Communcation Technologies

Giuseppe Anastasi

Executive Director, Industry 4.0 CrossLab

Dept. of Information Engineering, University of Pisa

E-mail: giuseppe.anastasi@unipi.it

Website: www.iet.unipi.it/g.anastasi/

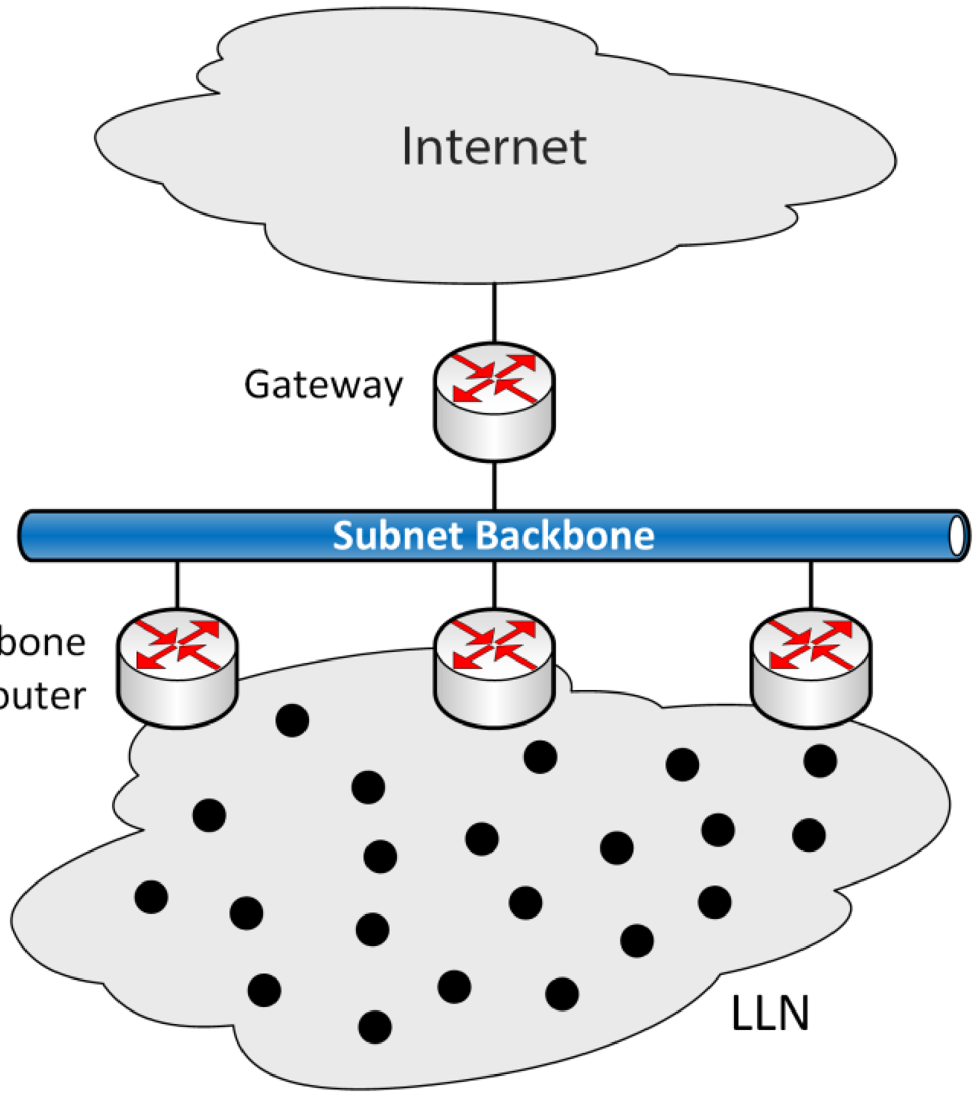
Goals

- Introducing low-layer protocols
  - Physical Layer
  - MAC
    - ⇨ Classification of MAC protocols
    - ⇨ Multiple Access + Power Management

- Presenting the main communication technologies for LLNs
  - IEEE 802.15.4, IEEE 802.15.4g
  - IEEE 802.11ah (WiFi HaLow)
  - Low-Power Wide Area Networks
  - PLC

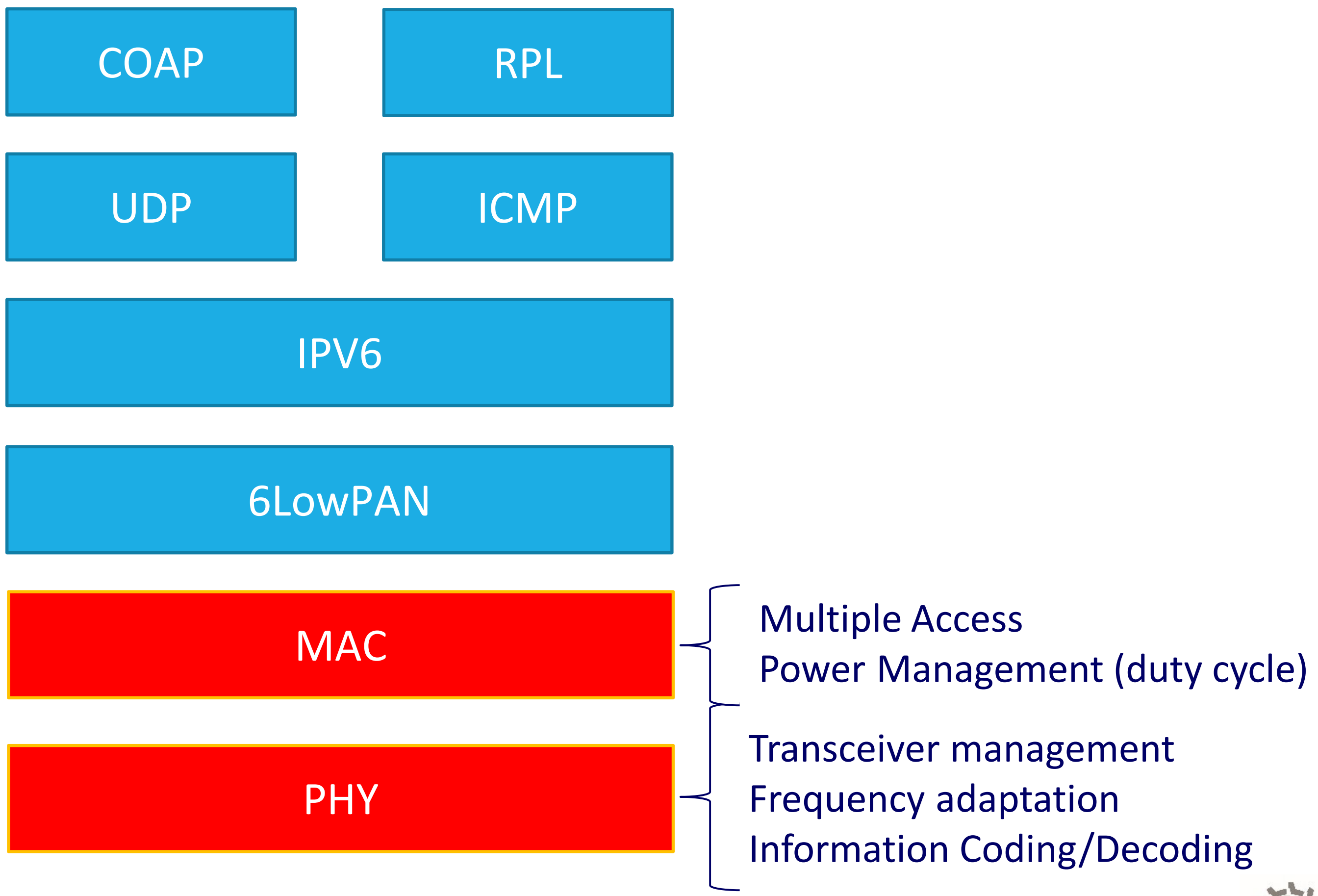
CROSSLAB Innovation for industry 4.0

IETF Reference Architecture for IoT



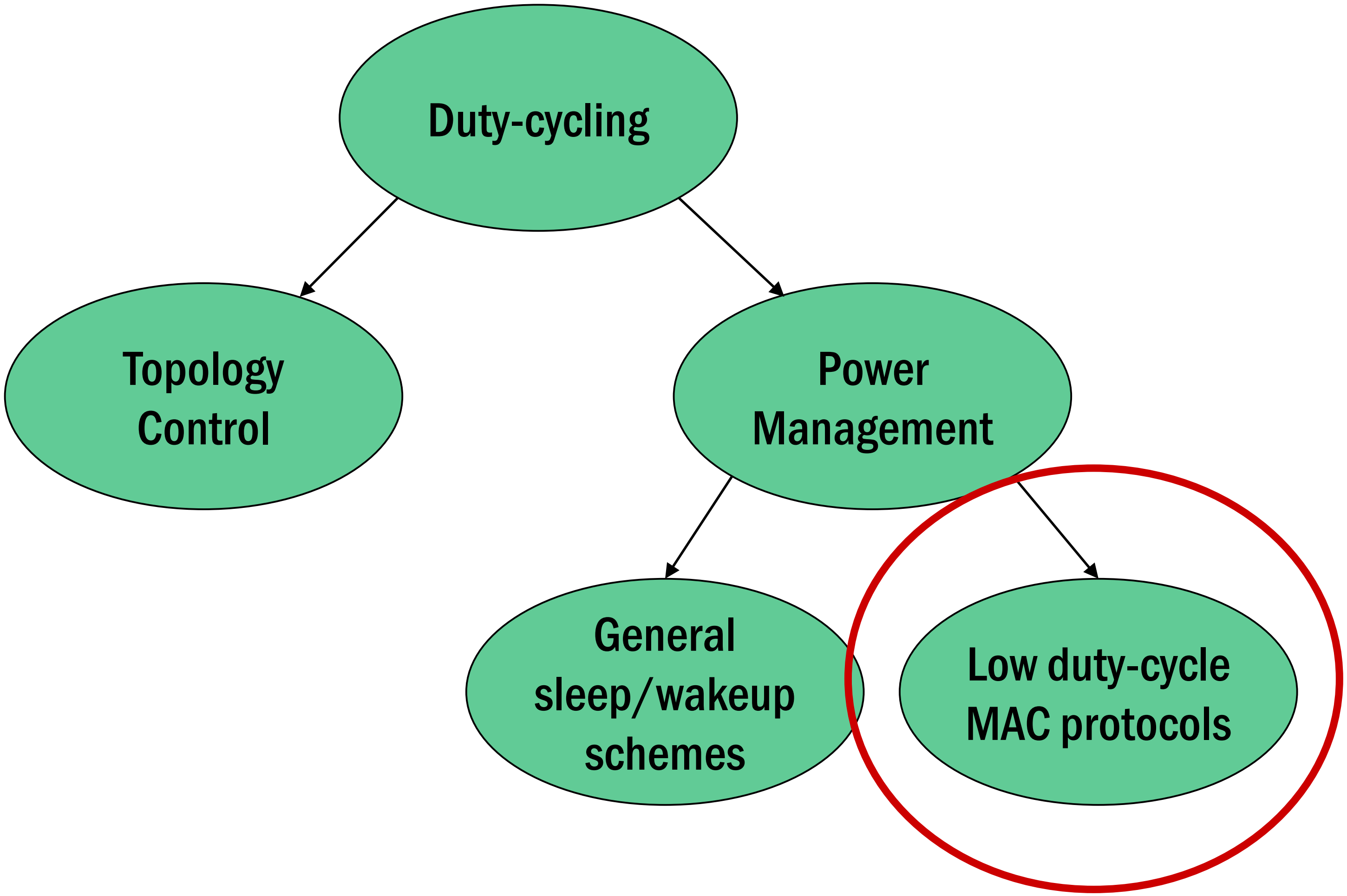
LLN: Low-power and Lossy Network

IETF IoT Protocol Stack



(Low-duty Cycle)
MAC Protocols

Power Management



Low duty-cycle MAC protocols

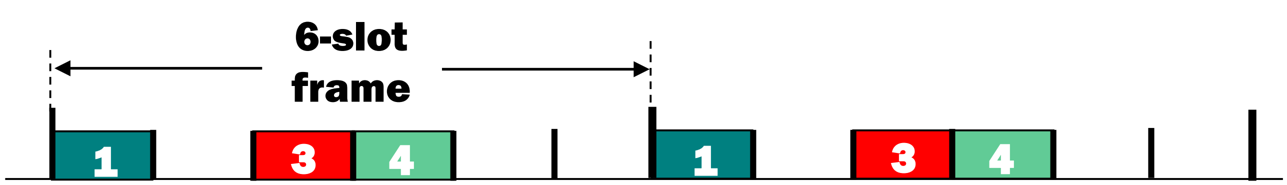
- Time-Slotted Access Protocols
  - ✓ effective reduction of power consumption
  - ✗ need precise synchronization, lack flexibility
- Contention-based MAC
  - ✓ good robustness and scalability
  - ✗ high energy expenditure (over-hearing, collisions)
- Hybrid schemes
  - Both TDMA + Contention Access Schemes
    - ⇨ 802.15.4 MAC
  - Switch between TDMA and CSMA, based on contention
    - ⇨ Z-MAC

Low duty-cycle MAC protocols

- Polling-based Access Protocols
  - Master-slave approach
  - Slaves must be polled by the master node
    - ⇨ According to a certain schedule
  - ✓ effective reduction of power consumption
  - ✗ need precise synchronization

Time-Slotted Access

- High Energy Efficiency: each node is active only during its own slot(s), and can sleep during the other slots
- Guaranteed Bandwidth: each node gets one or more fixed-length slots in each round
- Bounded and Predictable Latency: each node accesses the same slot(s) in every frame
- Synchronization: sensor nodes need to synchronize their clocks
- Lack of flexibility: Join and leave of nodes may cause slot re-allocation; unused slots go idle
- Vulnerability to Selective Jamming attacks



