
Modern Wireless Networks











Communication for Internet of Things



ICEN 574– Spring 2019

Prof. Dola Saha

Viability Options for IoT Communication

	Local Area Network Short Range Communication	Low Power Wide Area (LPWAN) Internet of Things	Cellular Network Traditional M2M
	40%	45%	15%
	Well established standards In building	Low power consumption Low cost Positioning	Existing coverage High data rate
	Battery Live Provisioning Network cost & dependencies	High data rate Emerging standards	Autonomy Total cost of ownership
	  		  

LPWAN – Design Goals

- Long Range (few Km in urban to 10s of Km in rural)
 - Use of sub-1 GHz band (*exception*: WEIGHTLESS-W, INGENU)
 - Modulation Techniques:
 - Narrowband (SigFox, NB-IoT) or
 - Spread Spectrum (LoRa)
- Ultra low power operation
 - Topology (star over mesh)
 - Duty Cycling (sleep/wake)
 - Lightweight Medium Access Control (ALOHA or TDMA)
 - Offloading complexity from end device

LPWAN – Design Goals

- Low Cost (per hardware cost < \$5)
 - Reduction in hardware complexity
 - Minimum infrastructure
 - Using license-free or owned licensed bands
- Scalability
 - Diversity techniques
 - Densification
 - Adaptive channel selection and data rate
- Quality of Service

Proprietary Technologies

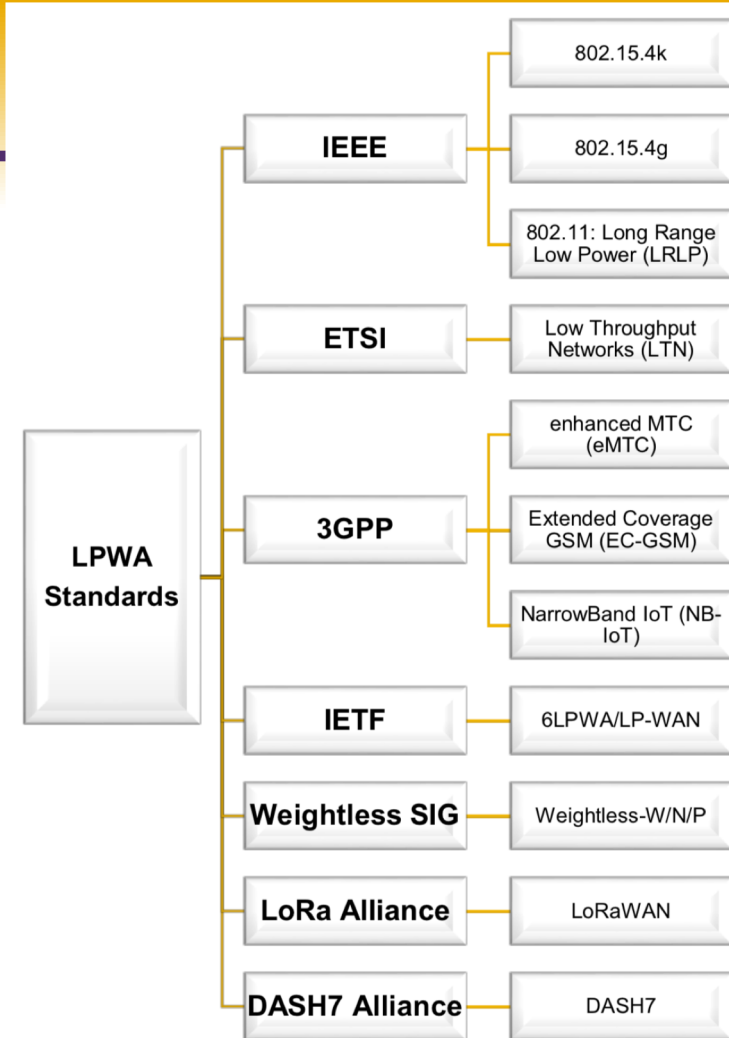
TABLE I
TECHNICAL SPECIFICATIONS OF VARIOUS LPWA TECHNOLOGIES (?=NOT KNOWN)

	SIGFOX	LoRAWAN	INGENU	TELENSA
Modulation	UNB DBPSK(UL), GFSK(DL)	CSS	RPMA-DSSS(UL), CDMA(DL)	UNB 2-FSK
Band	SUB-GHZ ISM:EU (868MHz), US(902MHz)	SUB-GHZ ISM:EU (433MHz, 868MHz), US (915MHz), Asia (430MHz)	ISM 2.4GHz	SUB-GHZ bands including ISM:EU (868MHz), US (915MHz), Asia (430MHz)
Data rate	100 bps(UL), 600 bps(DL)	0.3-37.5 kbps (LoRa), 50 kbps (FSK)	78kbps (UL), 19.5 kbps(DL) [39]	62.5 bps(UL), 500 bps(DL)
Range	10 km (URBAN), 50 km (RURAL)	5 km(URBAN), 15 km (RURAL)	15 km (URBAN)	1 km (URBAN)
Num. of channels / orthogonal signals	360 channels	10 in EU, 64+8(UL) and 8(DL) in US plus multiple SFs	40 1MHz channels, up to 1200 signals per channel	multiple channels
Link symmetry	×	✓	×	×
Forward error correction	×	✓	✓	✓
MAC	unslotted ALOHA	unslotted ALOHA	CDMA-like	?
Topology	star	star of stars	star, tree	star
Adaptive Data Rate	×	✓	✓	×
Payload length	12B(UL), 8B(DL)	up to 250B (depends on SF & region)	10KB	?
Handover	end devices do not join a single base station	end devices do not join a single base station	✓	?
Authentication & encryption	encryption not supported	AES 128b	16B hash, AES 256b	?
Over the air updates	×	✓	✓	✓
SLA support	×	×	×	×
Localization	×	✓	×	×

LPWAN Standards

➤ IEEE:

- IEEE 802.15.4k: Low Energy, Critical Infrastructure Monitoring Networks (DSSS and FSK as two PHY layers)
- IEEE 802.15.4g: Low-Data-Rate, Wireless, Smart Metering Utility Networks (three PHY layers: FSK, OFDMA, and offset Quaternary Phase Shift Keying (QPSK))
- IEEE 802.11: Wireless Local Area Networks (slower OFDM)



LPWAN Standards

➤ 3GPP

- LTE enhancements for Machine Type Communications (eMTC)
- EC-GSM (Extended Coverage GSM)
- NB-IoT (narrowband IoT)

Technical Specs

TABLE II
TECHNICAL SPECIFICATIONS OF VARIOUS LPWA STANDARDS

Standard	IEEE		WEIGHTLESS-W	WEIGHTLESS-SIG		DASH7 Alliance DASH7
	802.15.4k	802.15.4g		WEIGHTLESS-N	WEIGHTLESS-P	
Modulation	DSSS, FSK	MR-(FSK, OFDMA, OQPSK)	16-QAM, BPSK, QPSK, DBPSK	UNB DBPSK	GMSK, offset-QPSK	GFSK
Band	ISM SUB-GHZ & 2.4GHZ	ISM SUB-GHZ & 2.4GHZ	TV white spaces 470-790MHz	ISM SUB-GHZ EU (868MHz), US (915MHz)	SUB-GHZ ISM or licensed	SUB-GHZ 433MHz, 868MHz, 915MHz
Data rate	1.5 bps-128 kbps	4.8 kbps-800 kbps	1 kbps-10 Mbps	30 kbps-100 kbps	200 bps-100kbps	9.6,55.6,166.7 kbps
Range	5 km (URBAN)	up to several kms	5 km (URBAN)	3 km (URBAN)	2 km (URBAN)	0-5 km (URBAN)
Num. of channels / orthogonal signals	multiple channels. Number depends on channel & modulation		16 or 24 channels(UL)	multiple 200 Hz channels	multiple 12.5 kHz channels	3 different channel types (number depends on type & region)
Forward error correction	✓	✓	✓	✗	✓	✓
MAC	CSMA/CA, CSMA/CA or ALOHA with PCA	CSMA/CA	TDMA/FDMA	slotted ALOHA	TDMA/FDMA	CSMA/CA
Topology	star	star, mesh, peer-to-peer (depends on upper layers)	star	star	star	tree, star
Payload length	2047B	2047B	>10B	20B	>10B	256B
Authentication & encryption	AES 128b	AES 128b	AES 128b	AES 128b	AES 128/256b	AES 128b

Low Power Wide-Area Networks (LPWAN)

Technologies	LTE-Evolution	Narrowband			Non-3GPP	
	LTE-M	NB-IoT		EC-GSM	LoRa	SigFox
		NB-LTE	NB-ClIoT			
Coverage	< 11 km	< 15 km	< 15 km	< 15 km	< 20 km	< 13 km
Spectrum	Licensed (7-900 MHz)	Licensed (7-900 MHz)	Licensed (8-900 MHz)	Licensed (7-900 MHz)	Unlicensed (867-869 MHz or 902-928 MHz)	Unlicensed (900 MHz)
Bandwidth	1.4 MHz	200 kHz	200 kHz	2.4 MHz	125 kHz, 250 kHz, 500 kHz	100 kHz
Date Rate	< 1 Mbps	< 150 kbps	< 400 kbps	10 kbps	< 50 kbps	< 100 bps
Battery Life	> 10 years	> 10 years	< 10 years	> 10 years	< 10 years	> 10 years

Feature	LoRaWAN	Narrow-Band	LTE Cat-1 2016 (Rel12)	LTE Cat-M 2018 (Rel13)	NB-LTE 2019(Rel13+)
Modulation	SS Chirp	UNB / GFSK/BPSK	OFDMA	OFDMA	OFDMA
Rx bandwidth	500 - 125 KHz	100 Hz	20 MHz	20 - 1.4 MHz	200 KHz
Data Rate	290bps - 50Kbps	100 bit/sec 12 / 8 bytes Max	10 Mbit/sec	200kbps – 1Mbps	~20K bit/sec
Max. # Msgs/day	Unlimited	UL: 140 msgsg/day	Unlimited	Unlimited	Unlimited
Max Output Power	20 dBm	20 dBm	23 - 46 dBm	23/30 dBm	20 dBm
Link Budget	154 dB	151 dB	130 dB+	146 dB	150 dB
Batery lifetime - 2000mAh	105 months	90 months		18 months	
Power Efficiency	Very High	Very High	Low	Medium	Med high
Interference immunity	Very high	Low	Medium	Medium	Low
Coexistence	Yes	No	Yes	Yes	No
Security	Yes	No	Yes	Yes	Yes
Mobility / localization	Yes	Limited mobility, No loc	Mobility	Mobility	Limited Mobility No Loc

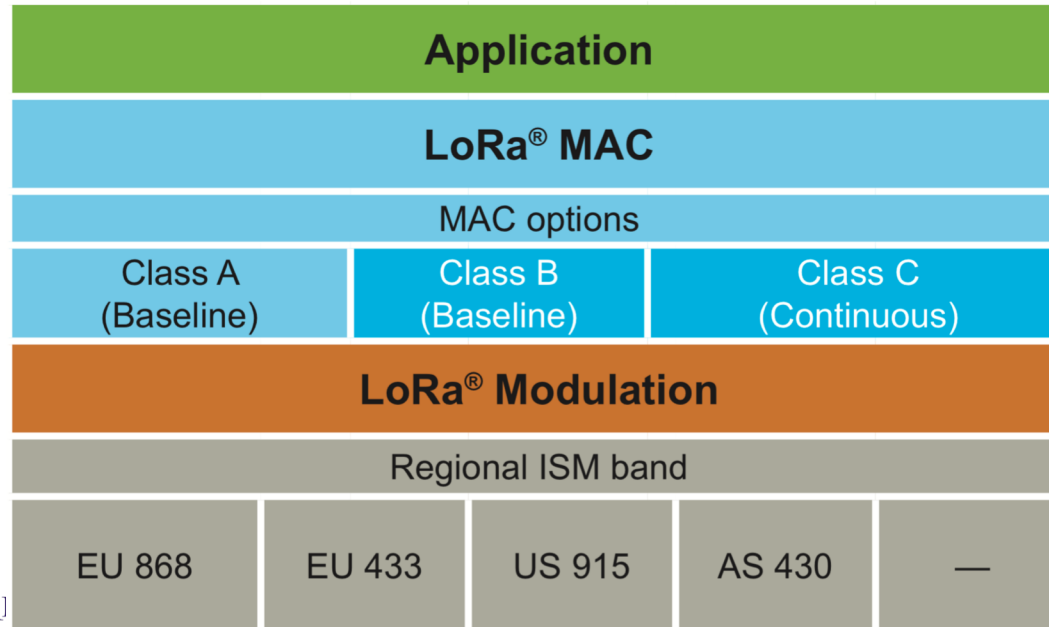
LoRaWAN



UNIVERSITY
AT ALBANY
State University of New York

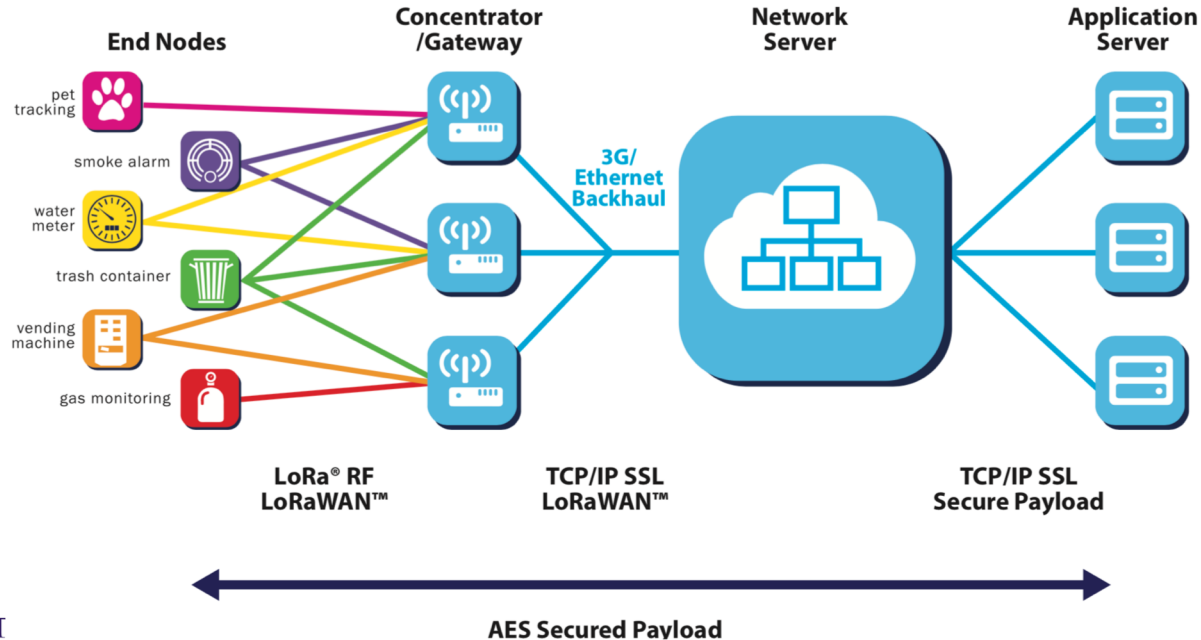
LoRaWAN

- LoRaWAN defines the communication protocol and system architecture for the network
- LoRa physical layer enables the long-range communication link.



