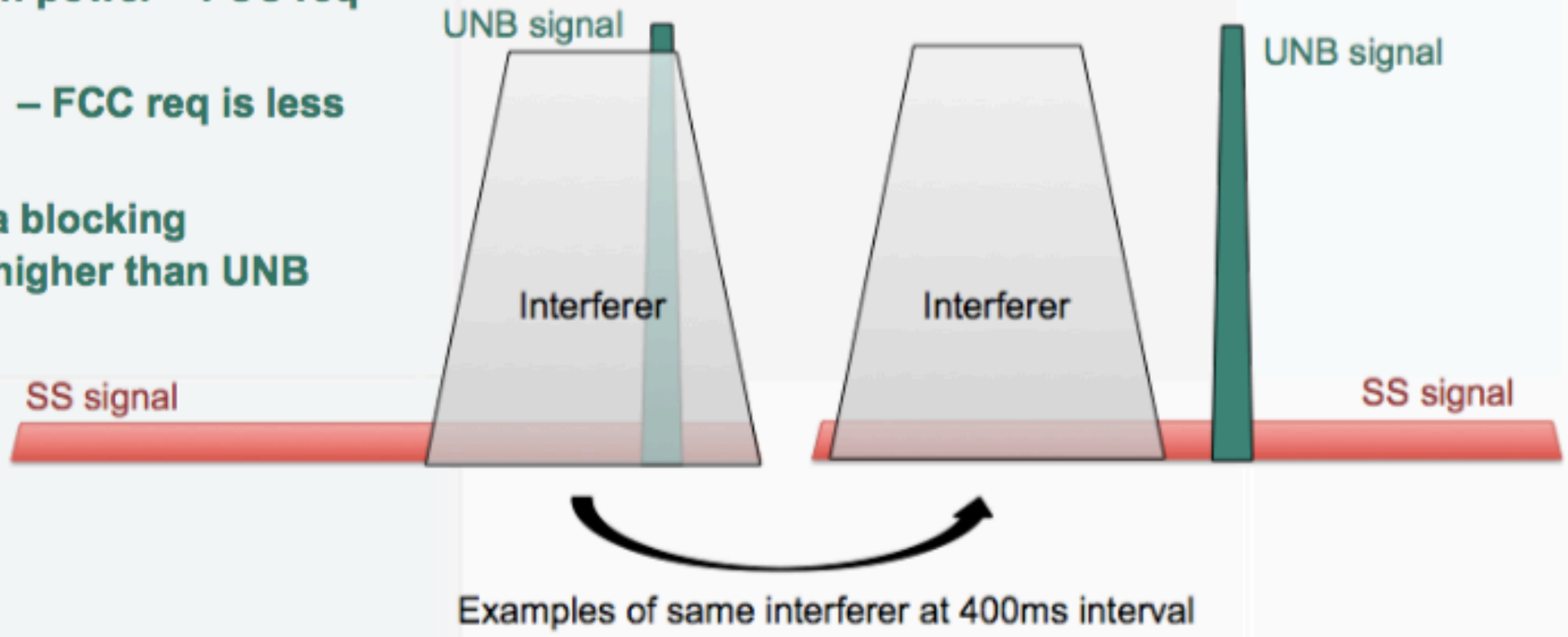
Institute for the Wireless Internet of Things at Northeastern

UNB BETTER RESISTANCE TO INTERFERER

Interferers in ISM band :

- **Can be very high power – FCC req is P<4W**
- **Are hoping fast – FCC req is less than 400ms**

Chances of having a blocking interferer in SS are higher than UNB



Sigfox Link and Network

Institute for the Wireless Internet of Things at Northeastern

UPLINK MESSAGE

PROTOCOL

Each uplink message is self contained – less than 26 bytes

preamble	frame sync	device ID	payload container 0 - 4 - 8 – 12 bytes	authentication hash	CRC