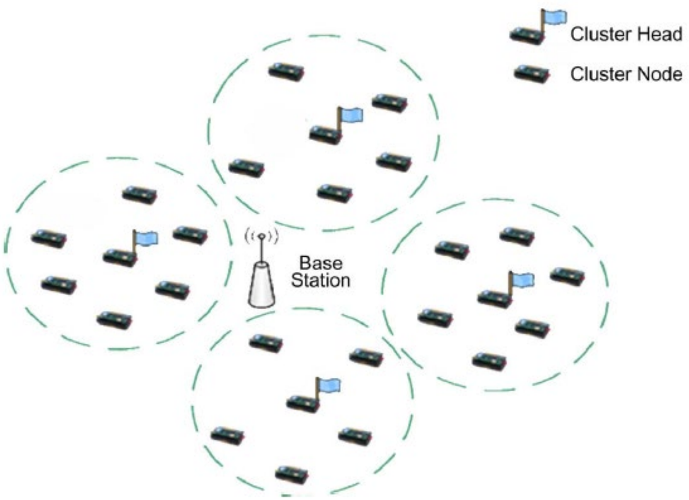
Time-Sotted Access

- Master node
  - Synchronization ➔ Superframe
  - Slot allocation (static or dynamic allocation)
- Superframe
  - A number of slots reserved for
    - ⇨ Master to slave communication (SYNCH, slot allocation,…)
    - ⇨ Slave to master communication (slot request, …)
- Extension to multi-hop sensor networks
  - Synchronization
  - Slot allocation

LEACH

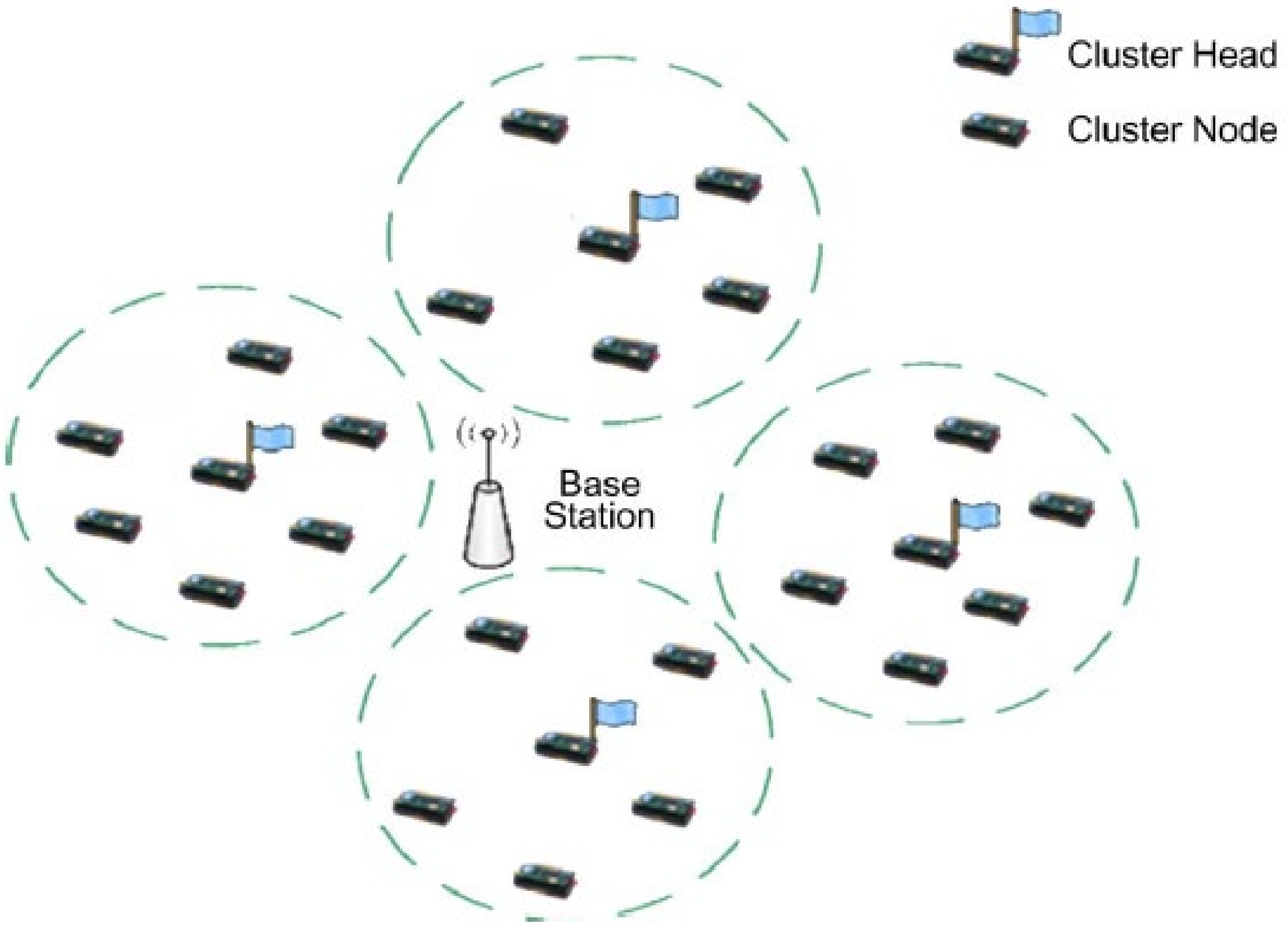
Low Energy Adaptive Clustering Hierarchy

- Nodes are organized in clusters
- A Cluster-Head (CH) for each cluster
  - Coordinates all the activities within the cluster
- Nodes report data to their CH through TDMA
  - Each nodes has a predefined slot
  - Nodes wakeup only during their slot
- The CH has the highest energy consumption
  - sensor nodes rotate in the role of CH



W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, **Energy-Efficient Communication Protocol for Wireless Microsensor Networks**, *Proc. Hawaii International Conference on System Sciences (HICSS 2000)*, January, 2000.

Hierarchical LEACH



Cluster Heads also use a Time-slotted approach for sending data received from Cluster Nodes to the Base Station

Time-Slotted Access: Summary

- High energy efficiency
  - Nodes are active only during their slots
  - Minimum energy consumption without extra overhead
- Limited Flexibility
  - A topology change may require a different slot allocation pattern
- Limited Scalability
  - Finding a scalable slot allocation function is not trivial, especially in multi-hop (i.e., hierarchical) networks
- Interference prone
  - Finding an interference-free schedule may be hard
  - The interference range is larger than the transmission range
- Tight Synchronization Required
  - Clock synch introduces overhead

CSMA-based MAC Protocols

- No synchronization required
  - Robustness
  - Synch may be needed for power management
- Large Flexibility
  - A topology change do not require any re-configuration or schedule update notification
- Limited Scalability
  - A large number of nodes can cause a large number of collisions and retransmissions
- Low Energy Efficiency
  - Nodes may conflict
  - Energy consumed for overhearing

B-MAC with Low-power Listening

- Availability
  - Designed before the IEEE 802.15 MAC (at UCB)
  - Shipped with the TinyOS operating system
- B-MAC design considerations
  - simplicity
  - configurable options
  - minimize idle listening (to save energy)
- B-MAC components
  - CSMA without RTS/CTS
  - optional low-power listening (LPL)
  - optional acknowledgements

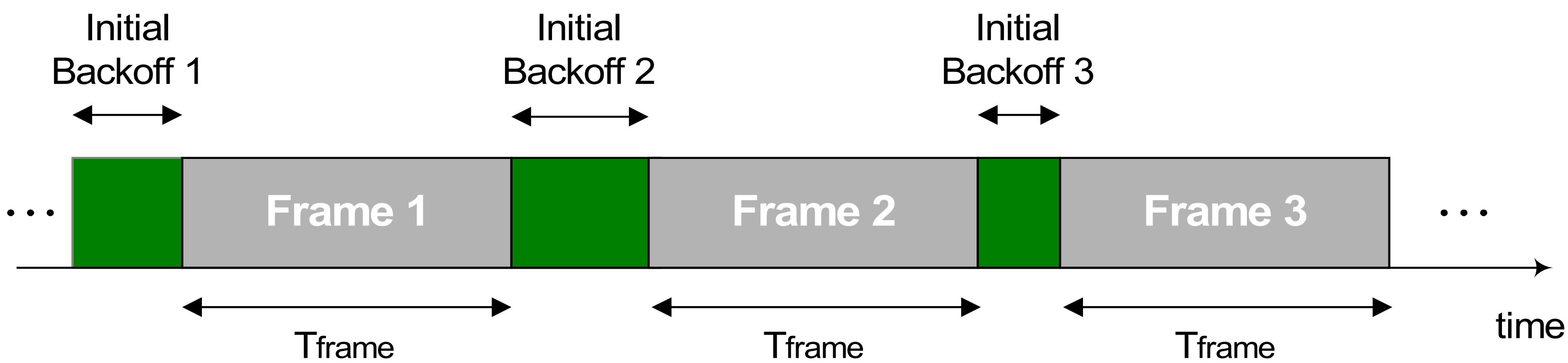
Access Protocol

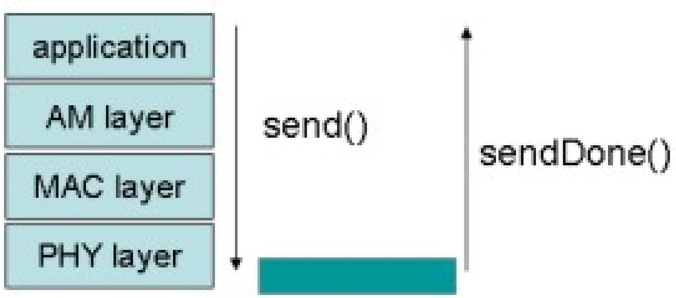
1. Generate random delay before transmitting
   - ⇨ Uniformly distributed in [15-68.3] ms
2. Channel assessment
   a. If Channel free → transmit (and wait for ACK)
   b. Else (Channel busy) → random backoff
      - ⇨ Uniformly distributed in [12.08 - 193.3] ms
3. Go to 2