Network Architecture

- Long range star architecture
- Preserves battery power compared to Mesh

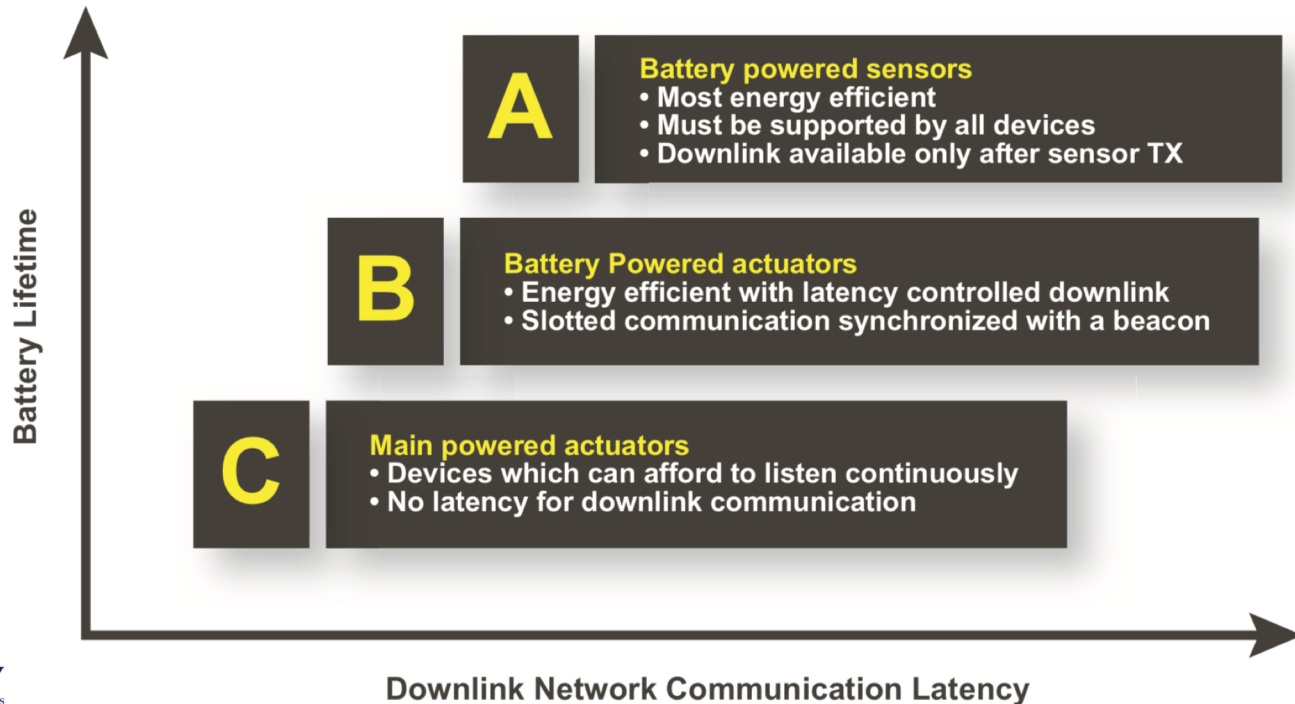


Network Architecture

- Nodes are NOT connected to specific gateway
 - Data transmitted by a node is received by multiple gateways
 - Each gateway will forward the received packet to the cloud-based network server via some backhaul (cellular/Wi-Fi)
 - The intelligence and complexity is pushed to the network server
 - Manages the network
 - Filters redundant received packets
 - Performs security checks
 - Schedules acknowledgments through the optimal gateway
 - Performs adaptive data rate
- Handover is not required

Device Classes

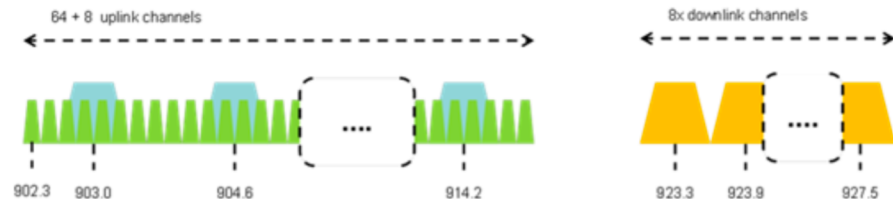
- The device classes trade off network downlink communication latency versus battery lifetime.



Regional Summary

	Europe	North America	China	Korea	Japan	India
Frequency band	867-869MHz	902-928MHz	470-510MHz	920-925MHz	920-925MHz	865-867MHz
Channels	10	64 + 8 + 8	In definition by Technical Committee	In definition by Technical Committee	In definition by Technical Committee	In definition by Technical Committee
Channel BW Up	125/250kHz	125/500kHz				
Channel BW Dn	125kHz	500kHz				
TX Power Up	+14dBm	+20dBm typ (+30dBm allowed)				
TX Power Dn	+14dBm	+27dBm				
SF Up	7-12	7-10				
Data rate	250bps- 50kbps	980bps-21.9kbps				
Link Budget Up	155dB	154dB				
Link Budget Dn	155dB	157dB				

- The ISM band for North America is from **902-928MHz**.
- LoRaWAN defines **64, 125kHz uplink** channels from 902.3 to 914.9MHz in 200kHz increments.
- There are an additional **eight 500kHz uplink** channels in 1.6MHz increments from 903MHz to 914.9MHz.
- The eight **downlink** channels are **500kHz** wide starting from 923.3MHz to 927.5MHz.
- The maximum output power in North America is **+30dBm** but for most devices +20dBm is sufficient.
- Under FCC there are no duty cycle limitations but there is a 400msec max dwell time per channel.



Physical Message Format

➤ Uplink

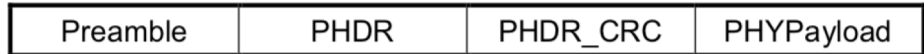
Uplink PHY:



- LoRa physical header (**PHDR**) plus a header CRC (**PHDR_CRC**)
- The integrity of the payload is protected by a CRC
- The **PHDR**, **PHDR_CRC** and payload **CRC** fields are inserted by the radio transceiver.

➤ Downlink

Downlink PHY:



- No payload integrity check is done at this level to keep messages as short as possible with minimum impact on any duty-cycle limitations of the ISM bands used

MAC Message Format

- All LoRa uplink and downlink messages carry a PHY payload (**Payload**) starting with a single-octet MAC header (**MHDR**), followed by a MAC payload (**MACPayload**), and ending with a 4-octet message integrity code (**MIC**)
- Maximum MACPayload size depends on region

Radio PHY layer:



Figure 5: Radio PHY structure (CRC* is only available on uplink messages)

PHYPayload:

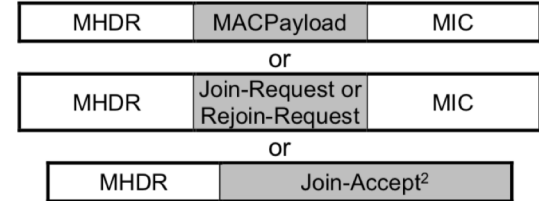


Figure 6: PHY payload structure

MACPayload:



Figure 7: MAC payload structure

FHDR:



Figure 8: Frame header structure

Size (bytes)	1	7..M	4
PHYPayload	MHDR	MACPayload	MIC

Figure 9: PHY payload format

MAC Header

- Mtype: Message Type
- RFU: Reserved for Future Use
- Major: Major Version

Bit#	7..5	4..2	1..0
MHDR bits	MType	RFU	Major

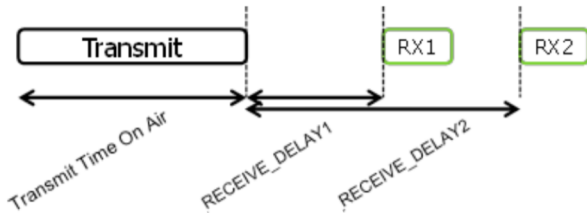
Figure 10: MAC header field content

MType	Description
000	Join-request
001	Join-accept
010	Unconfirmed Data Up
011	Unconfirmed Data Down
100	Confirmed Data Up
101	Confirmed Data Down
110	Rejoin-request
111	Proprietary



Frame Header

- Adaptive Data Rate (ADR) - when this is enabled the network will be optimized to use the fastest data rate possible.
- After ADR_ACK_LIMIT uplinks ($ADR_ACK_CNT \geq ADR_ACK_LIMIT$) without any downlink response, it sets the ADR acknowledgment request bit (**ADRACKReq**)
- The network is required to respond with a downlink frame



Size (bytes)	4	1	2	0..15
FHDR	DevAddr	FCtrl	FCnt	FOpts

Figure 11 : Frame header format

Bit#	7	6	5	4	[3..0]
FCtrl bits	ADR	RFU	ACK	FPending	FOptsLen

Figure 12 : downlink FCtrl fields

Bit#	7	6	5	4	[3..0]
FCtrl bits	ADR	ADRACKReq	ACK	ClassB	FOptsLen

Figure 13 : uplink FCtrl fields

Class B - Beacon

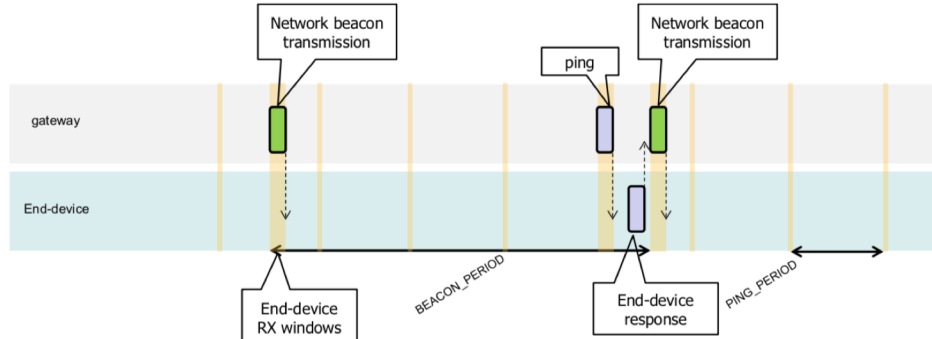


Figure 50: Beacon reception slot and ping slots

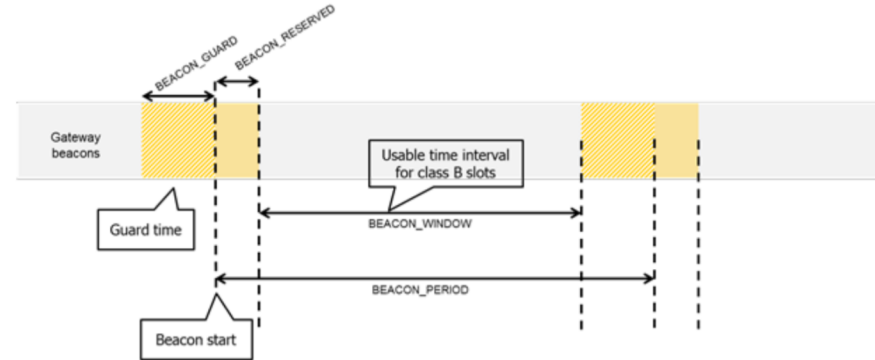


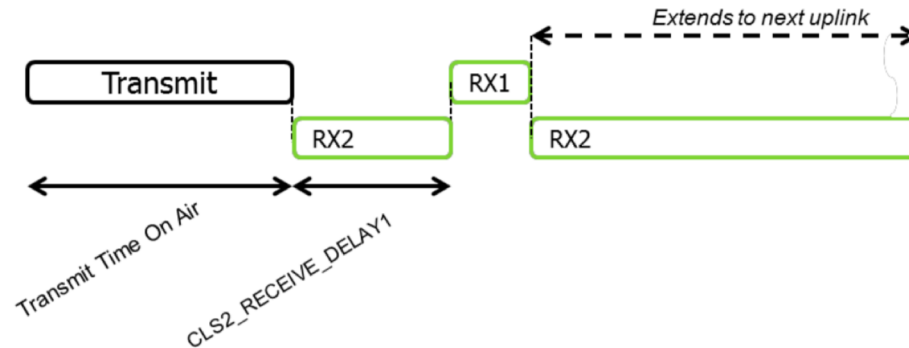
Figure 53: Beacon timing

Beacon_period	128 s
Beacon_reserved	2.120 s
Beacon_guard	3.000 s
Beacon-window	122.880 s

Table 18: Beacon timing

Class C: Continuously Listening End Device

- The end-devices implementing the Class C option are used for applications that have sufficient power available and thus do not need to minimize reception time.
- Class C end-devices SHALL NOT implement Class B option.
- The end-device SHALL listen on RX2 when it is not either (a) sending or (b) receiving on RX1, according to Class A definition.



LoRaWAN Network Reference Model

- The End-Device is a sensor or an actuator - wirelessly connected to a LoRaWAN network through Radio Gateways.
- The application layer of the End-Device is connected to a specific Application Server in the cloud. All application layer payloads of this End-Device are routed to its corresponding Application Server.

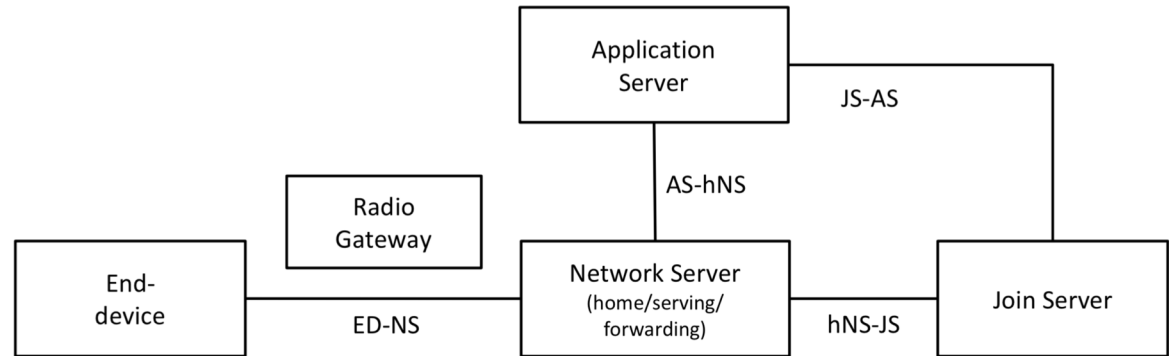
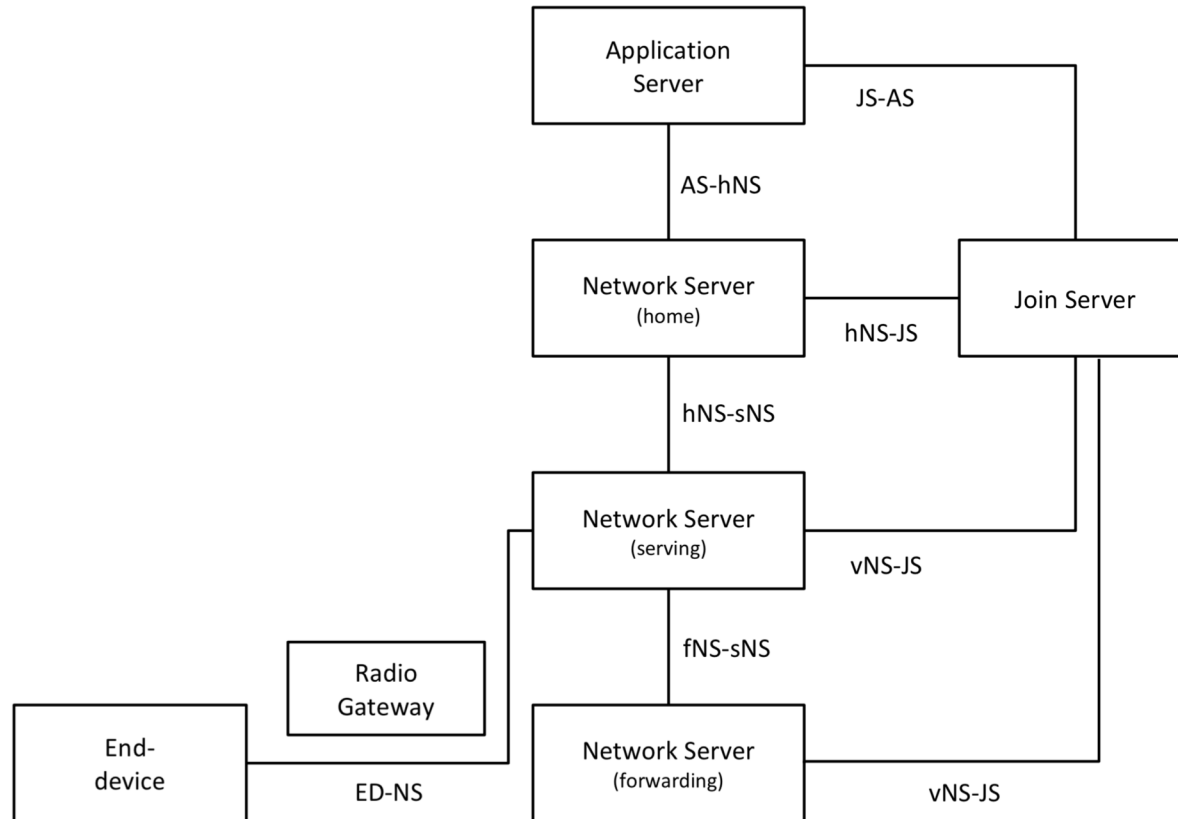


Figure 1 LoRaWAN Network Reference Model (NRM), End-Device at home

LoRaWAN Network Reference Model



Radio Gateway

- The Radio Gateway forwards all received LoRaWAN radio packets to the Network Server that is connected through an IP back-bone.
- The Radio Gateway operates entirely at the physical layer. Its role is simply to decode uplink radio packets from the air and forward them unprocessed to the Network Server.
- For downlinks, it executes transmission requests coming from the Network Server without any interpretation of the payload.