NO NETWORK SYNCHRONIZATION

MOST SIMPLE DESIGN

UPLINK TRANSMISSION

1. Device sends message when needed

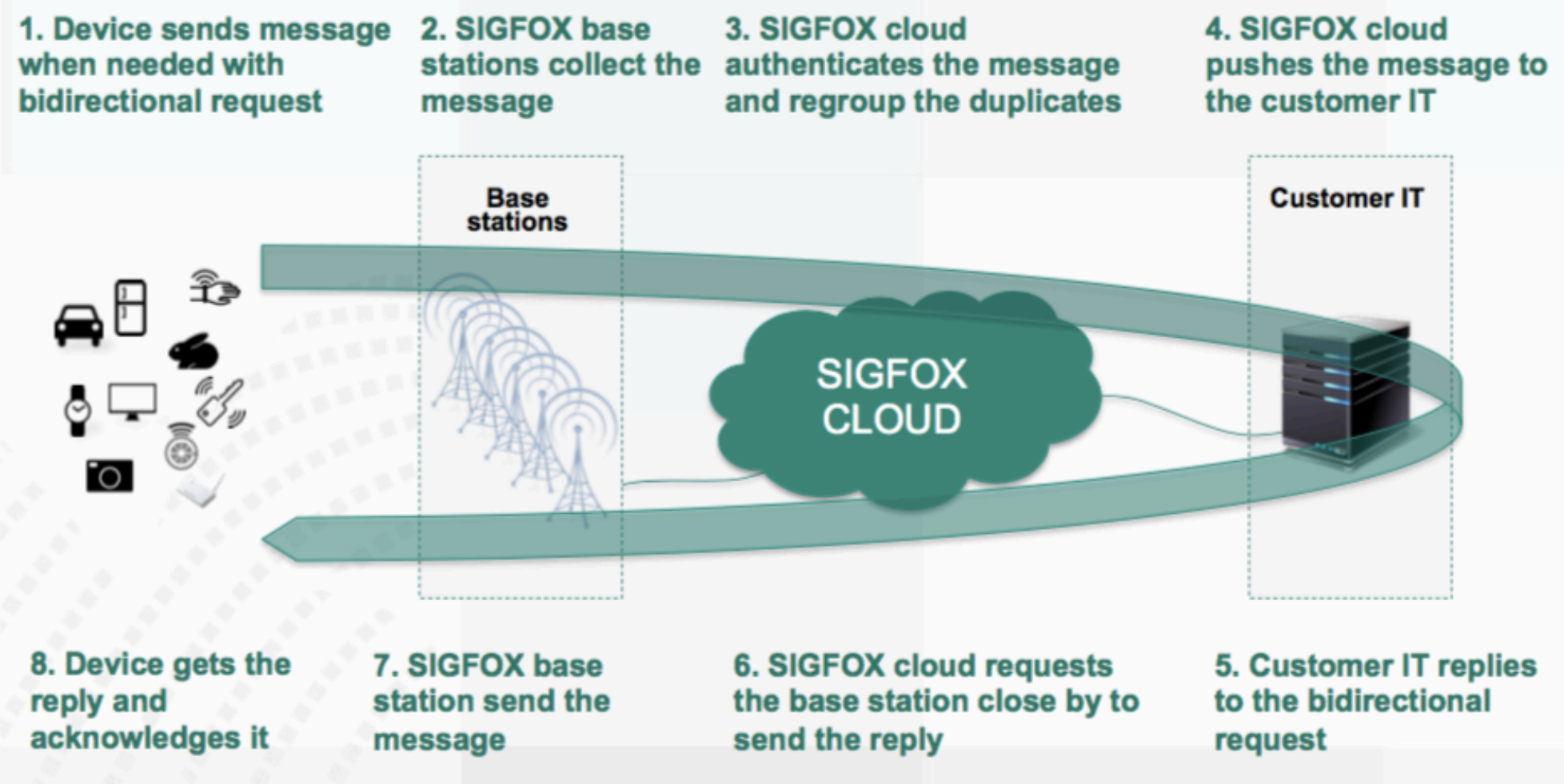
2. SIGFOX base stations collect the message

3. SIGFOX cloud authenticates the message and regroup the duplicates

4. SIGFOX cloud pushes the message to the customer IT

Sigfox Bidirectional Message

Institute for the Wireless Internet of Things at Northeastern



Sigfox Security

Institute for the Wireless Internet of Things at Northeastern

IDENTIFICATION AND AUTHENTICATION

Each device contains a unique ID and secure key

- Identification is done with the ID
- Authentication is done with an AES encrypted signature sent in the header

RESISTANCE TO SPOOFING

Each message contains a sequence number

SIGFOX cloud detects differences in the sequence number

RESISTANCE TO JAMMING

No synchronization is required to send messages on the SIGFOX network
So jamming the device receiver will not affect the delivery of the uplink message

Alternative LPWAN Technologies

Institute for the Wireless Internet of Things at Northeastern

- LinkLabs Symphony Link
  - LoRa based, but synchronized/slotted
- Ingenu
- 802.11ah
- Weightless-N
- Weightless-P

Next Steps

Institute for the Wireless Internet of Things at Northeastern

- Research paper:
  - Due on November 20
- Second computer laboratory assignment:
  - Due on November 15

- Coming soon:
  - Homework assignment (numerical)
  - Online (open-book) quiz (multiple choice questions)