CROSSLAB
Innovation for industry 4.0

B-MAC: maximum available throughput

Optimal case: just one node is sending

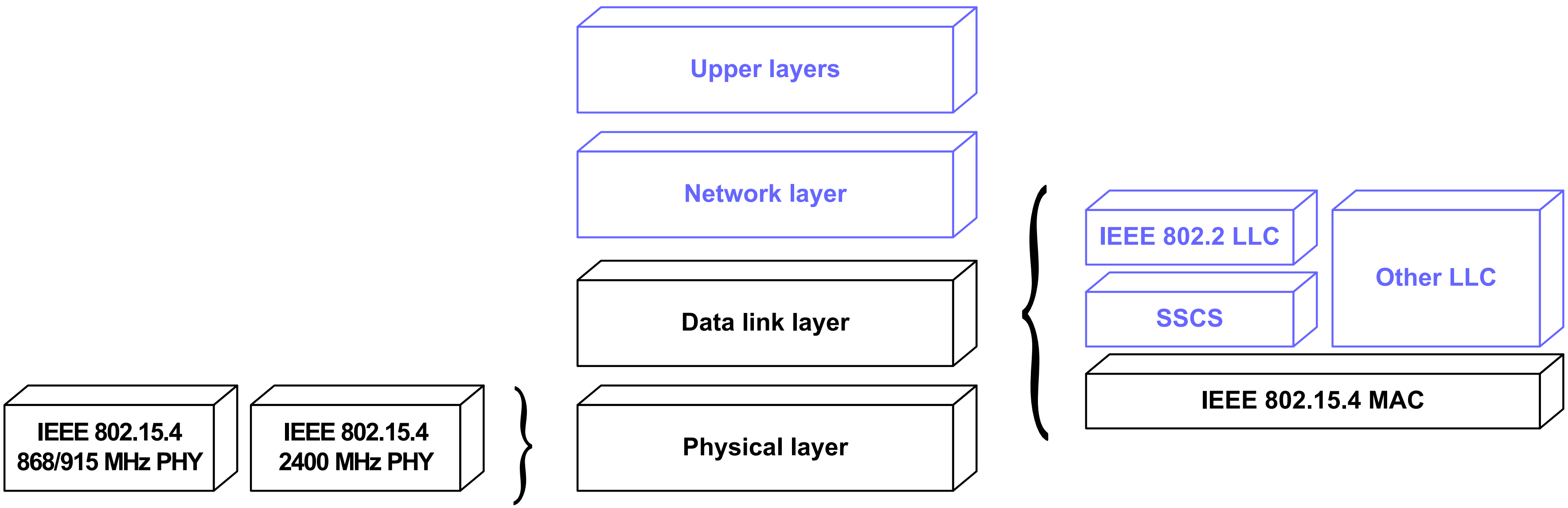




$$T_{th}(m) = \frac{m}{\cancel{\bar{T}_{sw}} + \bar{T}_{BO} + T_{frame}(m)}$$

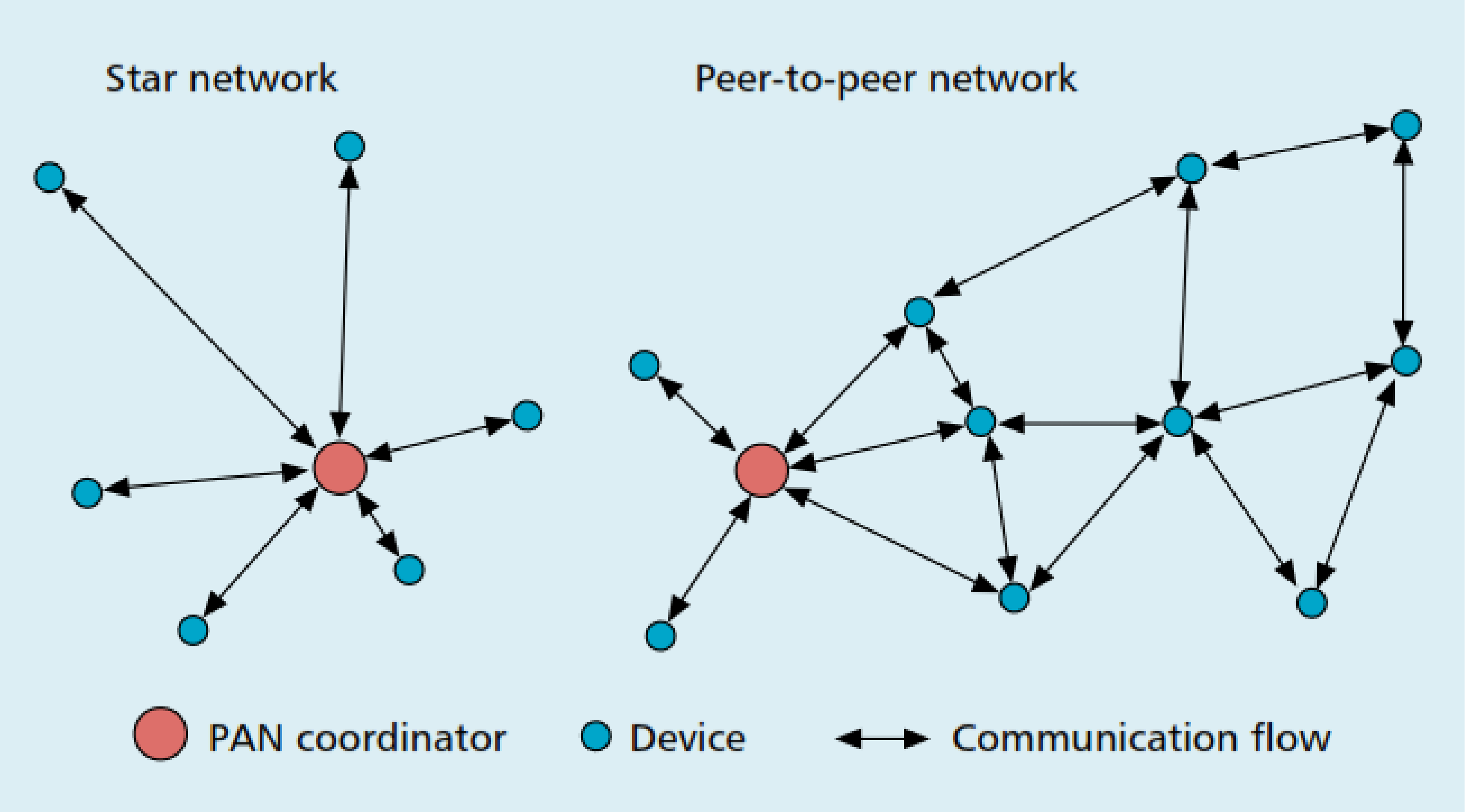
IEEE 802.1.5.4 Standard

IEEE 802.15.4 standard

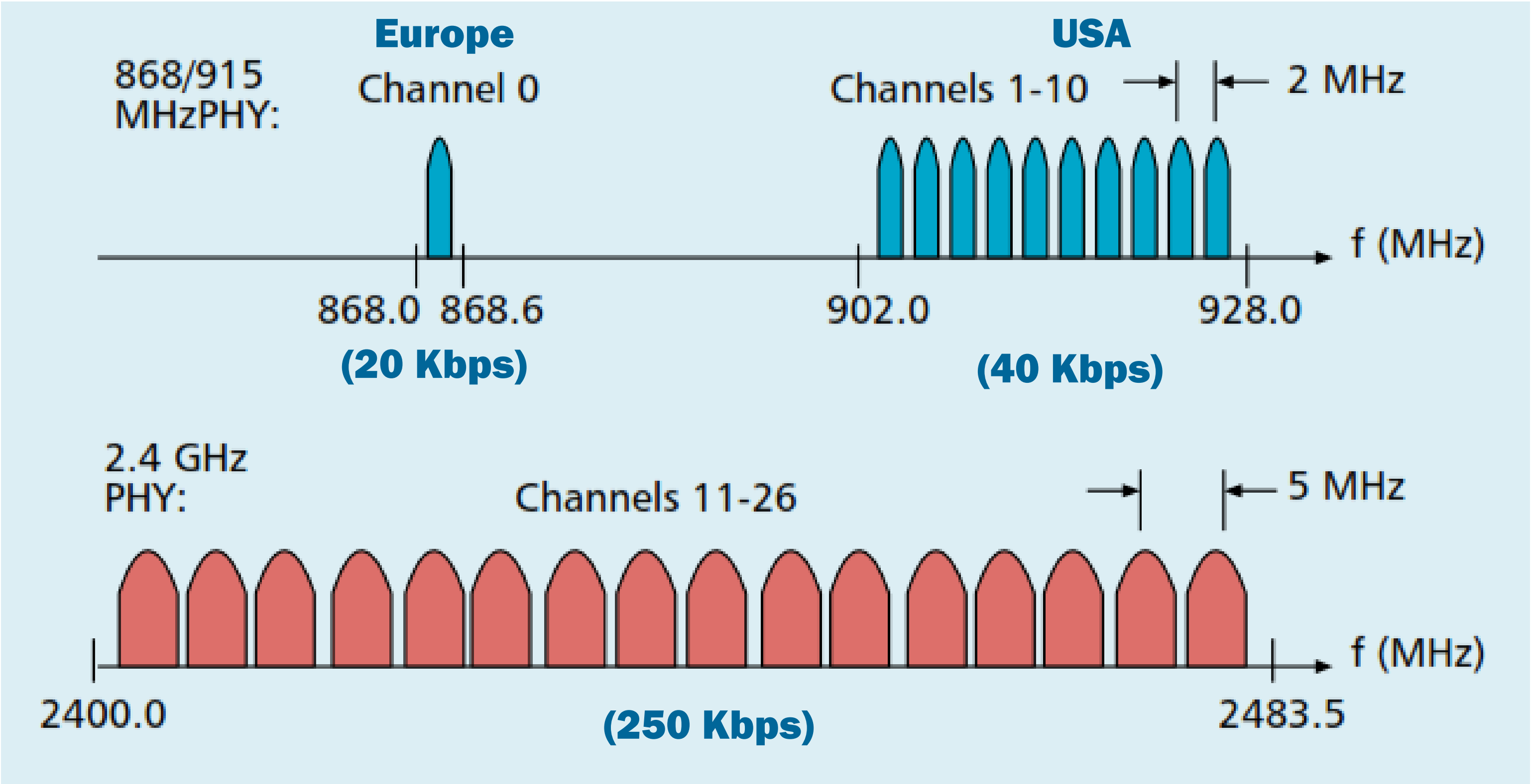


- Standard for Personal Area Networks (PANs)
  - low-rate and low-power
  - PHY and MAC layers
- Main features
  - transceiver management
  - channel access
  - PAN management

Network Topologies



Channel frequencies



Channel number	Channel center frequency (MHz)
$k = 0$	868.3
$k = 1, 2, \ldots, 10$	$906 + 2(k - 1)$
$k = 11, 12, \ldots, 26$	$2405 + 5(k - 11)$

MAC Addresses

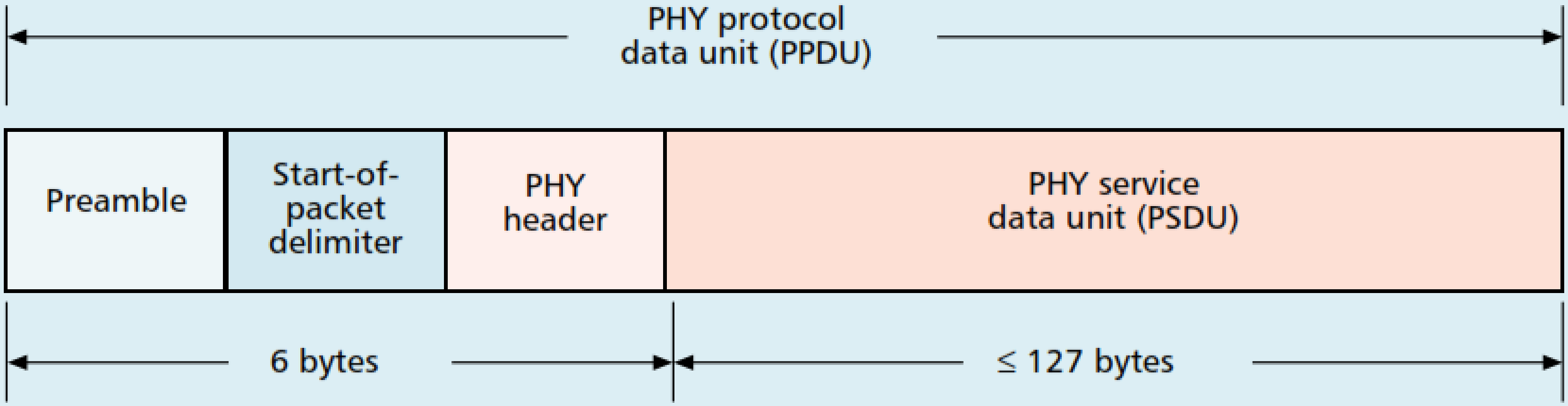
- PAN Address
  - Identifies the PAN within a certain geographic area
  - Allows the communication between different PANs
  - 16 bits (Broadcast PAN Address: 0x FFFF)

- Device Address
  - Identifies the device within a PAN
  - Extended Address: 64 bits
  - Reduced Address: 16 bits

Device Address

- Extended Address: 64 bits
  - IEEE Extended Unique Identifier (EUI-64)
    - ⇨ Most significant 24 bits assigned by IEEE (OUI)
    - ⇨ Least significant 40 bits assigned by manufacturer
- Reduced Address: 16 bits
  - Negotiated with the PAN coordinator
  - Can replace the extended address in all communications
  - Broadcast address: 0x FFFF

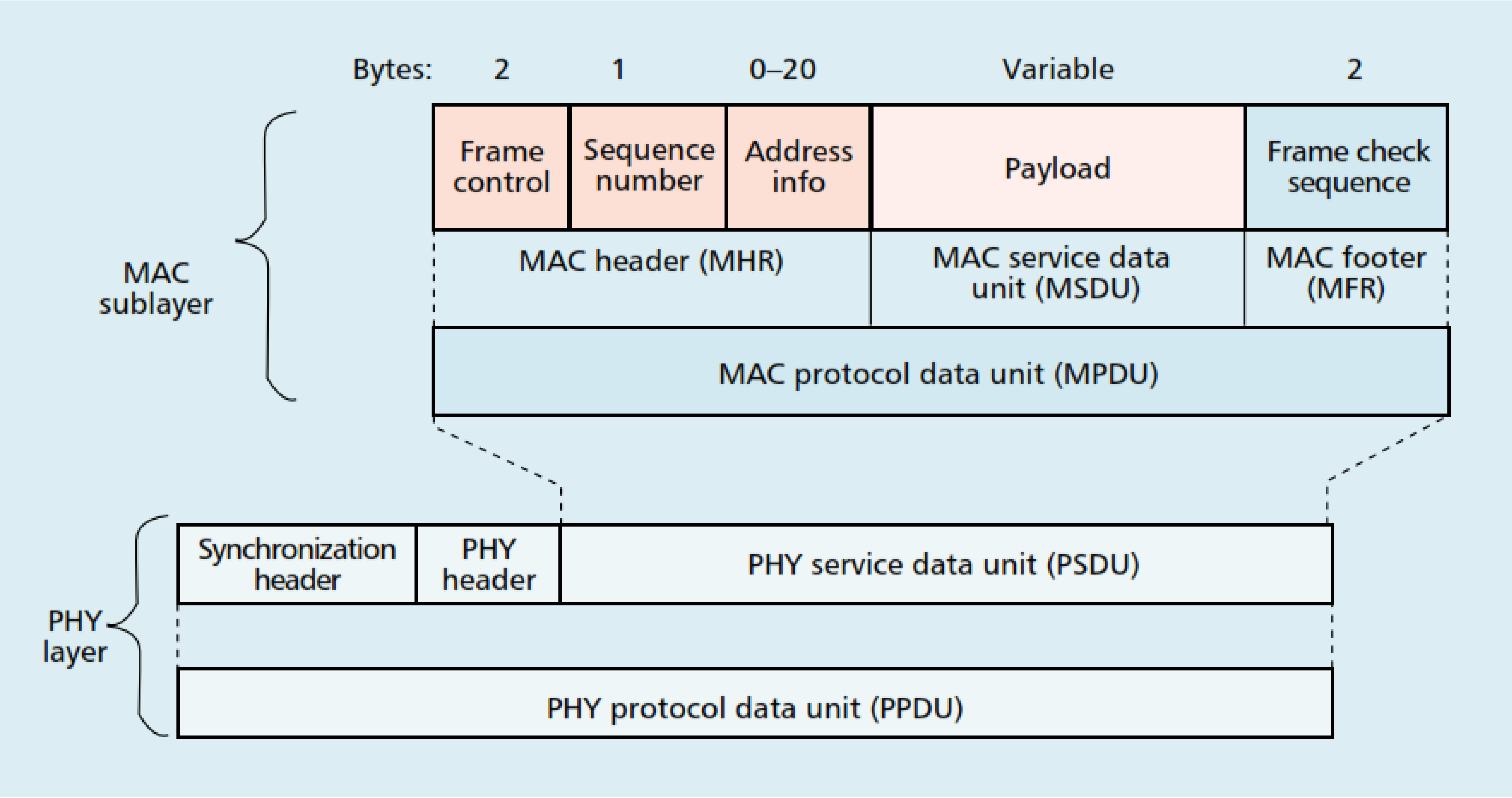
Frame Format



PHY packet fields:

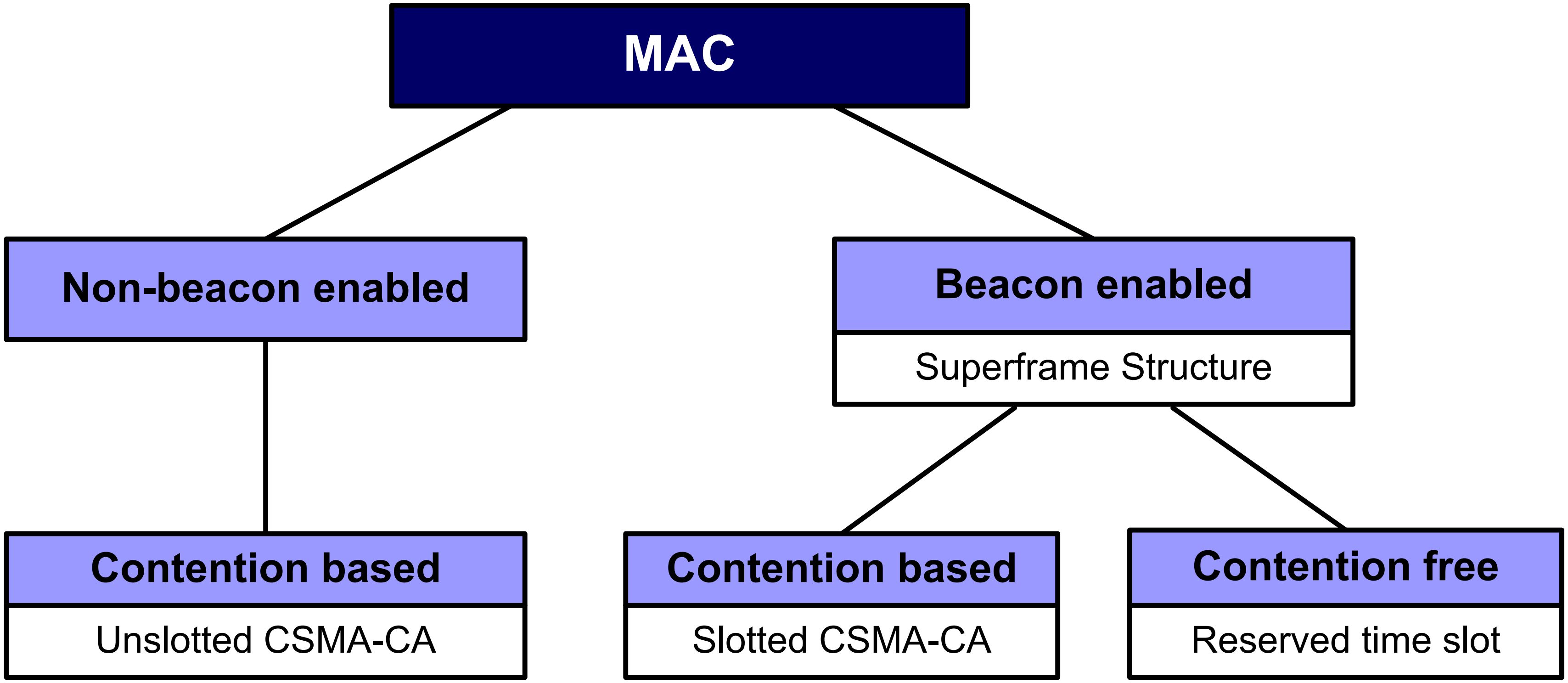
- Preamble (32 bits) — synchronization
- Start-of-packet delimiter (8 bits) — signify end of preamble
- PHY header (8 bits) — specify length of PSDU
- PSDU (≤ 127 bytes) — PHY layer payload

Frame Format



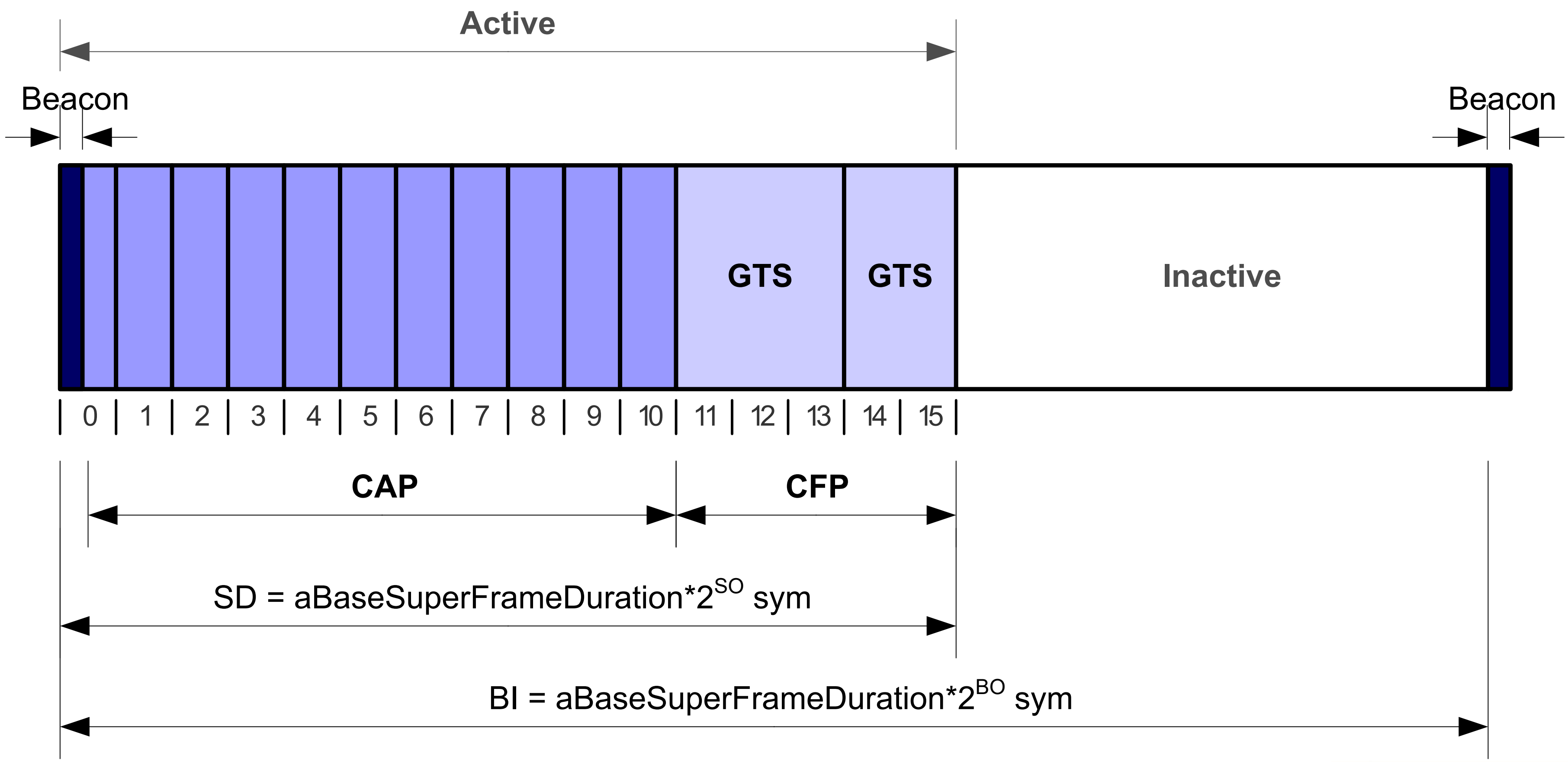
IEEE 802.15.4: MAC protocol

- Two different channel access methods
  - Beacon-Enabled duty-cycled mode
  - Non-Beacon Enabled mode (aka Beacon Disabled mode)

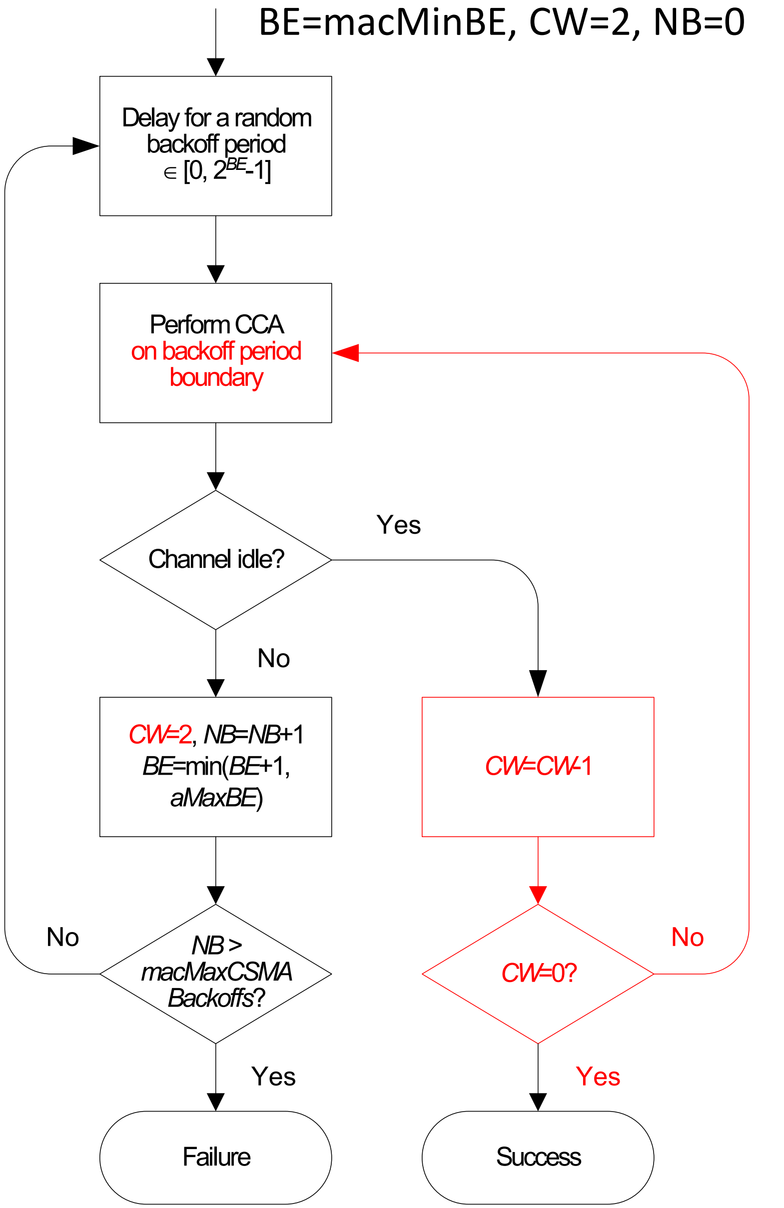


IEEE 802.15.4 MAC
Beacon Enabled Mode

IEEE 802.15.4: Beacon Enabled mode



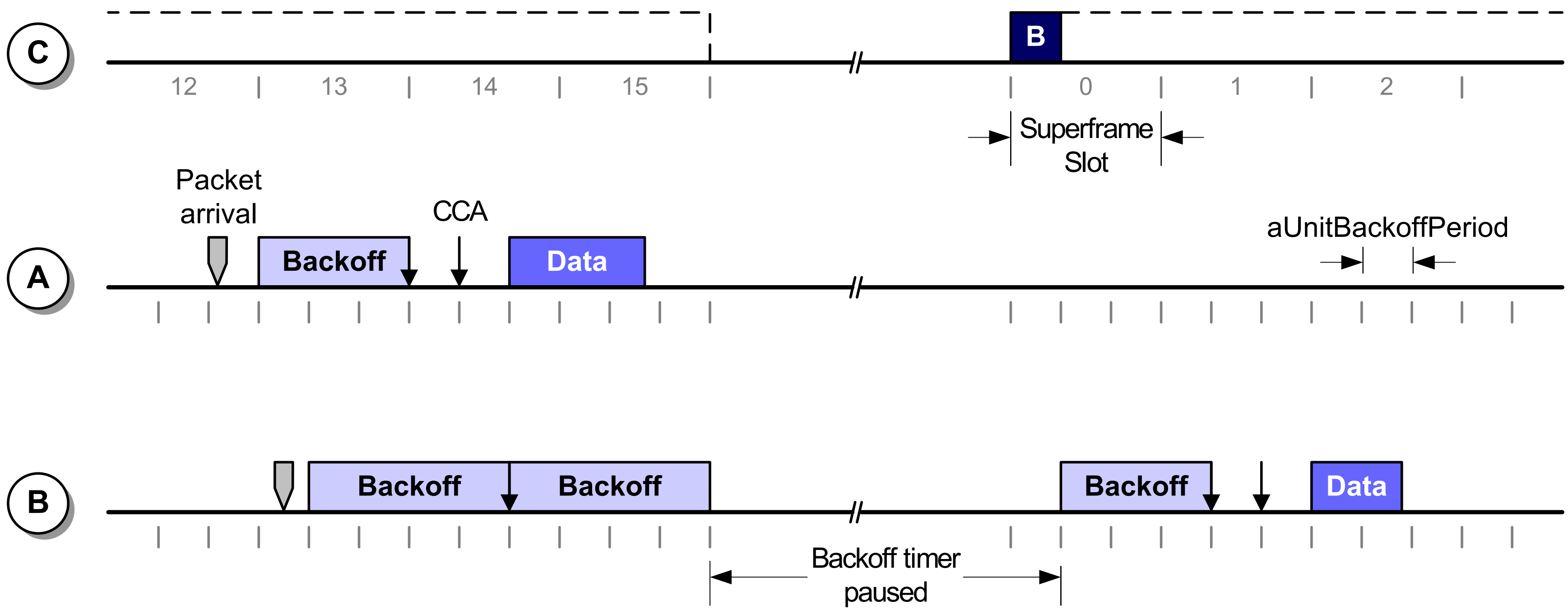
CSMA/CA: Beacon-enabled mode



At each trial the backoff-window size is doubled

Only a limited number of attempts is permitted (***macMaxCSMABackoffs***)