Network Server

- The Network Server (NS) terminates the LoRaWAN MAC layer for the End-Devices connected to the network. It is the center of the star topology.
- Generic features of NS are:
 - End-Device address check, Frame authentication and frame counter checks, Acknowledgements, Data rate adaptation, Responding to all MAC layer requests coming from the End-Device, Forwarding uplink application payloads to the appropriate Application Servers, Queuing of downlink payloads coming from any Application Server to any End- Device connected to the network, Forwarding Join-request and Join-accept messages between the End-Devices and the Join Servers.

Network Servers

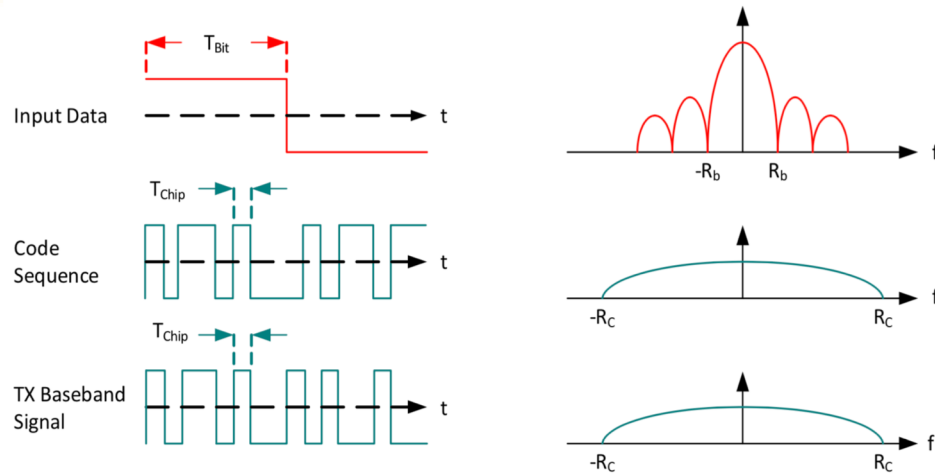
- Serving NS (sNS) controls the MAC layer of the End-Device
- Home NS (hNS) is where Device Profile, Service Profile, Routing Profile and DevEUI of the End-Device are stored.
- Forwarding NS (fNS) is the NS managing the Radio Gateways. When sNS and fNS are separated, they are in a roaming agreement.
- The Join Server (JS) manages the Over-the-Air (OTA) End-Device activation process. There may be several JSs connected to a NS, and a JS may connect to several NSs.
- The JS may be connected to several Application Servers (AS), and an AS maybe connected to several JSs.

LoRa PHY

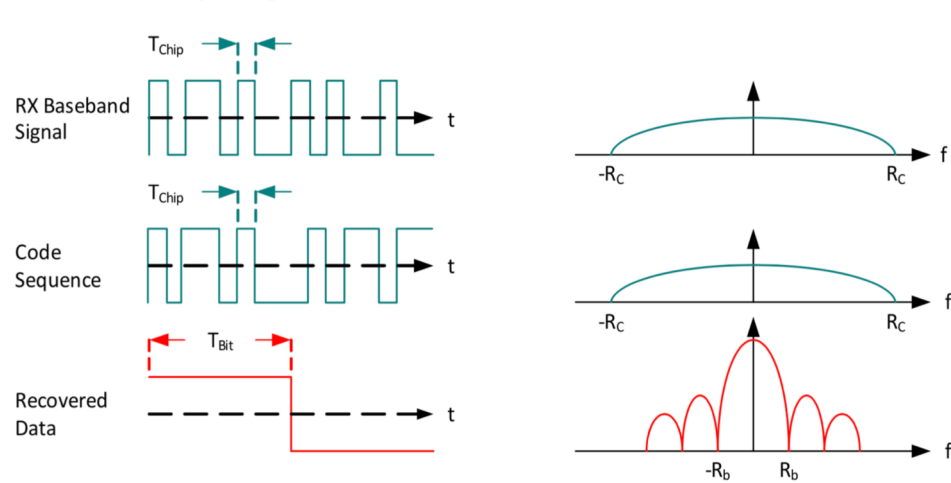
- LoRa is a proprietary spread spectrum modulation scheme that is derivative of Chirp Spread Spectrum modulation (CSS)
- It was developed by Cycleo of Grenoble, France, and acquired by Semtech in 2012
 - Constant bandwidth
 - Implements a variable data rate
 - utilizes orthogonal spreading factors
 - system designer can trade off between data rate for range or power
- LoRa is a PHY layer implementation and is agnostic with to higher-layer implementations.
 - LoRa can coexist and interoperate with existing network architectures.

Spread Spectrum Principles

Modulation / Spreading

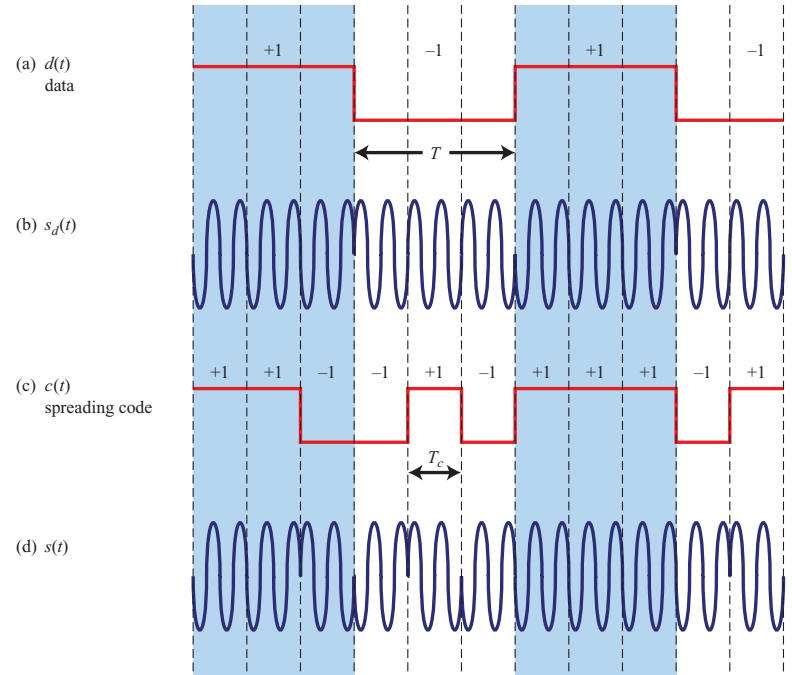
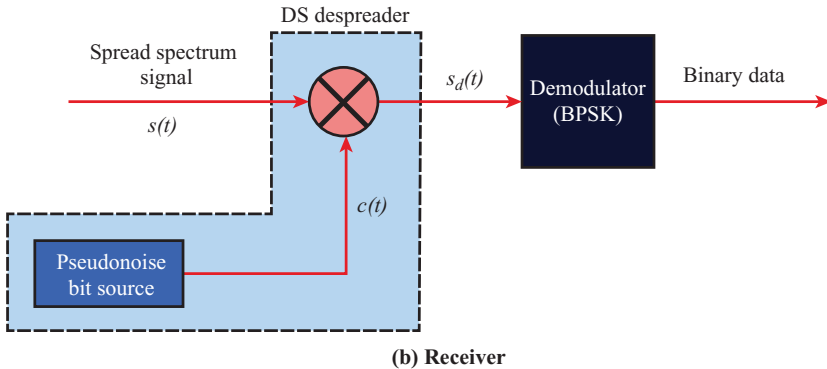
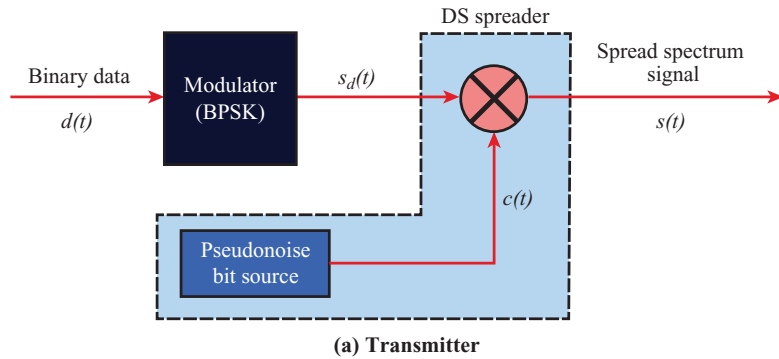


Demodulation / De-spreading



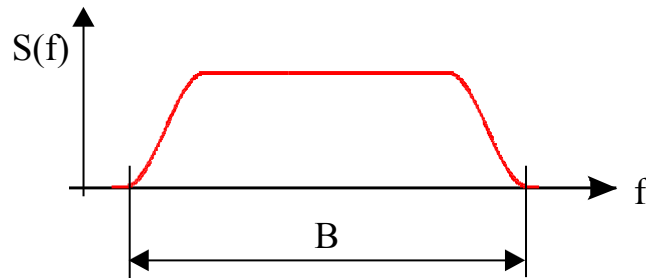
- Each bit in original signal is represented by multiple bits in the transmitted signal
- Spreading code spreads signal across a wider frequency band
 - Spread is in direct proportion to number of bits used
- One technique combines digital information stream with the spreading code bit stream using exclusive-OR

DSSS with BPSK

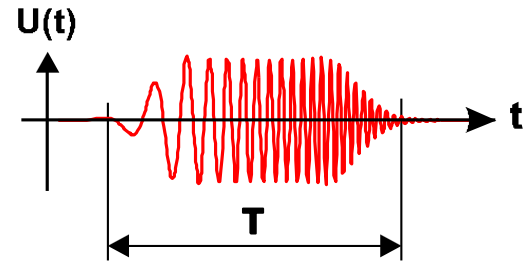


Characteristics of Chirp pulses

- A chirp pulse is a frequency modulated pulse.
 - Its duration is T ; within this time the frequency is changing in a monotonic manner from a lower value to a higher one (“Up-Chirp”) or reverse (“Down-Chirp”).
 - The difference between these two frequencies is a good approximation for the bandwidth B of the chirp pulse.

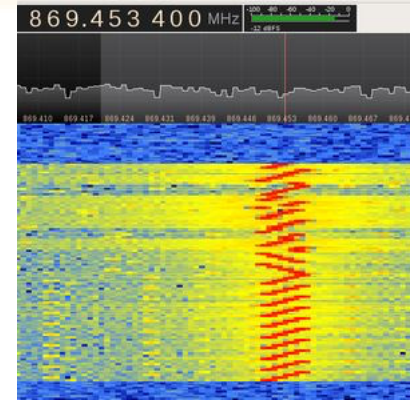
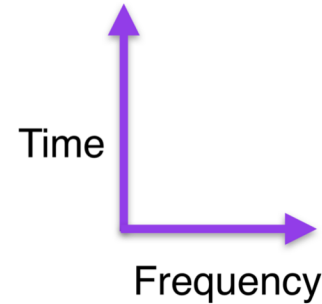
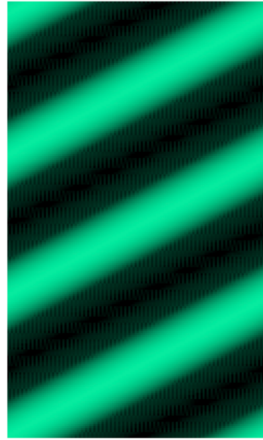
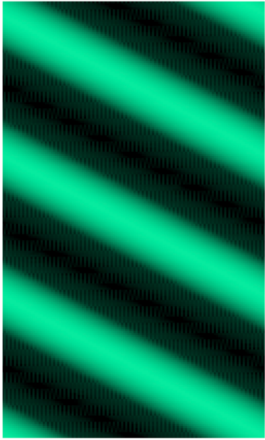


Spectrum of the chirp pulse with bandwidth B and a roll-off factor of 0.25



Up-Chirp in the time domain (roll-off factor 0.25)

CSS Chirps



LoRa Frequency:
<https://revspace.nl/DecodingLora>

- Upchirp
 - Increasing frequency
- Downchirp
 - Decreasing frequency

Steps for Modulation

- Gray Indexing - Adds error tolerance
- Data Whitening - Induces randomness
- Interleaving - Scrambles bits within frame
- Forward Error Correction - Adds parity bits

1) Low power long range transmitter

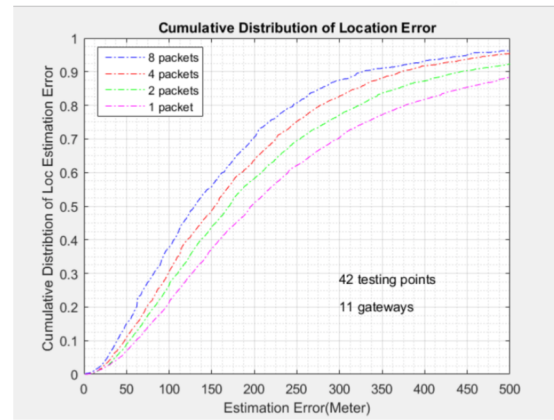
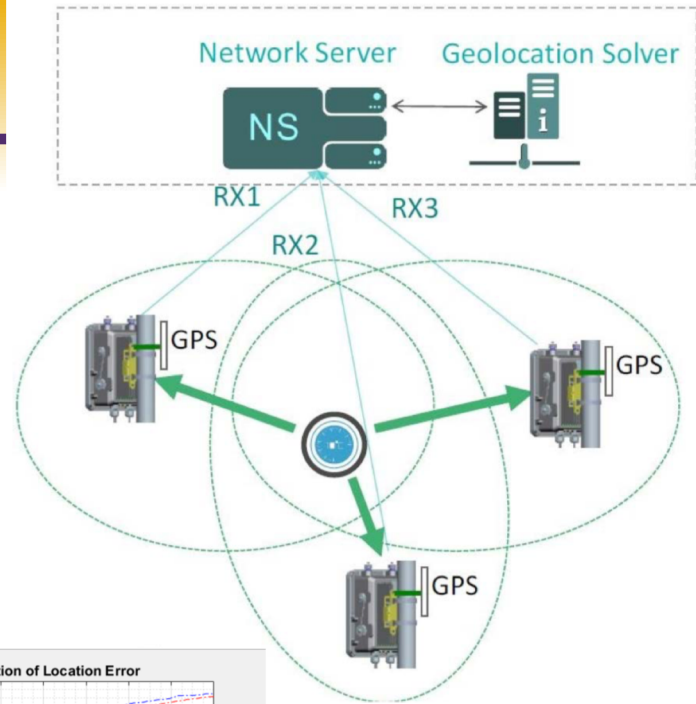
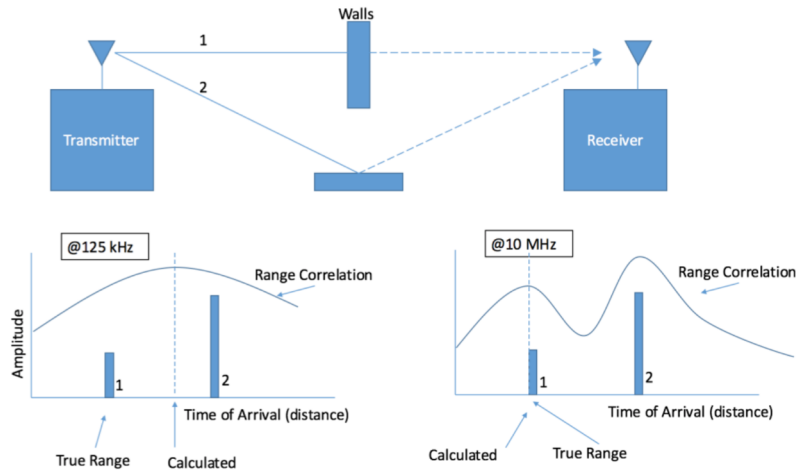
European Patent EP2763321A1

<https://patents.google.com/patent/EP2763321A1/en>

2) Matt Knight, “Decoding LoRa, a Wireless Network for the Internet of Things”, RSA Conference 2017

LoRa Localization

- Direct Path Energy
- TDoA & Phase
- Multiple Gateways



LoRa Localization

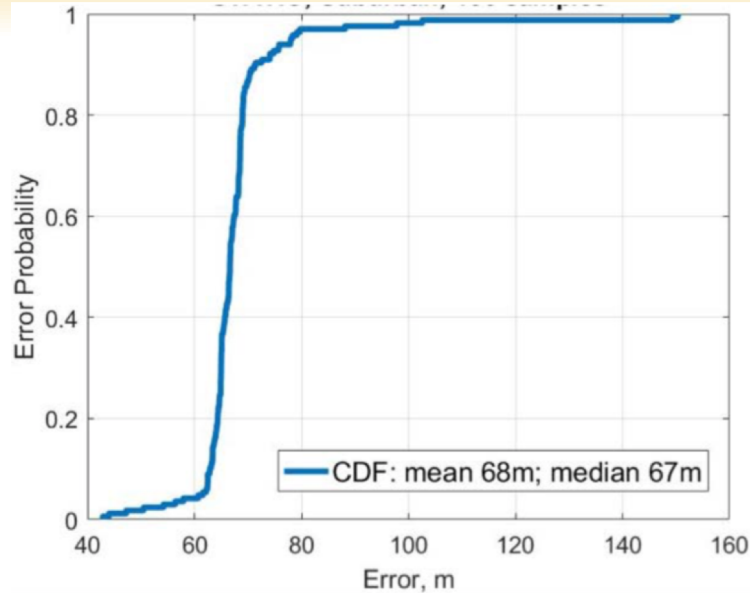


Figure 5-2: ZAL Port TDOA Position Accuracy, Stationary (Parked) Vehicles

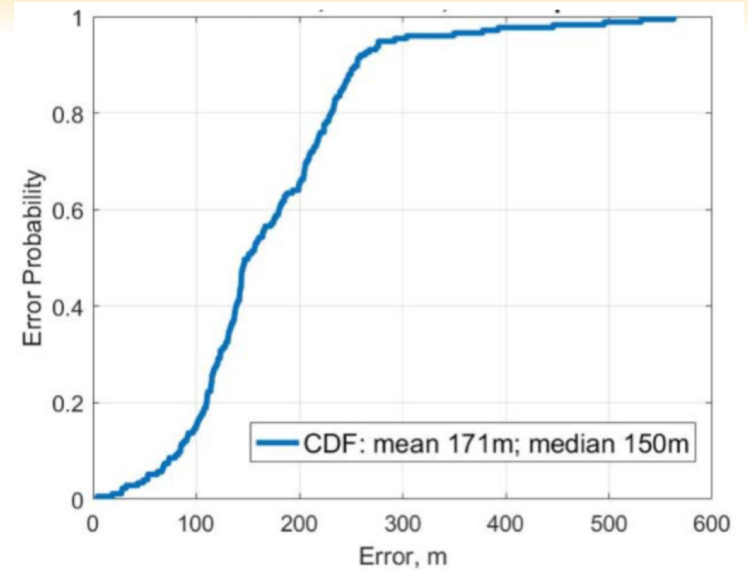


Figure 5-3: ZAL Port TDOA Position Accuracy, Moving Vehicles

SigFox



UNIVERSITY
AT ALBANY

State University of New York

SigFox

- Ultra narrow band
- Random Access
- Cooperative Reception
- Small Messages (*12-byte payload Uplink, 8 byte payload downlink*)
- Bi-directional
- Cloud-based Core Network

SigFox in comparison to other technologies

ENERGY & COST
EFFICIENCY

PERSONAL & PRIVATE
NETWORKS

PUBLIC
CONNECTIVITY

LPWAN requirements

sigfox

LoRa SEMTECH uGenu

2G
3G
4G
5G
LTE-M
NB-IoT

WAN

SCALE

Bluetooth[®]
SMART

ZigBee

ZWAVE

M-Bus
wireless

Wi-Fi
802.11ah

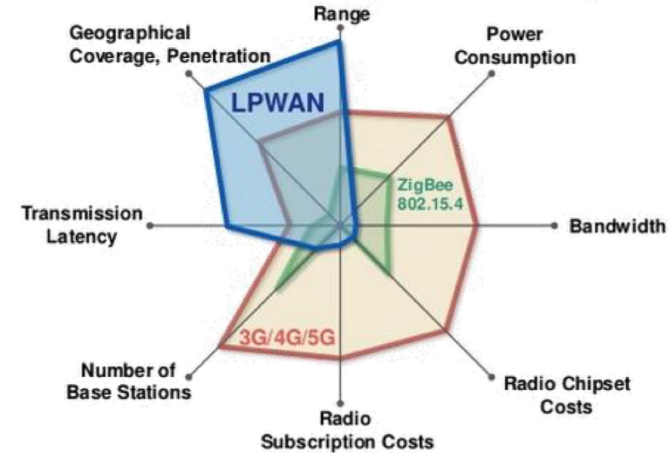
LoRa SEMTECH

LAN

PAN

LPWAN definition

- High density of objects
- Reduced H/W cost
- Reduced connectivity cost
- Low data rates
- Constrained latency



Ultra narrowband operation in EU



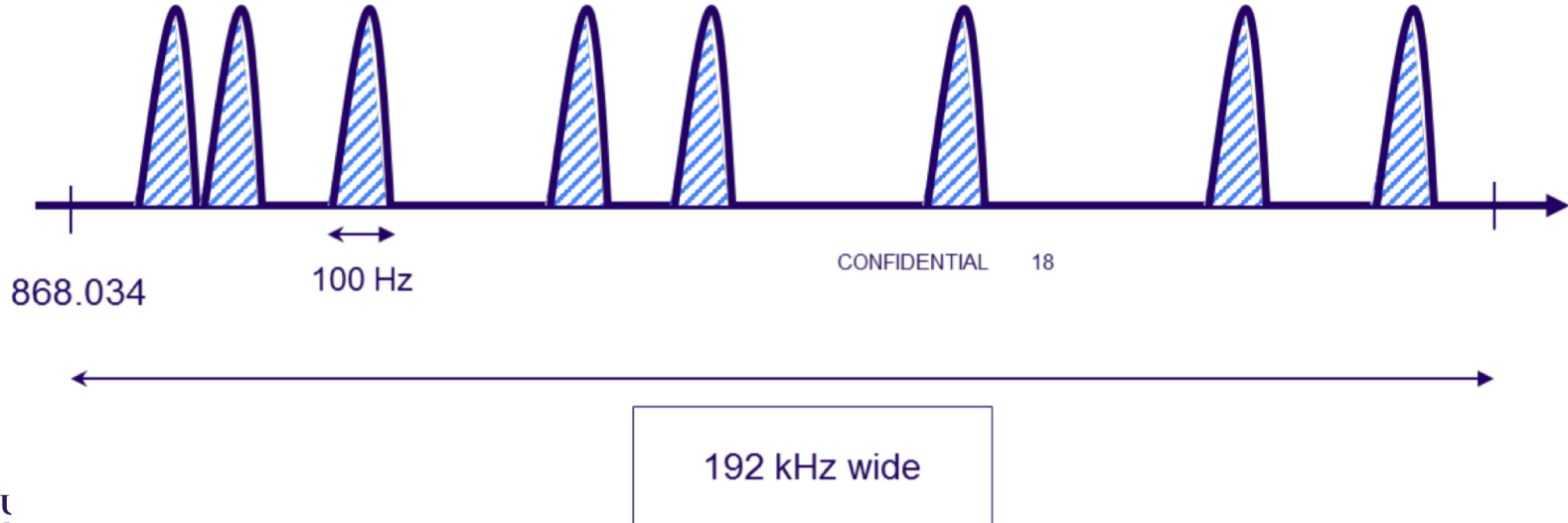
100Hz wide in a 200 kHz band



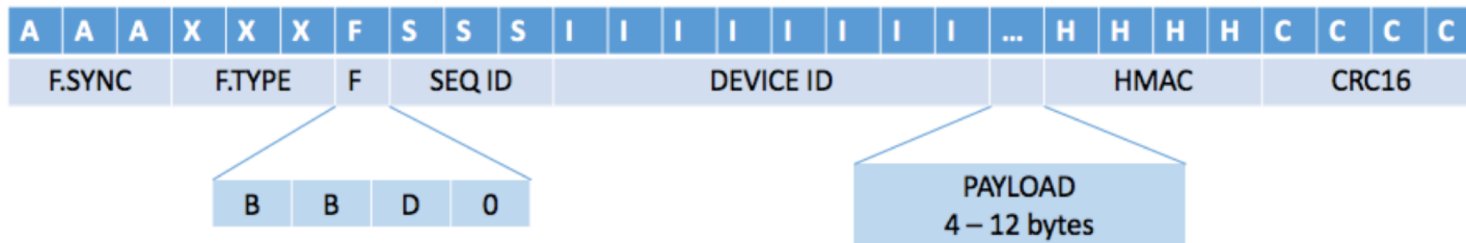
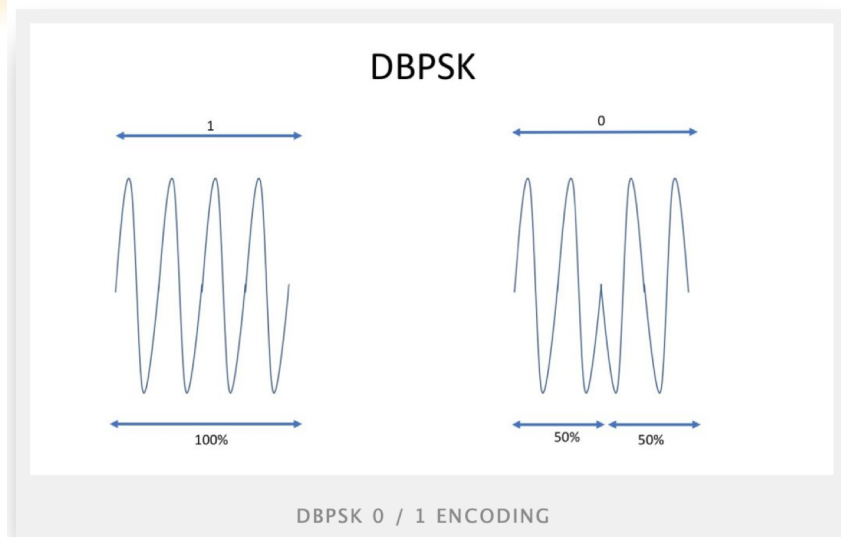
DBPSK



High spectrum efficiency 1bit/s = 1Hz of bandwidth



Modulation and Encoding



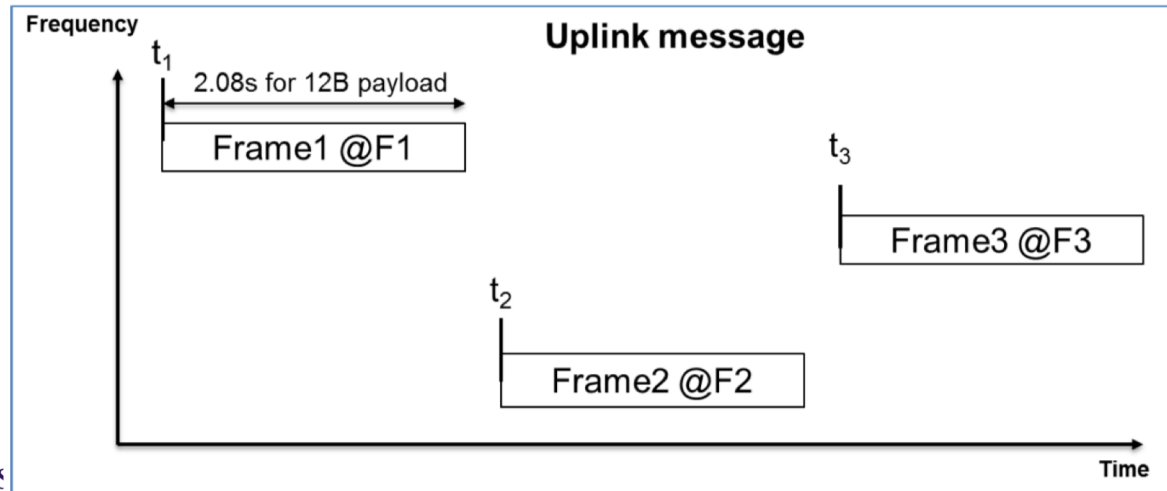
Each of the Cells represent a Quartet (4 bits)

Long Range

	Modulation	Data-rate (bps)	Tx Power	Compound TX Antenna Gain	Compound RX Antenna Gain	RX sensitivity	Link Budget
Uplink (ETSI)	DBPSK	100	+14 dBm	0dB	+6dB	-142dBm	+162dB
Downlink (ETSI)	GFSK	600	+27 dBm	+6dB	0dB	-130dBm	+163dB
Uplink (FCC)	DBPSK	600	+22 dBm	0dB	0dB	-134 dBm	+156dB
Downlink (FCC)	GFSK	600	+30 dBm	0dB	0dB	-129 dBm	+159dB