CSMA/CA: Beacon-enabled mode



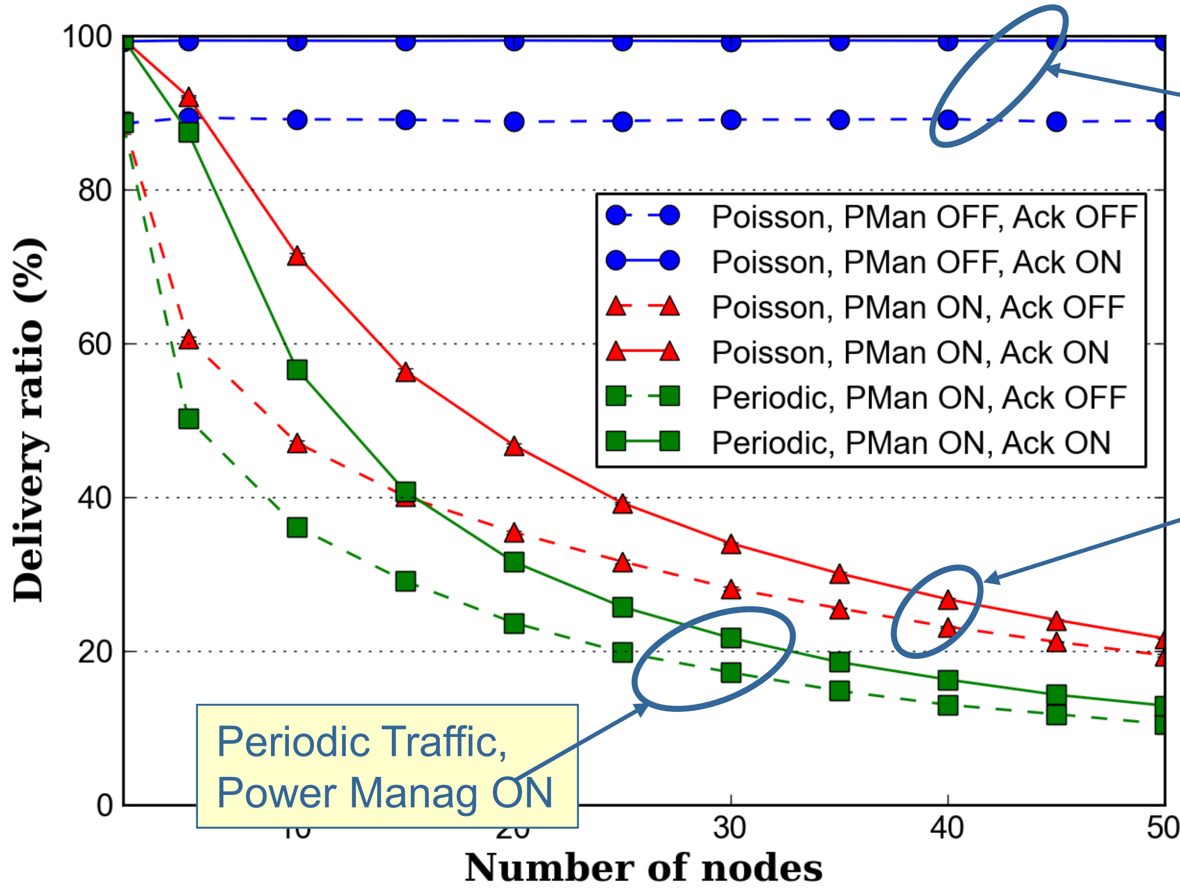
Acknowledgement Mechanism

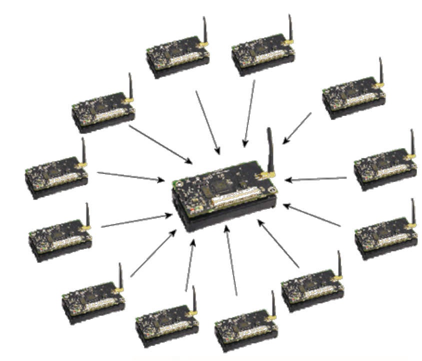
- Optional mechanism
- Destination Side
  - ACK sent upon successful reception of a data frame
- Sender side
  - Retransmission if ACK not (correctly) received within the timeout
  - At each retransmission attempt the backoff window size is re-initialized
  - Only a maximum number of retransmissions allowed (*macMaxFrameRetries)*

Security

- Unsecured Mode
  - No security service provided
- ACL Mode
  - Access Control based on Access Control List (ACL)
  - Any node has an ACL specifying nodes authorized to perform specific actions
- Secured Mode
  - Access Control List (always active)
  - replay attack protection, message integrity, confidentiality (optional)
  - Based on AES with 128-bit key

802.15.4 MAC Performance





G. Anastasi, M. Conti, M. Di Francesco, **A Comprehensive Analysis of the MAC Unreliability Problem in IEEE 802.15.4 Wireless Sensor Networks**, *IEEE Transactions in Industrial Informatics,* Vol. 7, N. 1, Feb 2011.

Key Question

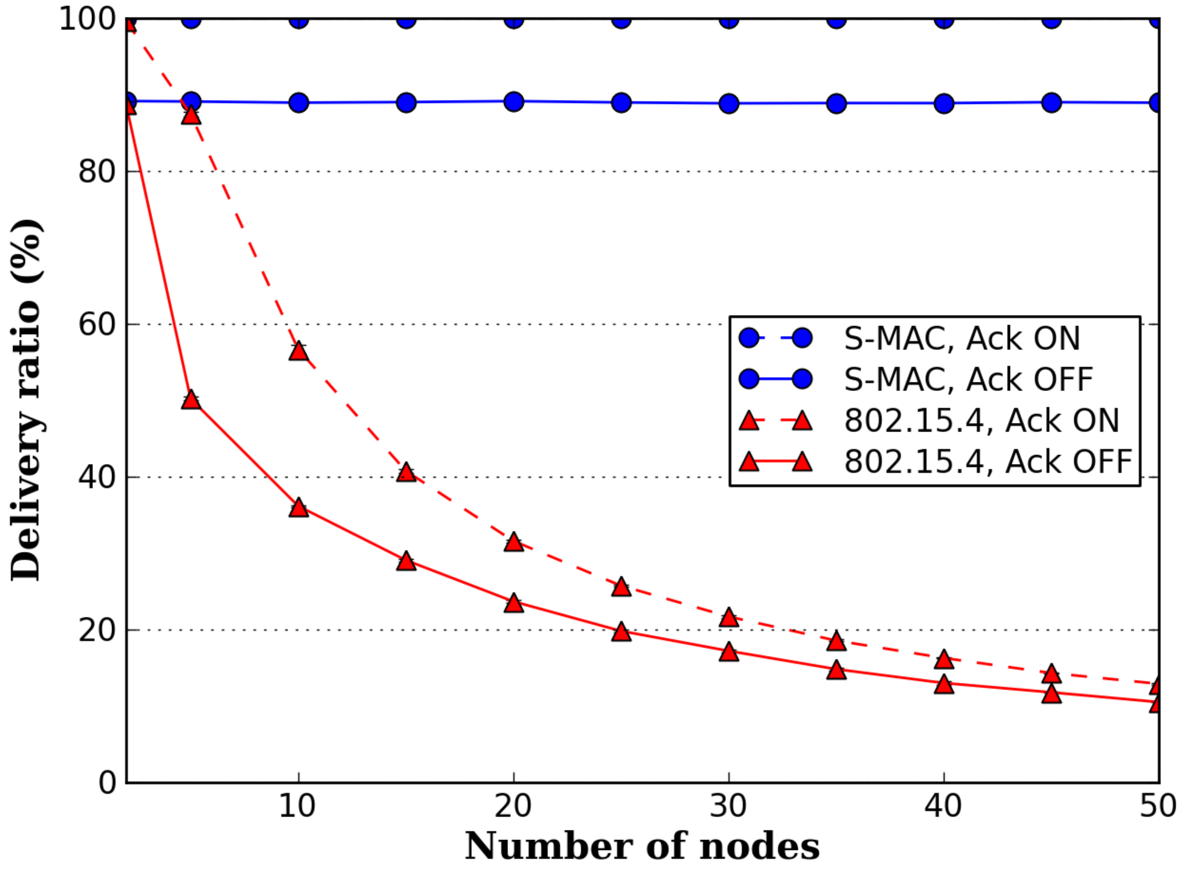
Why the 802.15.4 MAC Reliability Problem?

Possible Answers

- The access method is CSMA
  - Contention increases with the # of active nodes
- The periodic Beacon synchronizes nodes' accesses
  - *All* sensor nodes contend for channel access upon receiving a beacon

How about other CSMA-based MAC protocols operating in same conditions?

802.15.4 MAC vs. S-MAC



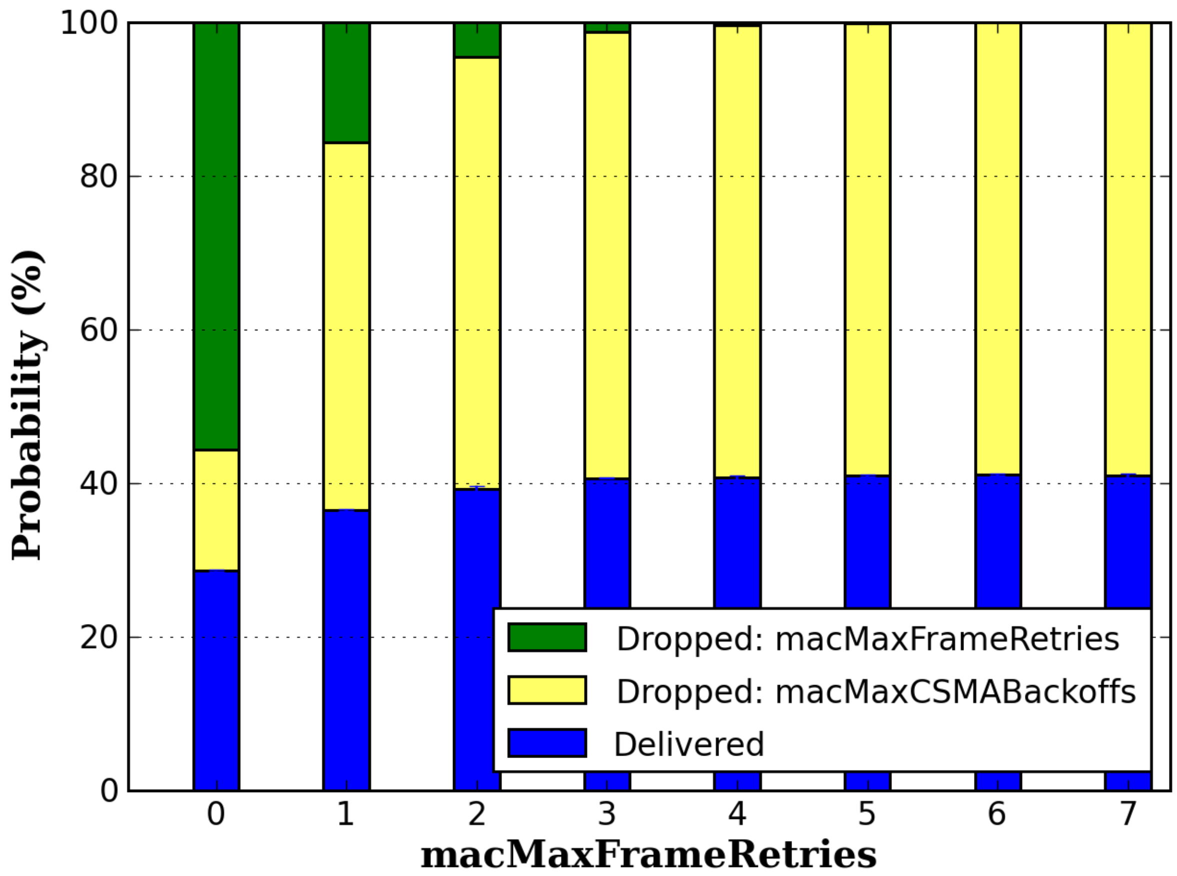
Influence of CSMA/CA parameters

- Analysis of each single CSMA/CA parameter
  - 15 sensor nodes
  - Periodic Traffic
  - Power Management ON, ACK ON

Parameter	2003 release	2006 release	Notes
macMaxFrameRetries	3 (*aMaxFrameRetries*)	0÷7 Default: 3	Max number of re-transmissions
macMaxCSMABackoff	0÷5 Default: 4	0÷5 Default: 4	Max number of backoff stages
macMaxBE	5 (*aMaxBE*)	3÷8 Default: 5	Maximum Backoff Window Exp.
macMinBE	0÷3 Default: 3	0÷7 Default: 3	Minimum Backoff Window Exp.

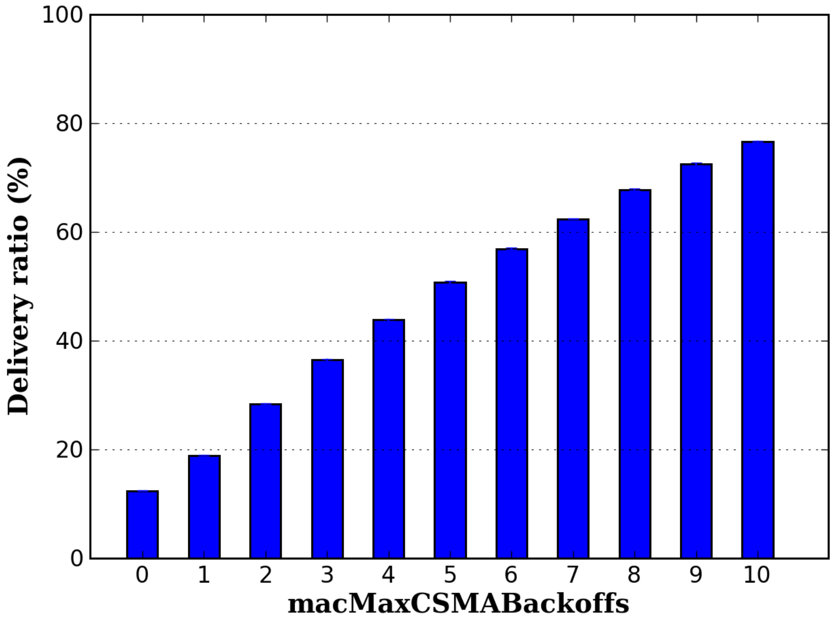
Influence of Number of RTx

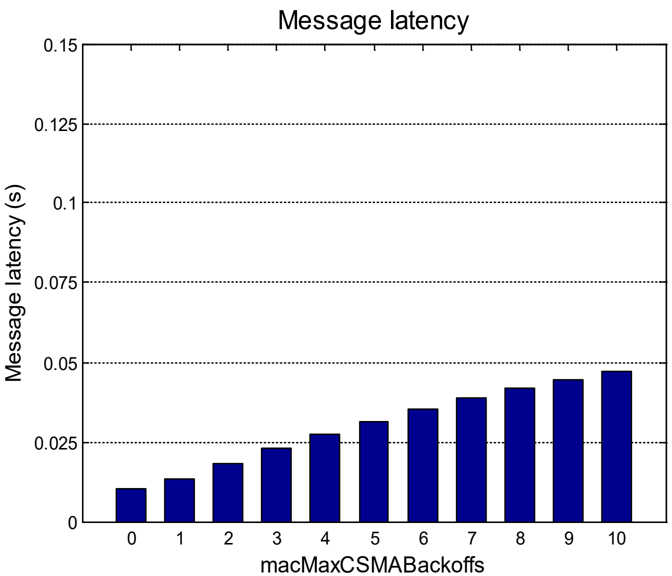
macMaxFrameRetries: 0-7 (default 3)

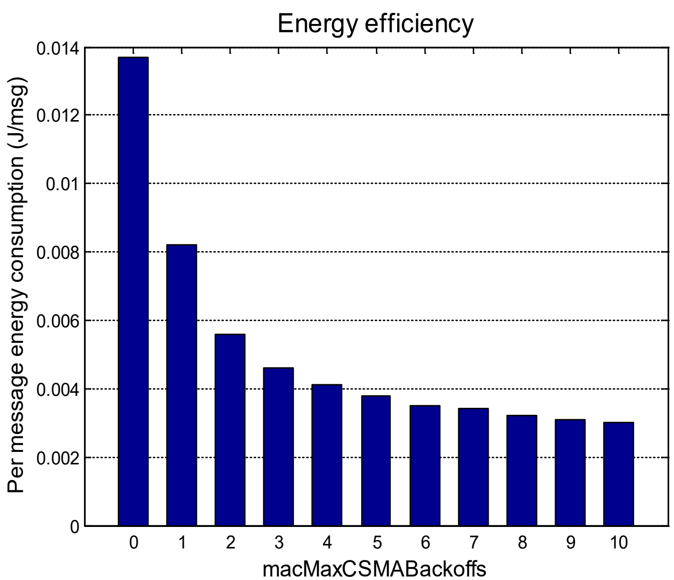


Influence of Number of Backoff Stages

macMaxCSMABackoffs: 0-5 (default 4)