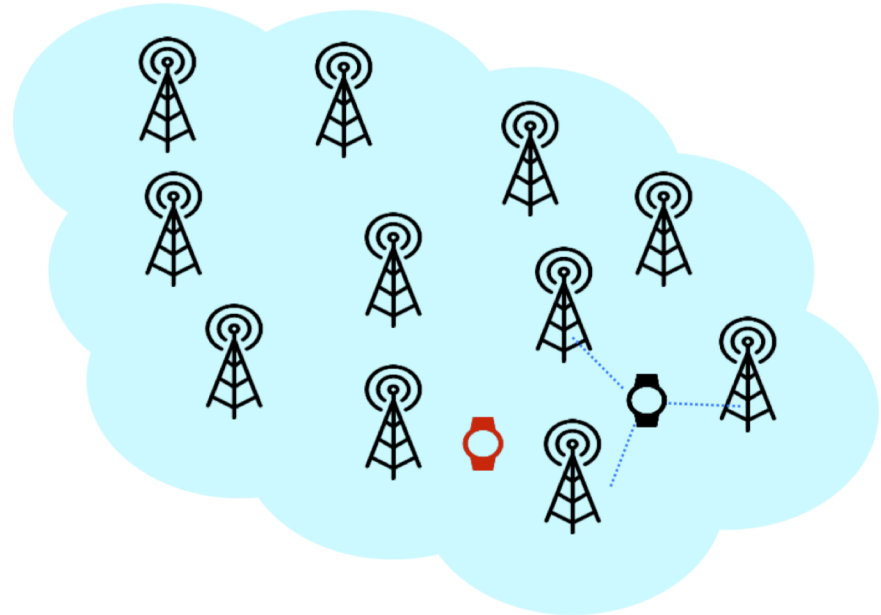
Random Access

- Unsynchronized transmission
- Random frequency
- SIGFOX Base stations permanently listen to the spectrum
- 3 replicas of the same frame @ 3 frequencies



Cooperative Reception

- Message received by 3 Base Stations in average
- Spatial diversity decreases collision probability
- MIMO like Approach



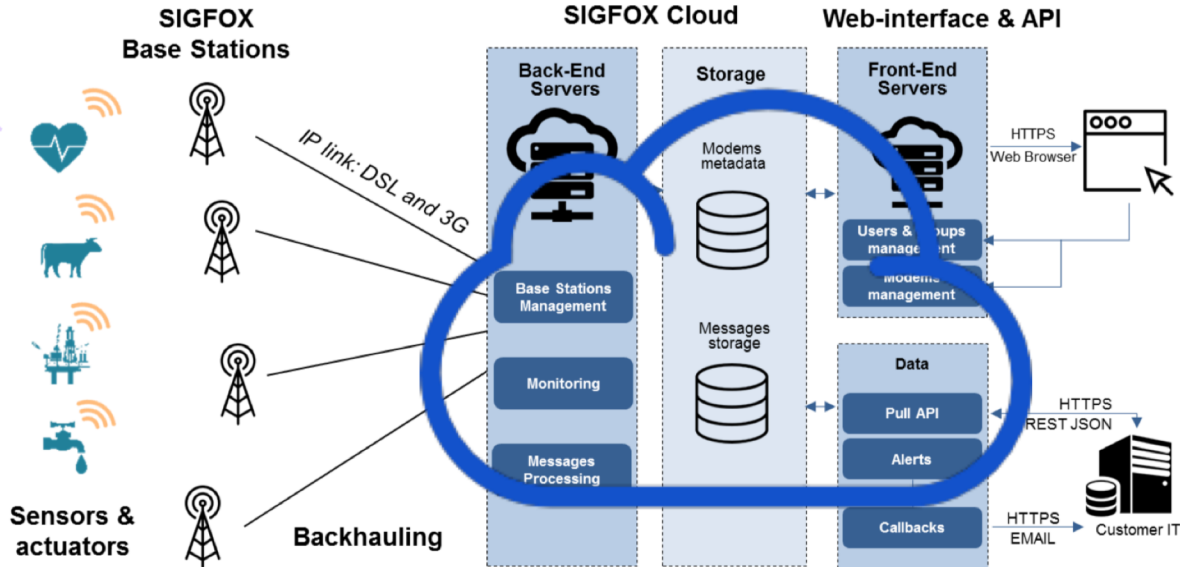
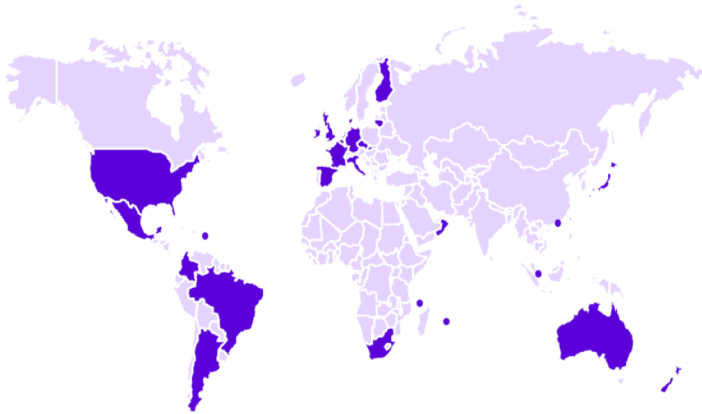
Cloud Based Core Network



Centralized Authentication & Message Forwarding



Flat RAN Architecture



Cellular IoT



UNIVERSITY
AT ALBANY
State University of New York

3GPP's Effort

- NB-IoT designed to exist in one of three ways:
 - In independently licensed bands.
 - In unused 200 kHz bands that have previously been used for GSM or CDMA.
 - On LTE base stations that can allocate a resource block to NB-IoT operations or in their guard bands (where regulations allow it)
- LTE-M
 - The advantage of LTE-M over NB-IoT is its higher data rate, mobility, and voice over the network
 - It requires more bandwidth, is more expensive, and cannot be put into guard band frequency band for now

Bluetooth



UNIVERSITY
AT ALBANY
State University of New York

IEEE 802.15

- **Wireless Personal Area Networks**
 - Short-range communication
 - Low-cost, low-energy to provide long battery life
- **Several standards have been provided**
- **We focus on 802.15 technologies**
 - Other viable WPAN alternatives exist

Bluetooth

- Universal short-range wireless capability
- Uses 2.4-GHz band
- Available globally for unlicensed users
- Devices within 10 m can share up to 2.1 Mbps or 24 Mbps of capacity
- Supports open-ended list of applications
 - Data, audio, graphics, video
- Started as IEEE 802.15.1
 - New standards come from the Bluetooth Special Interest Group (Bluetooth SIG)
 - Industry consortium
 - Bluetooth 2.0, 2.1, 3.0, and 4.0

Bluetooth Application Areas

- Data and voice access points
 - Real-time voice and data transmissions
- Cable replacement
 - Eliminates need for numerous cable attachments for connection
- Ad hoc networking
 - Device with Bluetooth radio can establish connection with another when in range

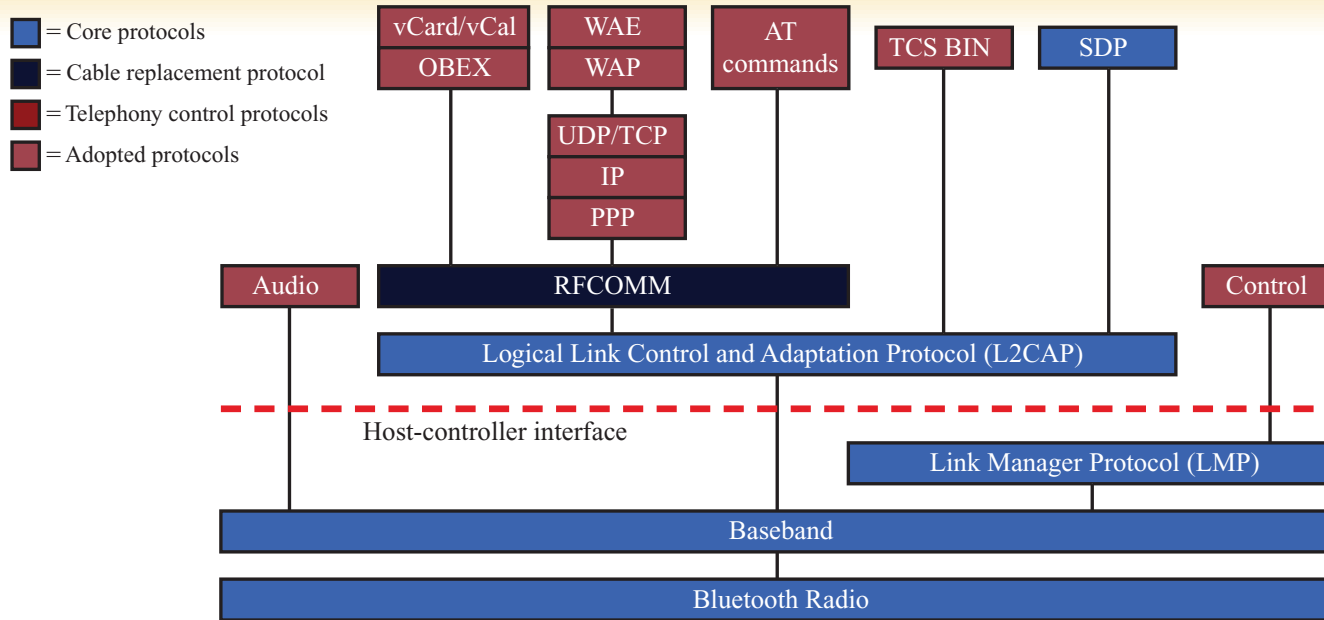
Top uses of Bluetooth

- Mobile handsets
- Voice handsets
- Stereo headsets and speakers
- PCs and tablets
- Human interface devices, such as mice and keyboards
- Wireless controllers for video game consoles
- Cars
- Machine-to-machine applications: credit-card readers, industrial automation, etc.

Bluetooth Standards Documents

- Core specifications
 - Details of various layers of Bluetooth protocol architecture
- Profile specifications
 - Use of Bluetooth technology to support various applications
- Initial Standard
 - 2.1 Basic/Enhanced Data Rate (BR/EDR)
- Later standards
 - 3.0 Alternative MAC/PHY (AMP)
 - 4.0 Bluetooth Smart (Bluetooth Low Energy)

Bluetooth Protocol Stack



- | | | | |
|--------|-------------------------------------|---------|--|
| AT | = Attention sequence (modem prefix) | TCS BIN | = Telephony control specification - binary |
| IP | = Internet Protocol | UDP | = User Datagram Protocol |
| OBEX | = Object exchange protocol | vCal | = Virtual calendar |
| PPP | = Point-to-Point Protocol | vCard | = Virtual card |
| RFCOMM | = Radio frequency communications | WAE | = Wireless application environment |
| SDP | = Service discovery protocol | WAP | = Wireless application protocol |
| TCP | = Transmission control protocol | | |

Protocol Architecture

- Bluetooth is a layered protocol architecture
 - Core protocols
 - Cable replacement and telephony control protocols
 - Adopted protocols
- Core protocols
 - Radio
 - Baseband
 - Link manager protocol (LMP)
 - Logical link control and adaptation protocol (L2CAP)
 - Service discovery protocol (SDP)

Protocol Architecture

- Cable replacement protocol
 - RFCOMM
- Telephony control protocol
 - Telephony control specification – binary (TCS BIN)
- Adopted protocols
 - PPP
 - TCP/UDP/IP
 - OBEX
 - WAE/WAP

Profiles

- Over 40 different profiles are defined in Bluetooth documents
 - Only subsets of Bluetooth protocols are required
 - Reduces costs of specialized devices
- All Bluetooth nodes support the Generic Access Profile
- Profiles may depend on other profiles
 - Example: File Transfer Profile
 - Transfer of directories, files, documents, images, and streaming media formats
 - Depends on the Generic Object File Exchange, Serial Port, and Generic Access Profiles.
 - Interfaces with L2CAP and RFCOMM protocols

Piconets and Scatternets

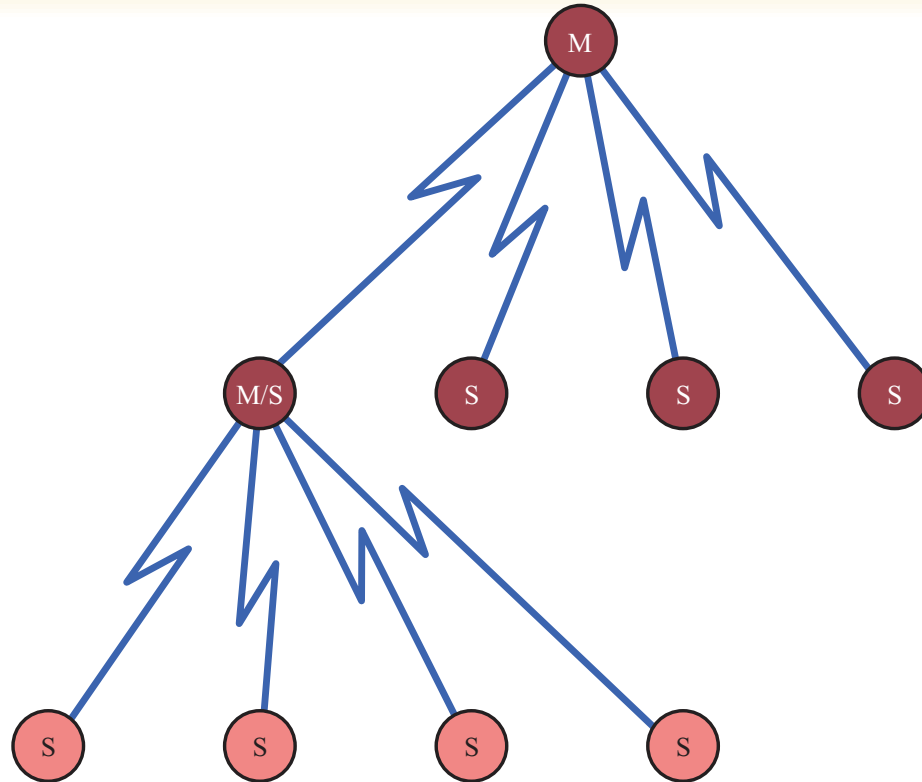
➤ Piconet

- Basic unit of Bluetooth networking
- Master and one to seven slave devices
- Master determines channel and phase

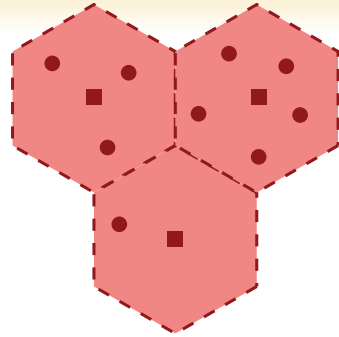
➤ Scatternet

- Device in one piconet may exist as master or slave in another piconet
- Allows many devices to share same area
- Makes efficient use of bandwidth

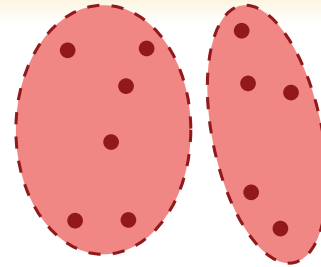
Master/Slave Relationships



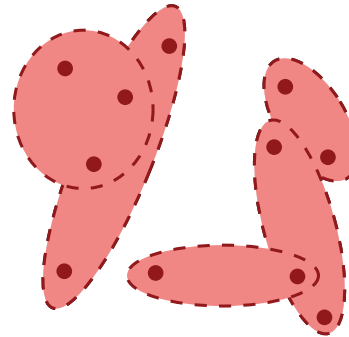
Wireless Network Configurations



(a) Cellular system (squares represent stationary base stations)