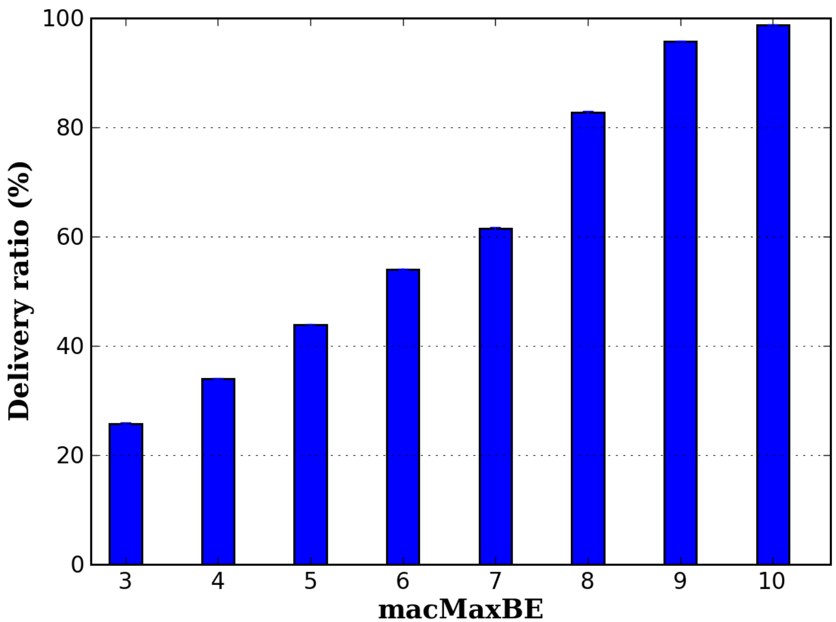


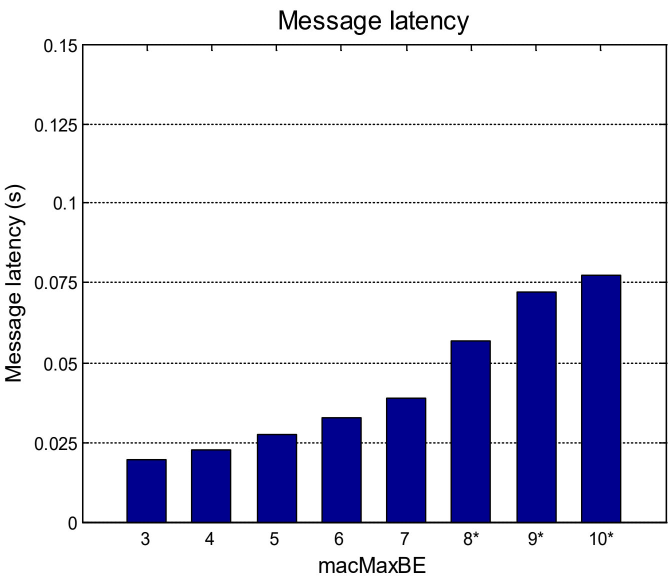


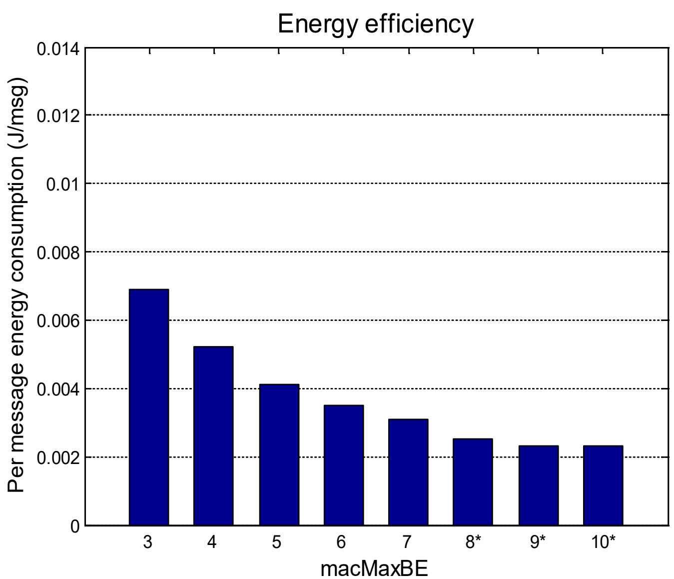
Influence of Maximum Backoff Window

macMaxBE: 3-8 (default 5)

macMaxCSMABackoffs ≥ macMaxBE – macMinBE



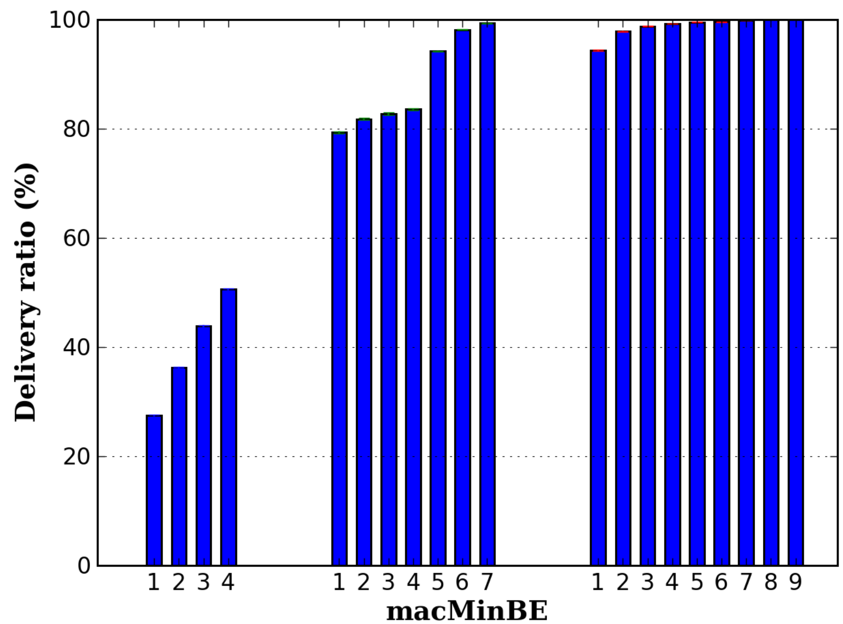


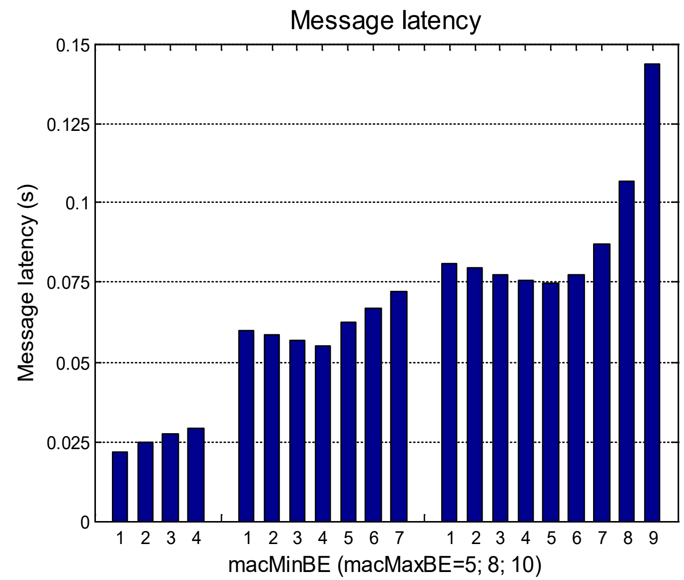


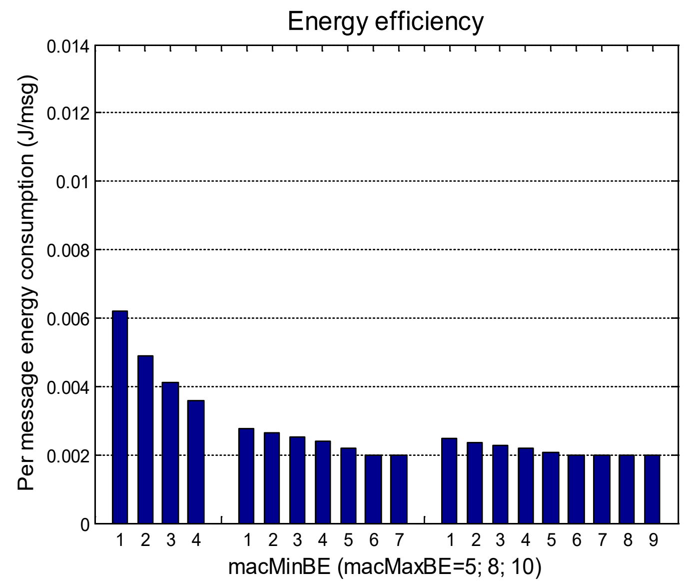
Influence of Minimum Backoff Window

macMinBE: 0-7 (default 3)

We varied *macMinBE* in [0, *macMaxBE*-1]





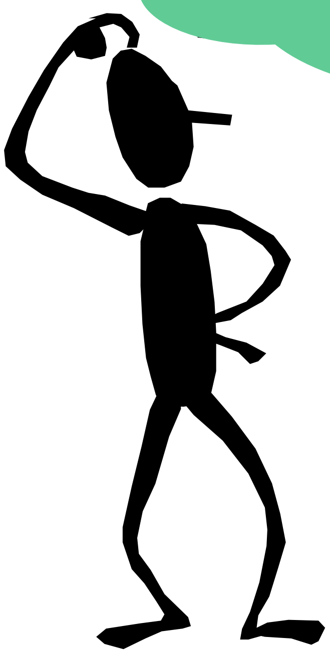


Learned Lesson

- The MAC unreliability problem is mainly due to the CSMA/CA algorithm
- The periodic beacon synchronizes channel accesses thus maximizing contention
- The problem is exacerbated by the default MAC parameter values
  - Not appropriate for WSNs operating in BE mode

Enhancements

How to avoid the MAC Reliability Problem?

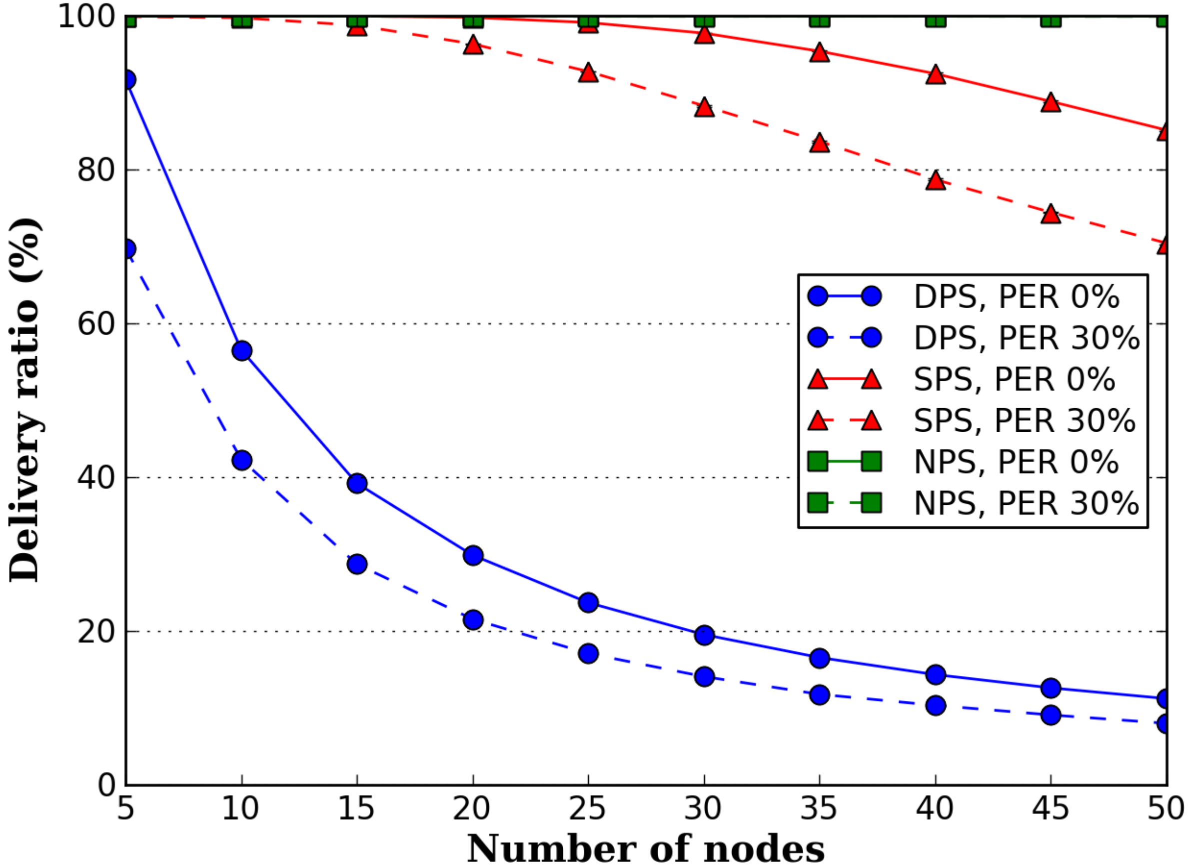


Possible Solutions

- *DPS (Default Parameter Set)*
  - Set di parametri con i *valori di default* previsti dallo standard
- *SPS (Standard Parameter Set)*
  - Set di parametri con i *valori massimi* previsti dallo standard
- *NPS (Non-standard Parameter Set)*:
  - Set di parametri con valori *oltre quelli consentiti* dallo standard

	macMinBE	macMaxBE	macMaxCSMABackoff	macMaxFrameRetries
DPS	3	5	4	3
SPS	7	8	5	7
NPS	8	10	10	10