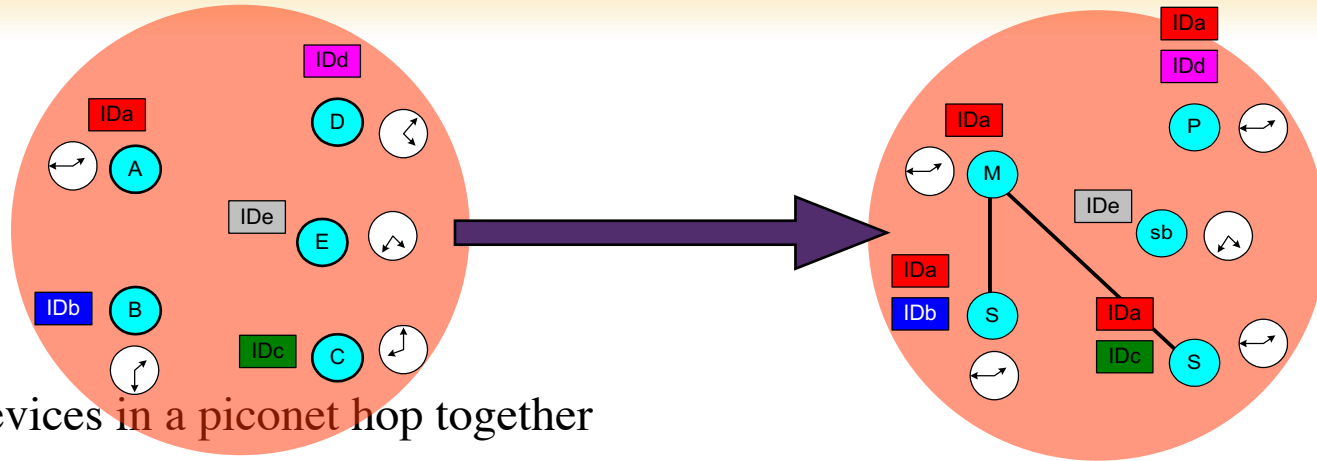


(b) Conventional ad hoc systems



(c) Scatternets

Piconet



- All devices in a piconet hop together
 - To form a piconet: master gives slaves its *clock* and *device ID*
 - Hopping pattern determined by *device ID* (48-bit)
 - Phase in hopping pattern determined by *Clock*
- Non-piconet devices are in standby
- Piconet Addressing
 - Active Member Address (AMA, 3-bits)
 - Parked Member Address (PMA, 8-bits)

Radio Specification

- **Classes of transmitters**
 - **Class 1: Outputs 100 mW for maximum range**
 - Power control mandatory
 - Provides greatest distance
 - **Class 2: Outputs 2.4 mW at maximum**
 - Power control optional
 - **Class 3: Nominal output is 1 mW**
 - Lowest power

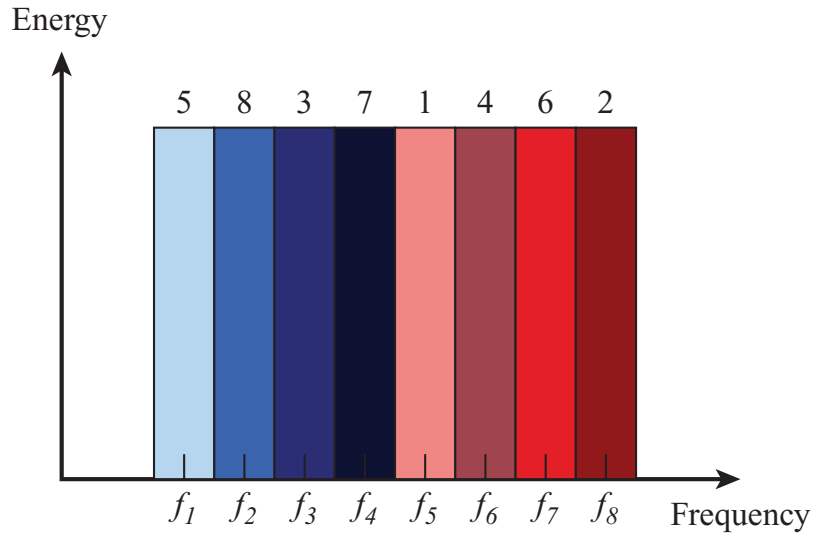
Frequency Hopping in Bluetooth

- Provides resistance to interference and multipath effects
- Provides a form of multiple access among co-located devices in different piconets

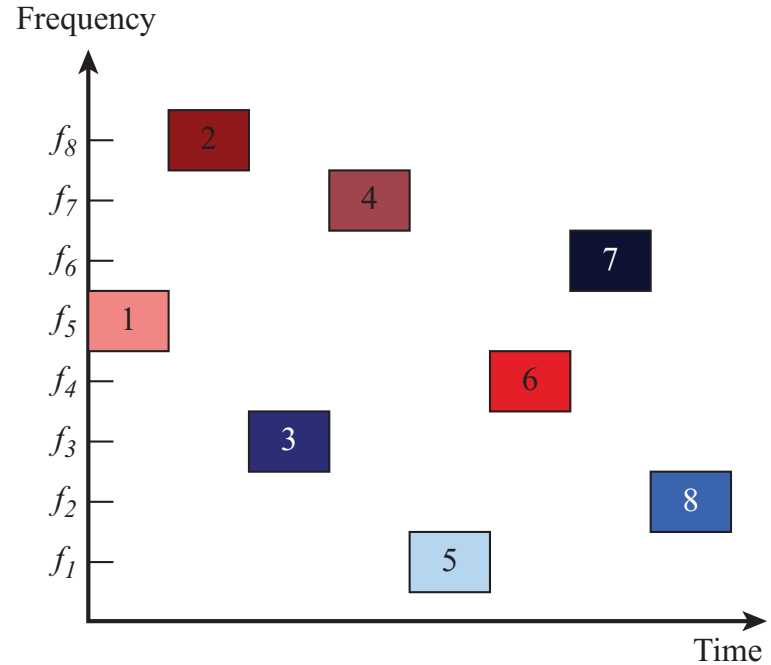
Frequency Hopping

- Total bandwidth divided into 1MHz physical channels
- FH occurs by jumping from one channel to another in pseudorandom sequence
- Hopping sequence shared with all devices on piconet
- Piconet access:
 - Bluetooth devices use time division duplex (TDD)
 - Access technique is TDMA
 - FH-TDD-TDMA

Frequency Hopping Example



(a) Channel assignment

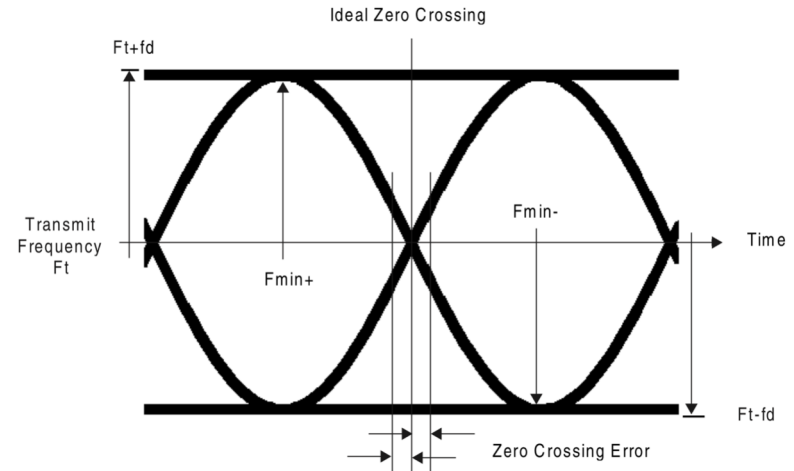
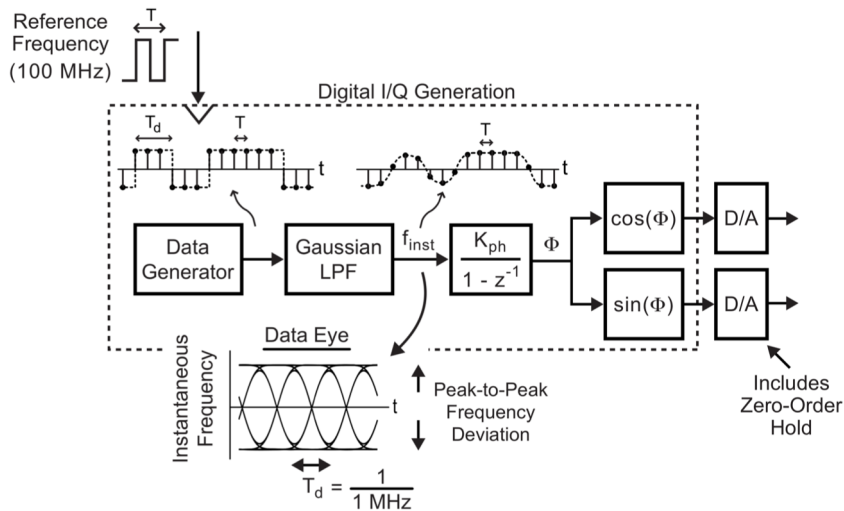


(b) Channel use

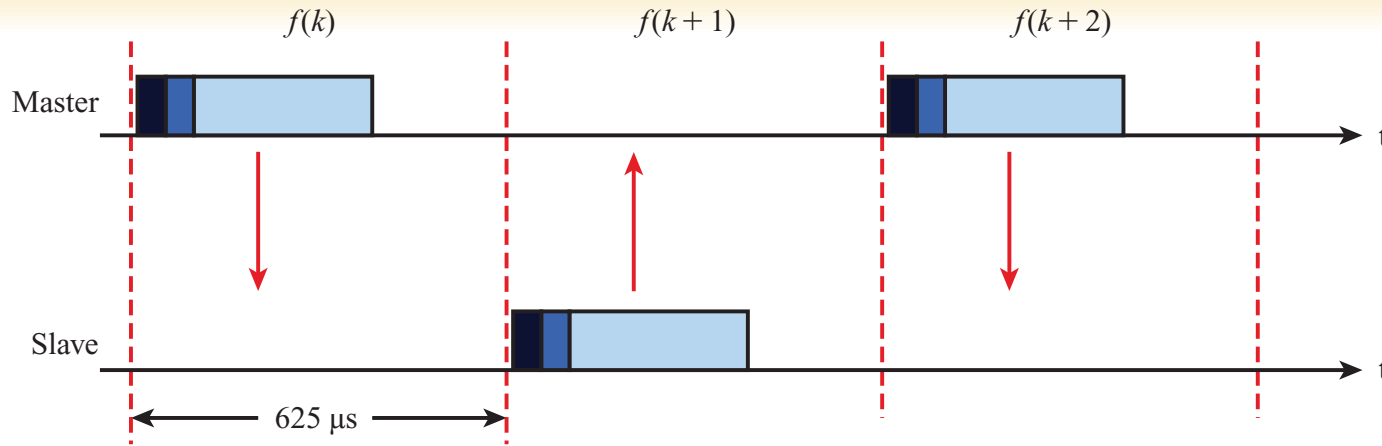
Modulation

➤ Gaussian frequency shift keying (GFSK)

- A type of FSK modulation which uses a Gaussian filter to shape the pulses before they are modulated.
- This reduces the spectral bandwidth and out-of-band spectrum, to meet adjacent-channel power rejection requirements.



Frequency-Hop Time-Division Duplex

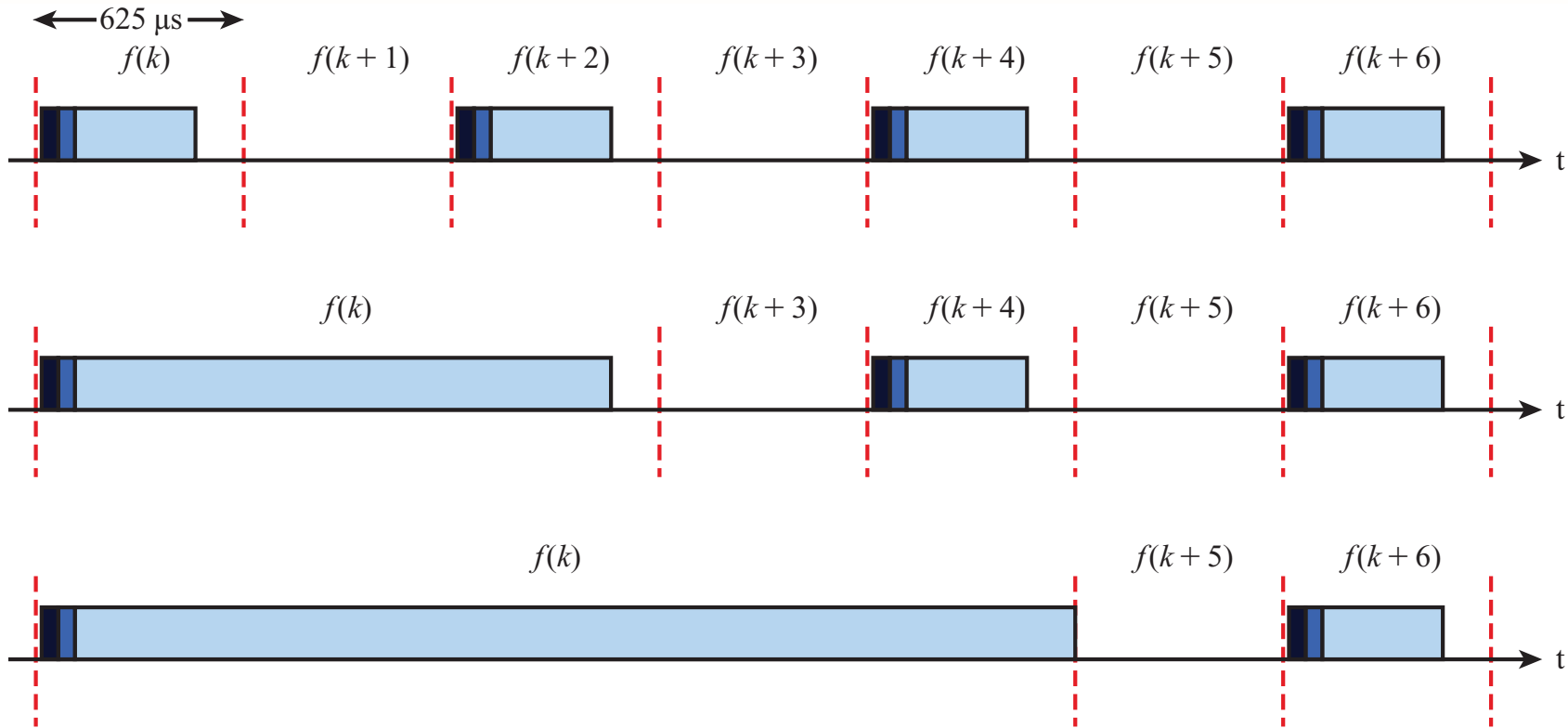


- The channel is divided into time slots, each $625 \mu\text{s}$ in length.
- The time slots are numbered according to the Bluetooth clock of the piconet master.
- Hop Rate = 1600 hops per sec
- FH occurs on a pseudorandom sequence
- Hopping sequence is shared among all devices in a piconet
- Different piconets will have different masters and will have different sequence

TDD

- A TDD scheme is used where master and slave alternatively transmit.
- The master shall start its transmission in even-numbered time slots only, and the slave shall start its transmission in odd-numbered time slots only.
- The packet start shall be aligned with the slot start.
- Packets transmitted by the master or the slave may extend over up to five time slots.

Examples of Multislot Packets



Physical Links between Master and Slave

- Synchronous connection oriented (SCO)
 - Allocates fixed bandwidth between *point-to-point connection* of master and slave
 - Master maintains link using reserved slots
 - Master can support three simultaneous links
- Asynchronous connectionless (ACL)
 - *Point-to-multipoint* link between master and all slaves
 - Only single ACL link can exist
- Extended Synchronous connection oriented (eSCO)
 - Reserves slots just like SCO
 - But these can be asymmetric
 - Retransmissions are supported

Bluetooth Baseband Formats



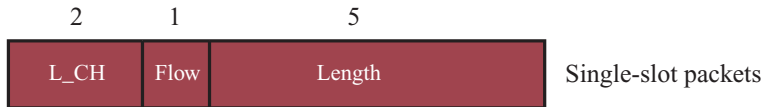
(a) Packet format



(b) Access code format

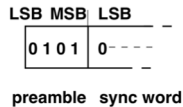
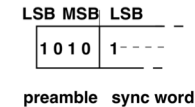


(c) Header format (prior to coding)



(d) Data payload header format

The preamble is a fixed zero-one pattern of four symbols used to facilitate dc compensation. The sequence is either 1010 or 0101, depending whether the LSB of the following sync word is 1 or 0, respectively.



Bluetooth Packet Fields

- Access code – used for timing synchronization, offset compensation, paging, and inquiry
- Header – used to identify packet type and carry protocol control information
- Payload – contains user voice or data and payload header, if present

Types of Access Codes

- Channel access code (CAC) – identifies a piconet
- Device access code (DAC) – used for paging and subsequent responses
- Inquiry access code (IAC) – used for inquiry purposes

Packet Header Fields

- AM_ADDR – contains “active mode” address of one of the slaves
- Type – identifies type of packet
- Flow – 1-bit flow control
- ARQN – 1-bit acknowledgment
- SEQN – 1-bit sequential numbering schemes
- Header error control (HEC) – 8-bit error detection code

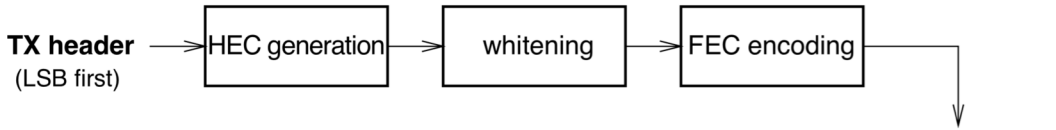
Payload Format

- Payload header
 - L_CH field – identifies logical channel
 - Flow field – used to control flow at L2CAP level
 - Length field – number of bytes of data
- Payload body – contains user data
- CRC – 16-bit CRC code

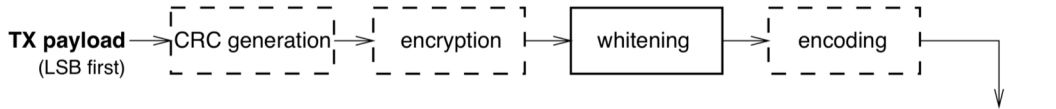
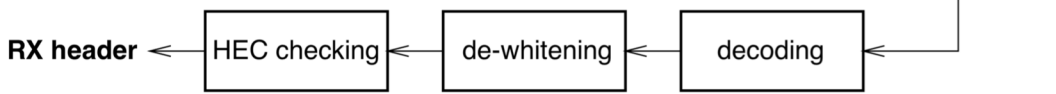
Error Correction Schemes

- 1/3 rate FEC (forward error correction)
 - Used on 18-bit packet header, voice field in HV1 packet
- 2/3 rate FEC
 - Used in DM packets, data fields of DV packet, FHS packet and HV2 packet
- ARQ
 - Used with DM and DH packets

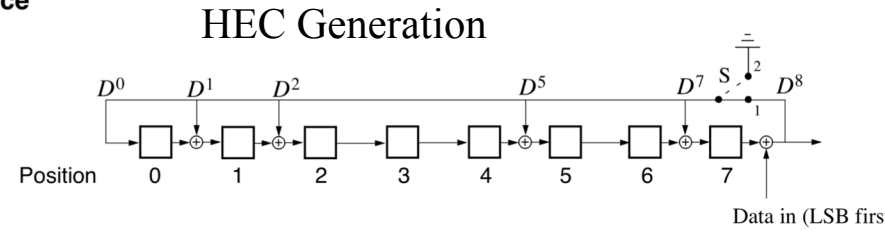
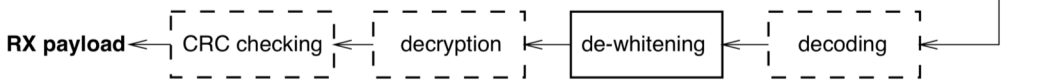
Bit Processing



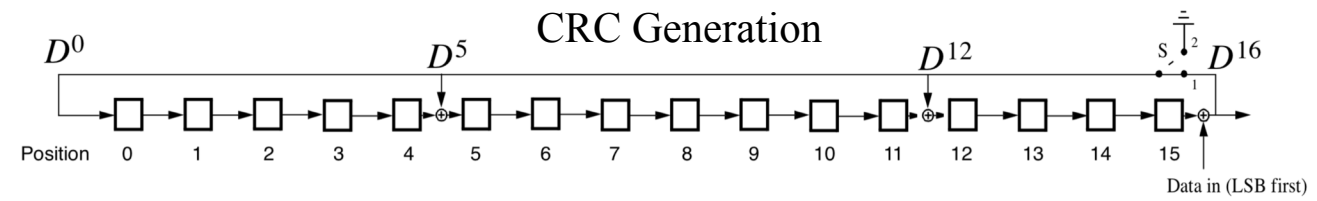
Header



Payload



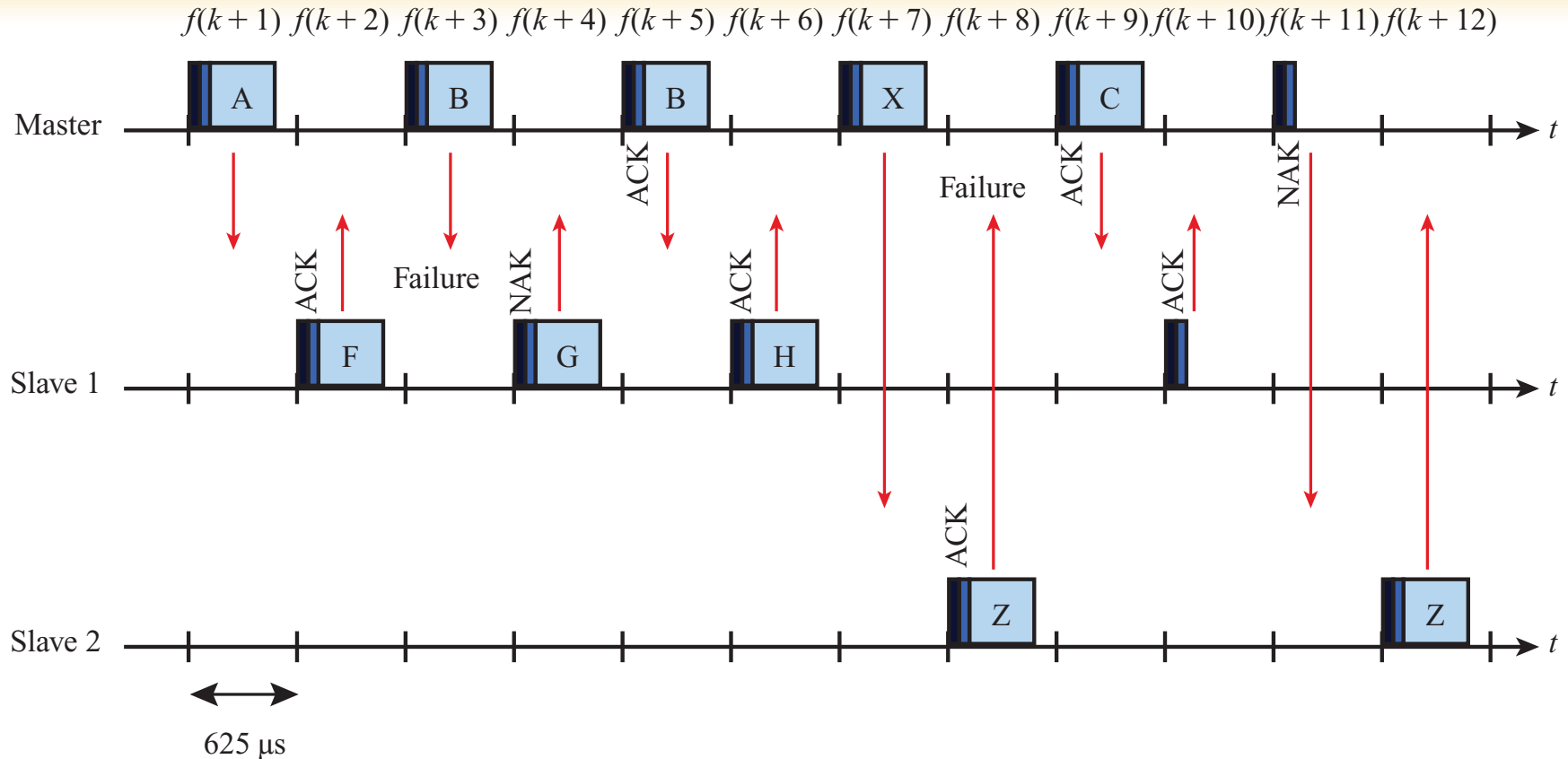
Data Whitening Polynomial
 $g(D) = D^7 + D^4 + 1$



ARQ Scheme Elements

- Error detection – destination detects errors, discards packets
- Positive acknowledgment – destination returns positive acknowledgment
- Retransmission after timeout – source retransmits if packet unacknowledged
- Negative acknowledgment and retransmission – destination returns negative acknowledgement for packets with errors, source retransmits

An Example of Retransmission Operation



Logical Channels

- Link control (LC)
- Link manager (LM)
- User asynchronous (UA)
- User isochronous (UI)
- Use synchronous (US)

Link manager

- Manages various aspects of the radio link between a master and a slave
- Involves the exchange LMP PDUs (protocol data units)
- Procedures defined for LMP are grouped into 24 functional areas, which include
 - Authentication
 - Pairing
 - Encryption
 - Clock offset request
 - Switch master/slave
 - Name request
 - Hold or park or sniff mode

Logical link control & adaptation protocol-L2CAP

- Provides a link-layer protocol between entities with a number of services
- Relies on lower layer for flow and error control
- Makes use of ACL links, does not support SCO links
- Provides two alternative services to upper-layer protocols
 - Connection service
 - Connection-mode service

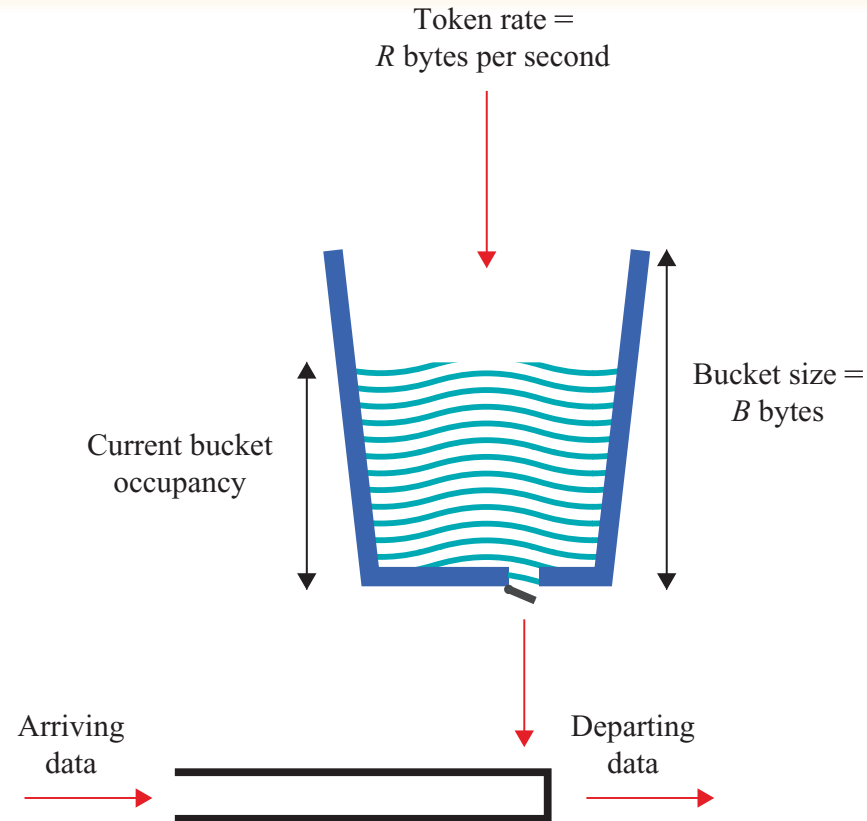
L2CAP Logical Channels

- **Connectionless**
 - Supports connectionless service
 - Each channel is unidirectional
 - Used from master to multiple slaves
- **Connection-oriented**
 - Supports connection-oriented service
 - Each channel is bidirectional
- **Signaling**
 - Provides for exchange of signaling messages between L2CAP entities

Flow Specification Parameters

- Service type
- Token rate (bytes/second)
- Token bucket size (bytes)
- Peak bandwidth (bytes/second)
- Latency (microseconds)
- Delay variation (microseconds)

Token Bucket Scheme



Bluetooth high speed

- Bluetooth 3.0+HS
- Up to 24 Mbps
- New controller compliant with 2007 version of IEEE 802.11
- Known as Alternative MAC/PHY (AMP)
 - Optional capability
- Bluetooth radio still used for device discovery, association, setup, etc.
- Allows more power efficient Bluetooth modes to be used, except when higher data rates are needed

Bluetooth smart

- Bluetooth 4.0
- Also known as Bluetooth Low Energy (BLE)
- An intelligent, power-friendly version of Bluetooth
- Can run long periods of time on a single battery
 - Or scavenge for energy
- Also communicates with other Bluetooth-enabled devices
 - Legacy Bluetooth devices or Bluetooth-enabled smartphones
 - Great feature
- Possible successful technology for the Internet of Things
 - For example, health monitoring devices can easily integrate with existing smartphones

Bluetooth smart

- Same 2.4 GHz ISM bands as Bluetooth BR/EDR
 - But uses 40 channels spaced 2 MHz apart instead of 79 channels spaced 1 MHz apart
- Devices can implement a transmitter, a receiver, or both
- Implementation
 - Single-mode Bluetooth Smart functionality
 - Reduced cost chips that can be integrated into compact devices.
 - Dual-mode functionality to also have the Bluetooth BR/EDR capability
- 10 mW output power
- 150 m range in an open field

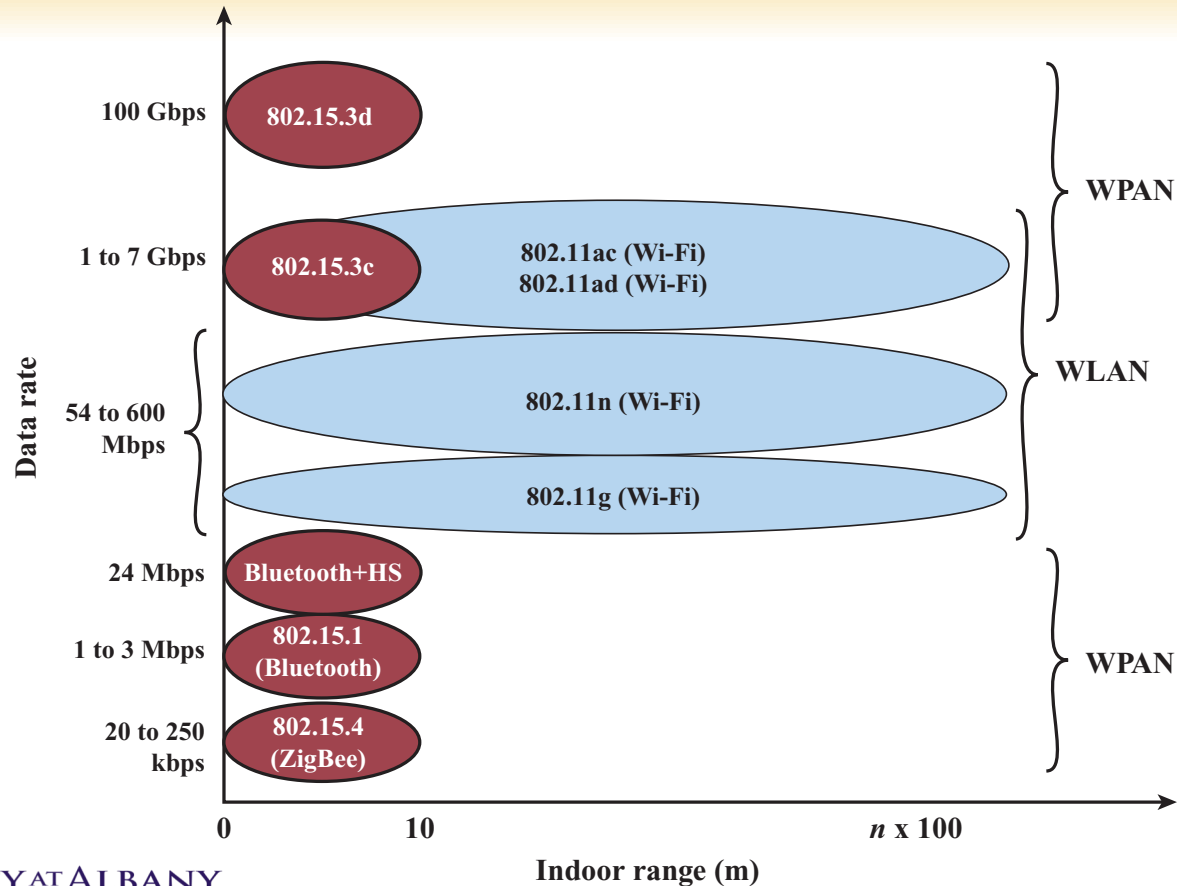
IEEE 802.15

- After 802.15.1, work went two directions
- 802.15.3
 - Higher data rates than 802.15.1
 - But still low cost, low power compared to 802.11
- 802.15.4
 - Very low cost, very low power compared to 802.15.1
- Figure 12.9 shows different options
- Figure 12.10 shows relative distances and rates