Single-hop scenario: PDR vs. PER

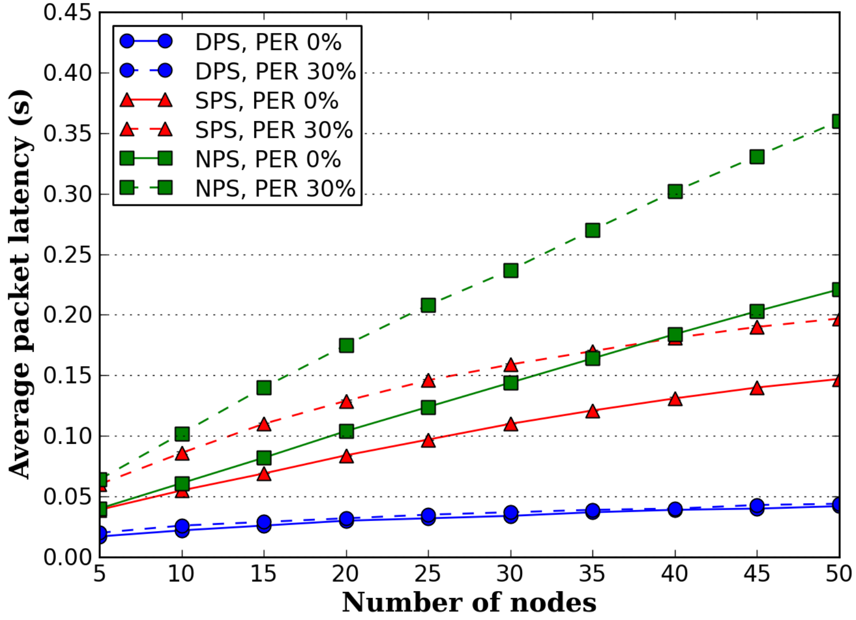


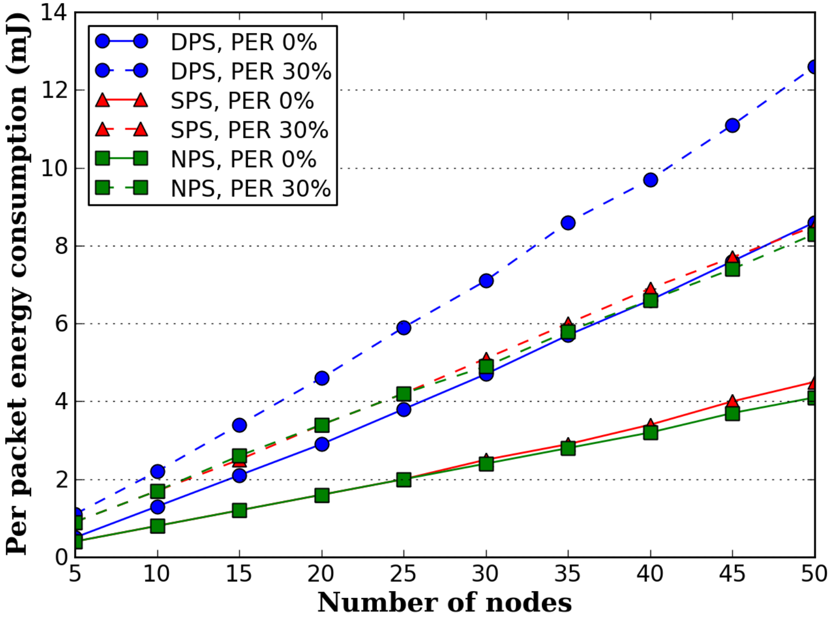
G. Anastasi, M. Conti, M. Di Francesco, **A Comprehensive Analysis of the MAC Unreliability Problem in IEEE 802.15.4 Wireless Sensor Networks**, *IEEE Transactions in Industrial Informatics,* Vol. 7, N. 1, Feb 2011.

Single-hop scenario

Avg. Latency

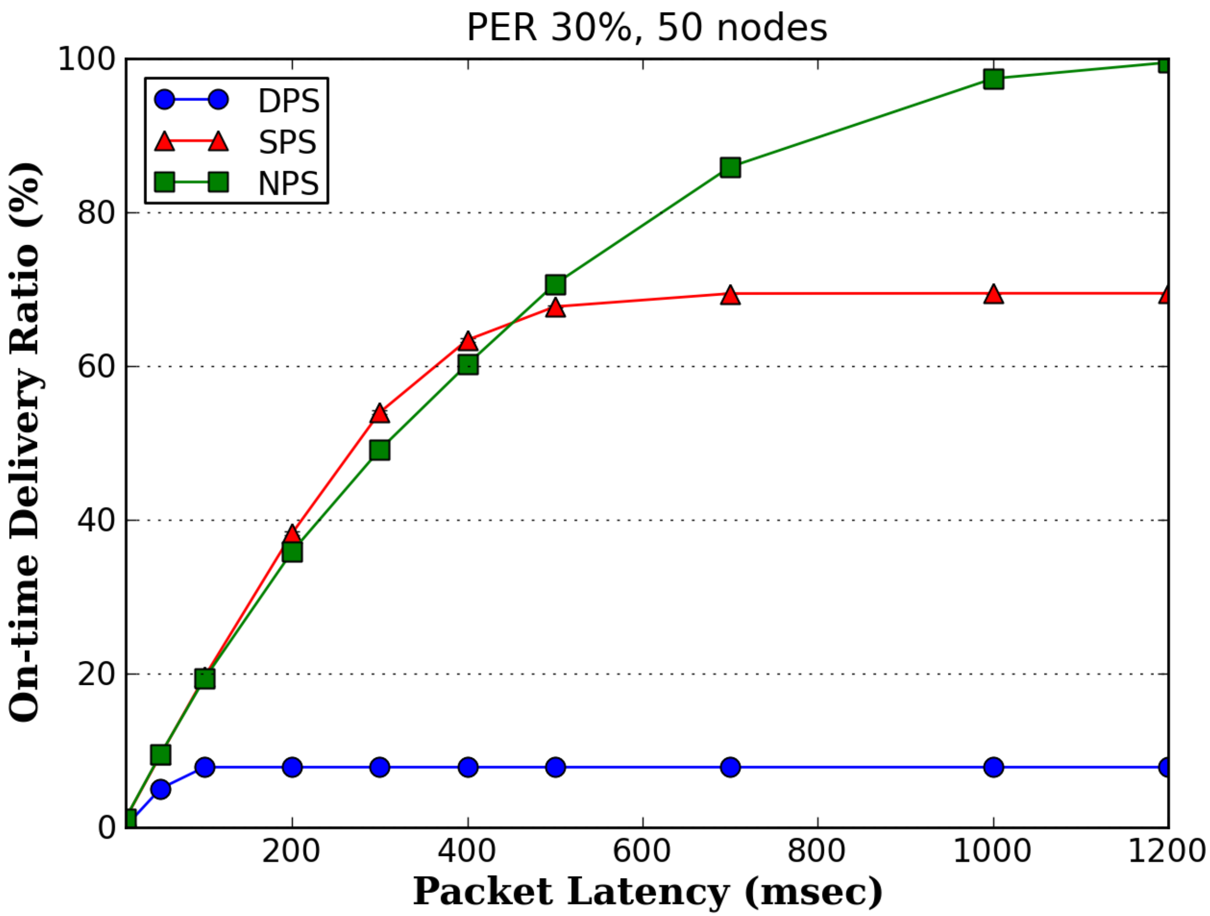
Energy/msg





G. Anastasi, M. Conti, M. Di Francesco, **A Comprehensive Analysis of the MAC Unreliability Problem in IEEE 802.15.4 Wireless Sensor Networks**, *IEEE Transactions in Industrial Informatics,* Vol. 7, N. 1, Feb 2011.

Timeliness vs. Delivery Ratio

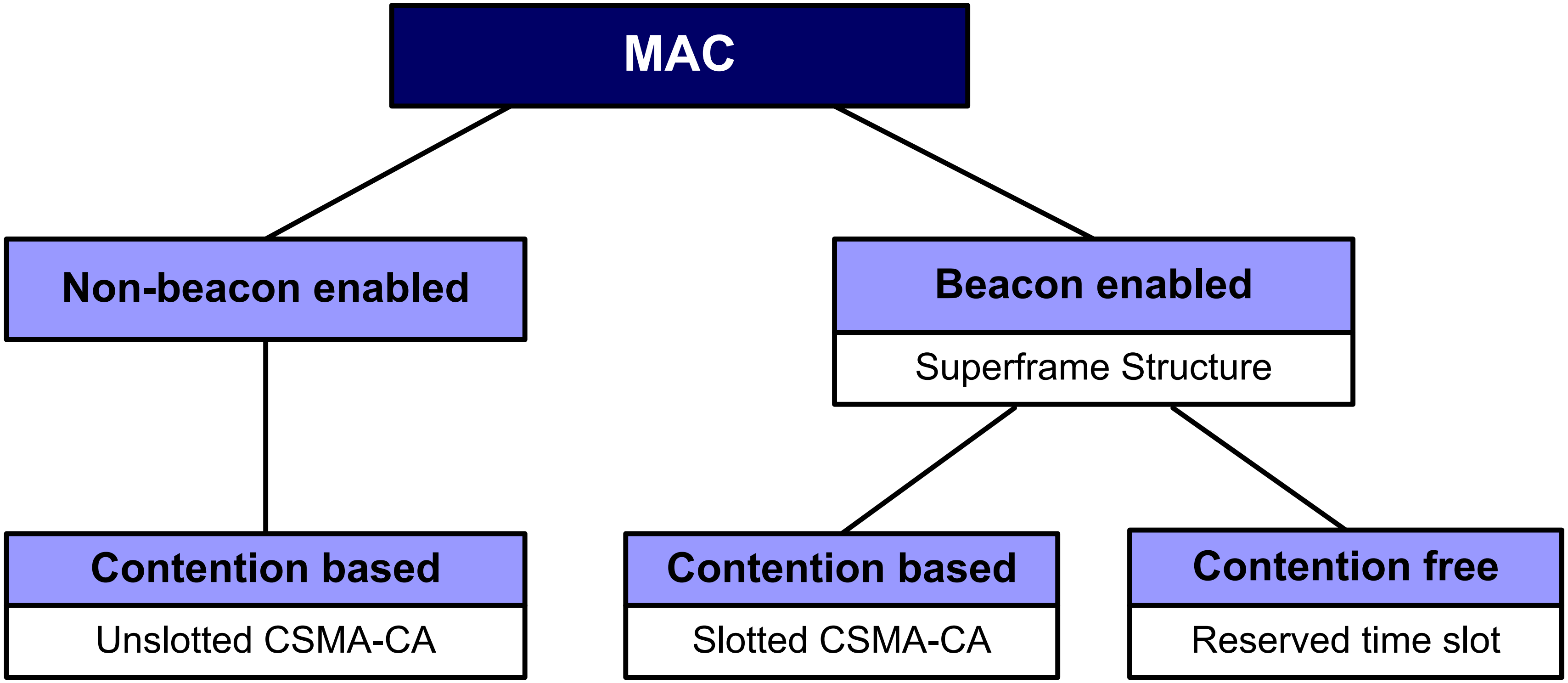


G. Anastasi, M. Conti, M. Di Francesco, **A Comprehensive Analysis of the MAC Unreliability Problem in IEEE 802.15.4 Wireless Sensor Networks**, *IEEE Transactions in Industrial Informatics,* Vol. 7, N. 1, Feb 2011.

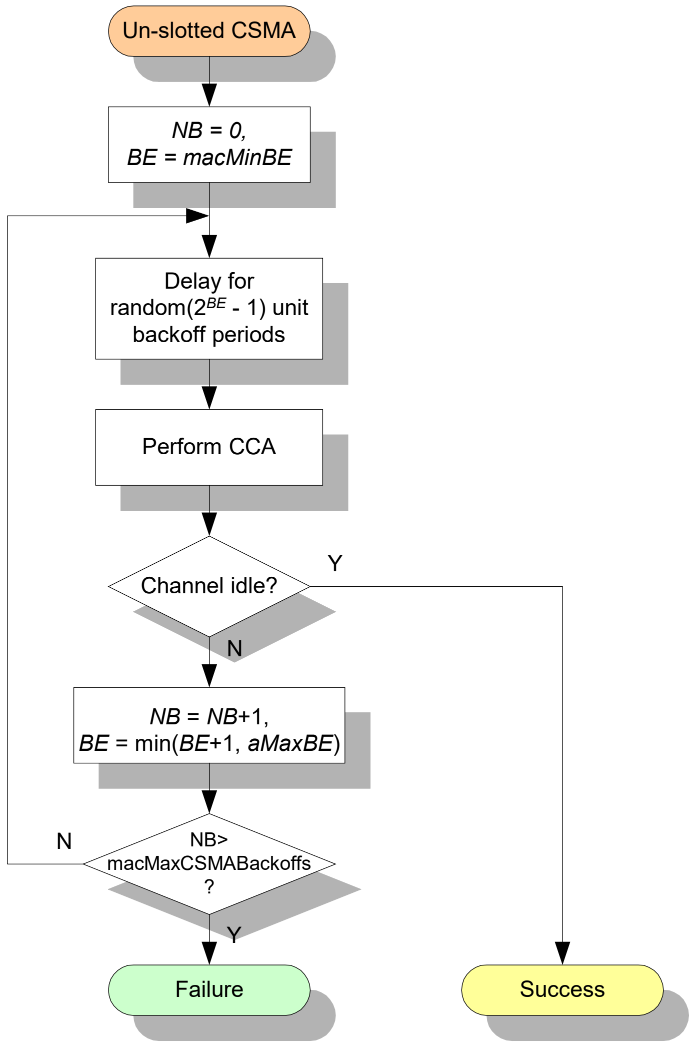
IEEE 802.15.4 MAC
Non-Beacon Enabled Mode

IEEE 802.15.4: MAC protocol

- Two different channel access methods
  - Beacon-Enabled duty-cycled mode
  - Non-Beacon Enabled mode (aka Beacon Disabled mode)