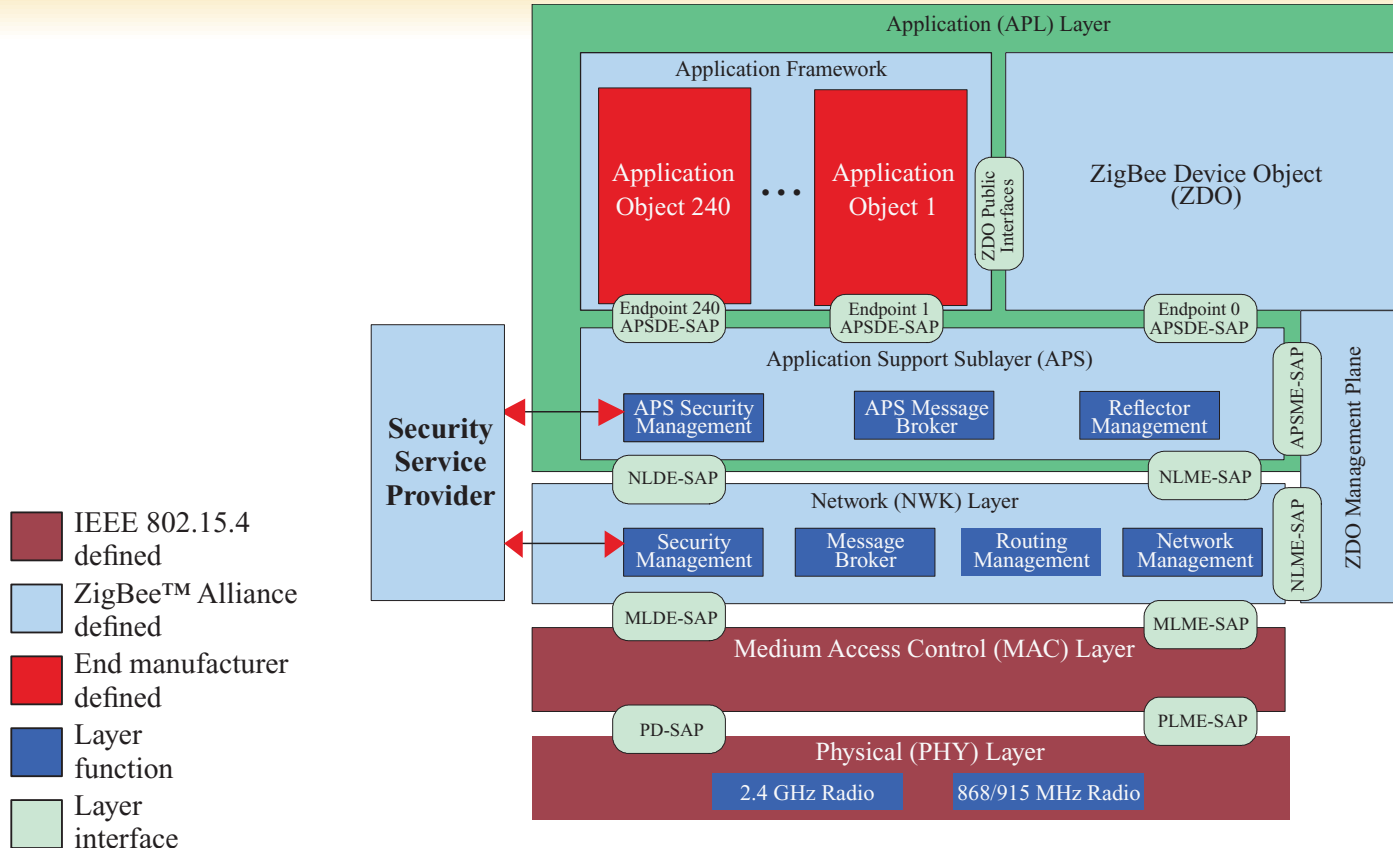
IEEE 802.15 Protocol Architecture

Logical link control (LLC)			
802.15.1 Bluetooth MAC	802.15.3 MAC		802.15.4, 802.15.4e MAC
802.15.1 2.4 GHz 1, 2, or 3 Mbps 24 Mbps HS	802.15.3c 60 GHz 1 to 6 Gbps	802.15.3d 60 GHz 100 Gbps	802.15.4, 802.15.4a 868/915 MHz, 2.4 GHz DSSS: 20, 40, 100, 250 kbps UWB: 110 kbps to 27 Mbps CSS: 250 kbps, 1 Mbps

Wireless Local Networks



ZigBee Architecture



IEEE 802.15.3

- High data rate WPANs
 - Digital cameras, speakers, video, music
- Piconet coordinator (PNC)
 - Sends beacons to devices to connect to the network
 - Uses superframes like 802.11
 - QoS based on TDMA
 - Controls time resources but does not exchange data
- 802.15.3c
 - Latest standard
 - Uses 60 GHz band, with same benefits as 802.11ad
 - Single-carrier and OFDM PHY modes

IEEE 802.15.4

- Low data rate, low complexity
 - Competitor to Bluetooth Smart
- PHY options in 802.15.4 and 802.15.4a
 - 868/915 MHz for 20, 40, 100, and 250 kbps
 - 2.4 GHz for 250 kbps
 - Ultrawideband (UWB)
 - Uses very short pulses with wide bandwidth
 - ✓ Low energy density for low interference with others
 - 851 kbps and optionally 110 kbps, 6.81 Mbps, or 27.234 Mbps
 - 2.4 GHz chirp spread spectrum for 1 Mbps and optionally 250 kbps
 - Sinusoidal signals that change frequency with time

IEEE 802.15.4

- Many other creative and practical activities
- IEEE 802.15.4f – Active Radio Frequency Identification Tags (RFIDs)
 - Attached to an asset or person with a unique identification
 - An Active RFID tag must employ some source of power
- IEEE 802.15.4g – Smart Utility Networks (SUN)
 - Facilitates very large scale process control applications such as the utility smart-grid network
- IEEE 802.15.4j – Medical Body Area Networks
- IEEE 802.15.4k – Low Energy Critical Infrastructure Networks (LECIM)
 - To facilitate point to multi-thousands of points communications for critical infrastructure monitoring devices with multi-year battery life.
- IEEE 802.15.4p – Positive Train Control
 - Sensor, control and information transfer applications for rail transit

Other IEEE 802.15 standards

- 802.15.2 – Coexistence between 802.11 and 802.15
- 802.15.5 – Mesh networks
 - Multihop networking
- 802.15.6 – Body area networks
- 802.15.7 – Visible light communication

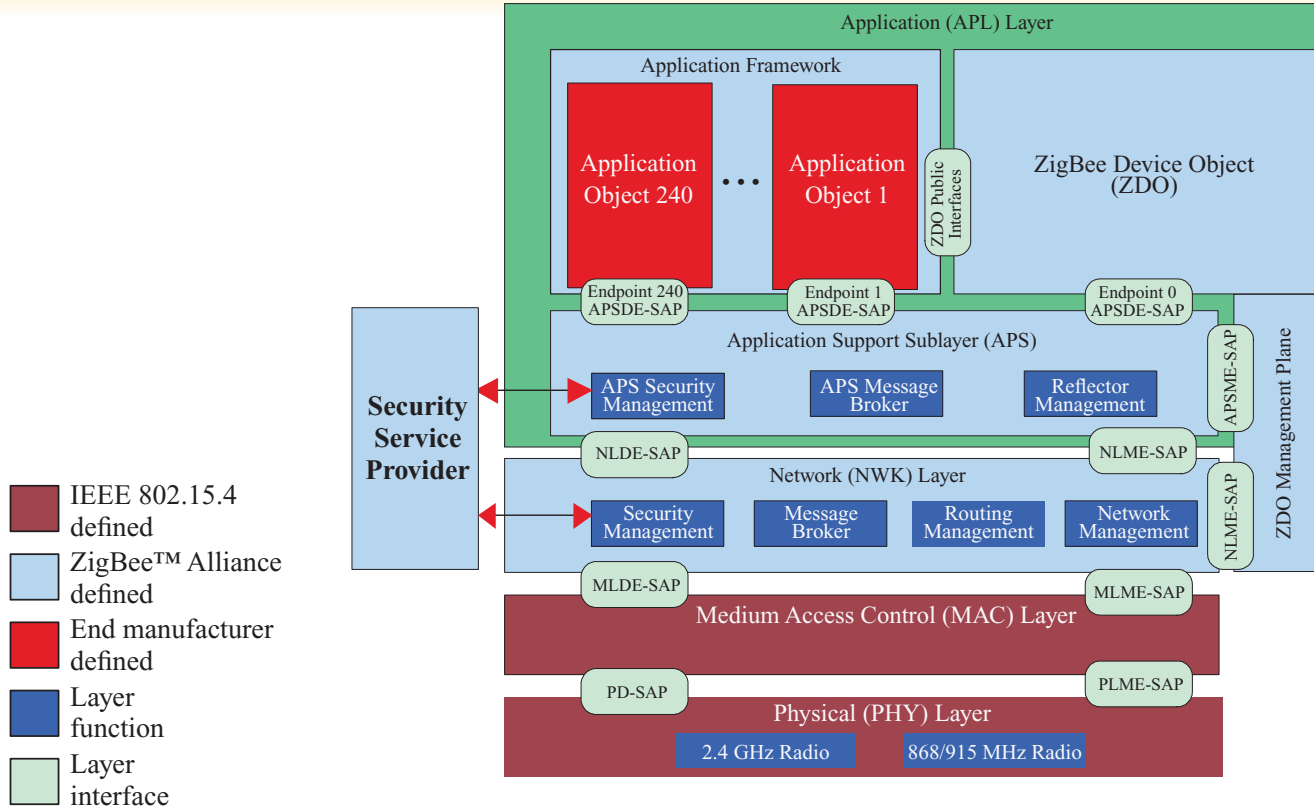
ZigBee

- Extends IEEE 802.15.4 standards
- Low data rate, long battery life, secure networking
- Data rates 20 to 250 kbps
- Operates in ISM bands
 - 868 MHz (Europe), 915 MHz (USA and Australia), 2.4 GHz (worldwide)
- Quick wake from sleep
 - 30 ms or less compared to Bluetooth which can be up to 3 sec.
 - ZigBee nodes can sleep most of the time

ZigBee

- ZigBee complements the IEEE 802.15.4 standard by adding four main components
 - Network layer provides routing
 - Application support sublayer supports specialized services.
 - ZigBee device objects (ZDOs) are the most significant improvement
 - Keep device roles, manage requests to join the network, discover devices, and manage security.
 - Manufacturer-defined application objects allow customization.

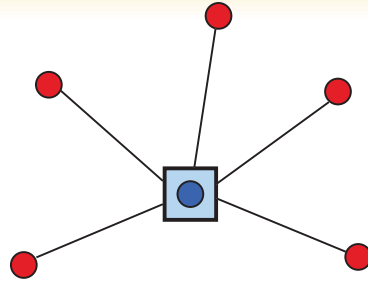
ZigBee Architecture



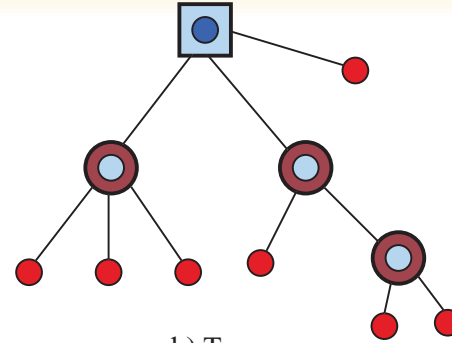
ZigBee

- Star, tree, or general mesh network structures
- ZigBee Coordinator
 - Creates, controls, and maintains the network
 - Only one coordinator in the network
 - Maintains network information, such as security keys
- ZigBee Router
 - Can pass data to other ZigBee devices
- ZigBee End Device
 - Only enough functionality to talk to a router or coordinator
 - Cannot relay information
 - Sleeps most of the time
 - Less expensive to manufacture

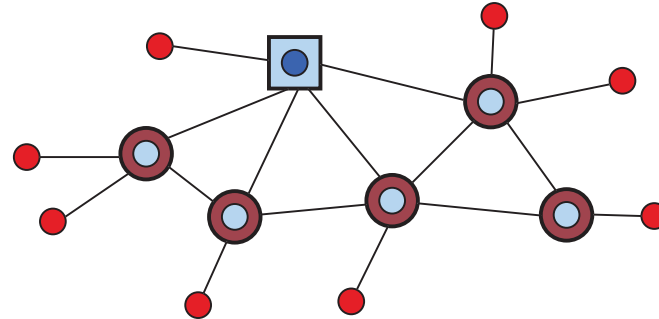
ZigBee Network



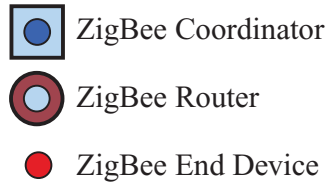
a) Star



b) Tree



c) Mesh



ZigBee alliance

- Industry consortium
- Maintains and publishes the ZigBee standard
 - ZigBee specifications in 2004
 - ZigBee PRO completed in 2007
 - Enhanced ZigBee
 - Profile 1 – home and light commercial use
 - Profile 2 – more features such as multicasting and higher security
- Application profiles
 - Allow vendors to create interoperable products if they implement the same profile

ZigBee application profiles

- ZigBee Building Automation (Efficient commercial spaces)
- ZigBee Health Care (Health and fitness monitoring)
- ZigBee Home Automation (Smart homes)
- ZigBee Input Device (Easy-to-use touchpads, mice, keyboards, wands)
- ZigBee Light Link (LED lighting control)
- ZigBee Network Devices (Assist and expand ZigBee networks)
- ZigBee Retail Services (Smarter shopping)
- ZigBee Remote Control (Advanced remote controls)
- ZigBee Smart Energy 1.1 (Home energy savings)
- ZigBee Smart Energy Profile 2 (IP-based home energy management)
- ZigBee Telecom Services (Value-added services)