CSMA/CA: Beacon-Disabled mode



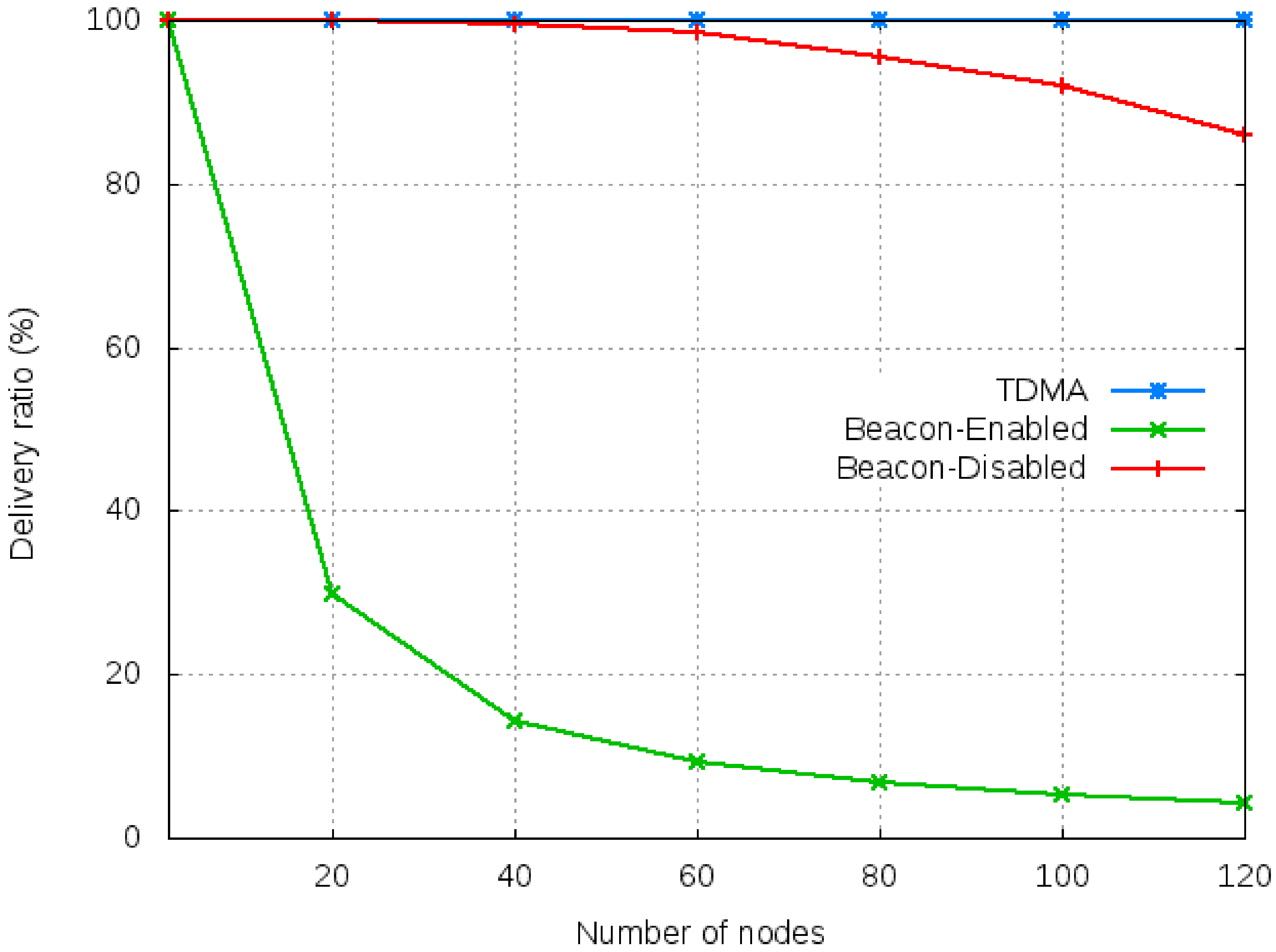
At each trial the backoff-window size is doubled

Only a limited number of attempts is permitted (***macMaxCSMABackoffs***)

Acknowledgement Mechanism

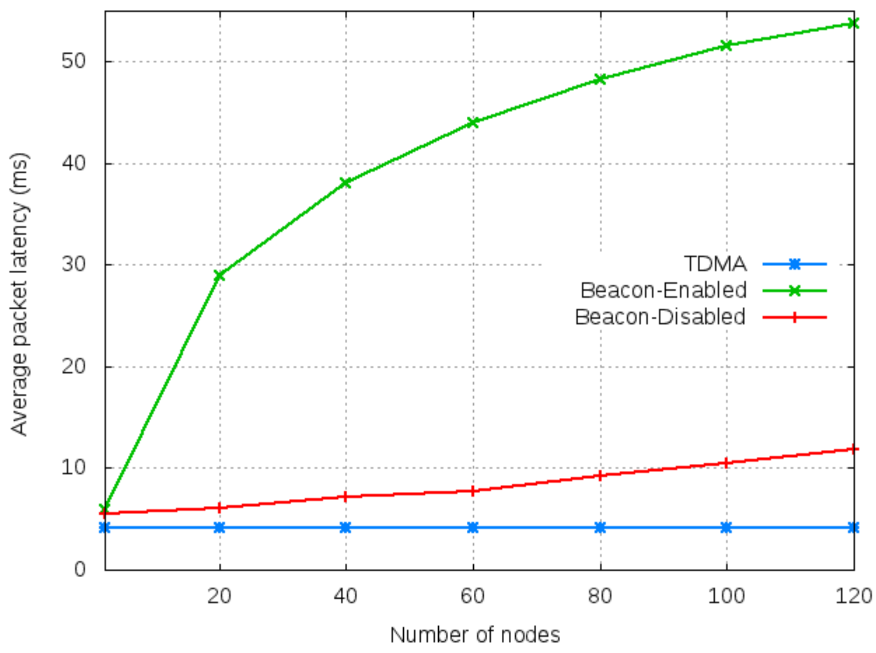
- Optional mechanism
- Destination Side
  - ACK sent upon successful reception of a data frame
- Sender side
  - Retransmission if ACK not (correctly) received within the timeout
  - At each retransmission attempt the backoff window size is re-initialized
  - Only a maximum number of retransmissions allowed (*macMaxFrameRetries)*

Performance with Beacon Disabled

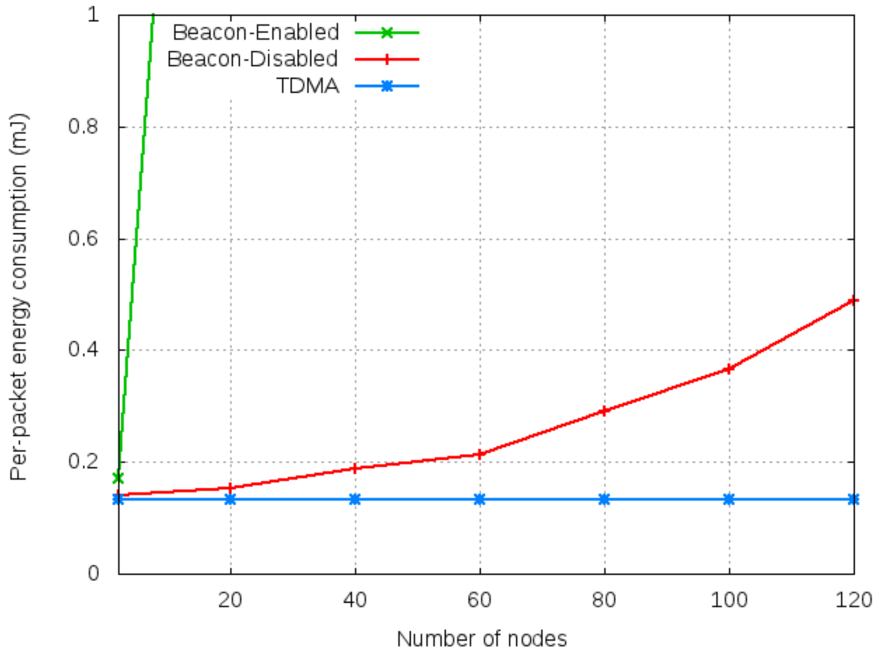


Performance with Beacon Disabled

Latency



Energy/packet



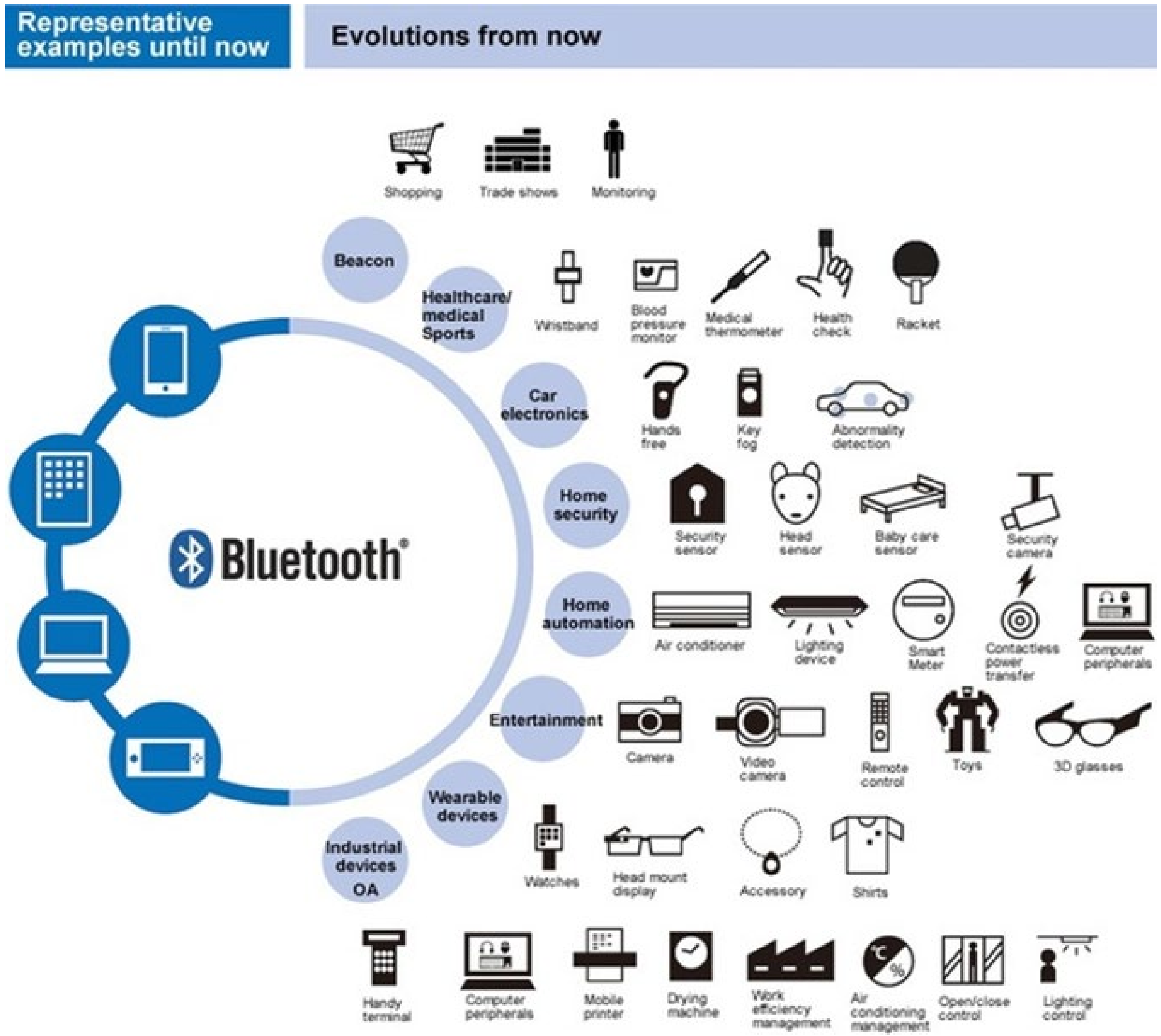
Other LLN Technologies

Bluetooth

Bluetooth Evolution

Version	
Bluetooth 5	
Bluetooth 4.2	
Bluetooth 4.1	
Bluetooth 4.0	Bluetooth Low Energy
Bluetooth 3.0	Highspeed 24Mbps
Bluetooth 2.0	2.1Mbps
Bluetooth 1.2	723.1Kbps
Bluetooth 1.1	

Bluetooth Evolution

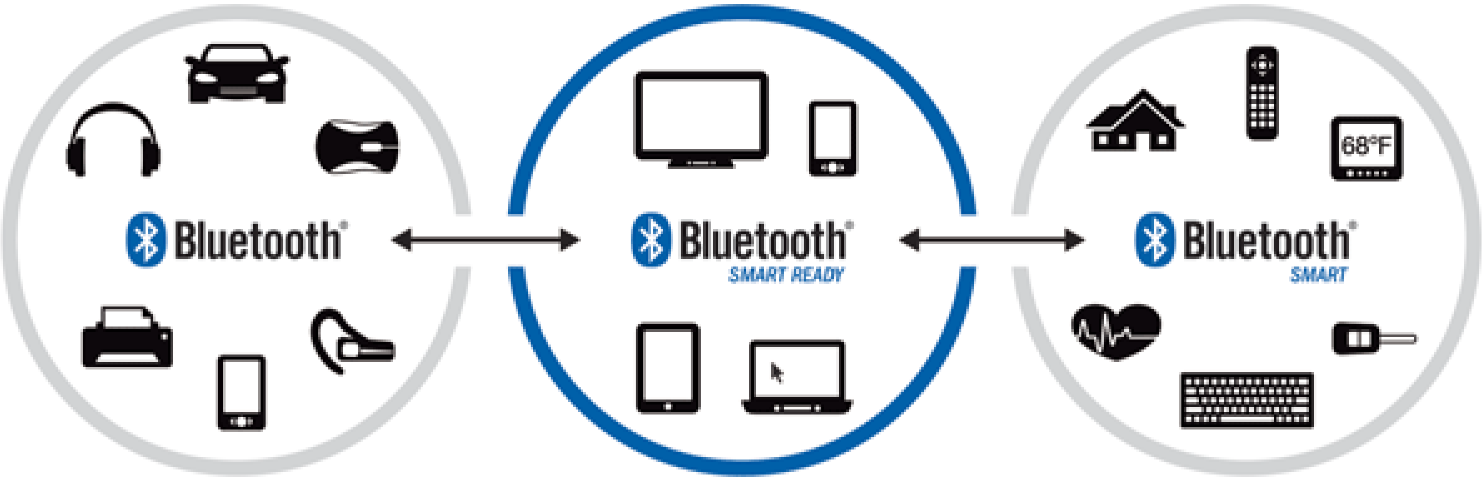


Bluetooth versions

Year Introduced	Bluetooth Version	Feature
2004	2.0	Enhanced Data Rate
2007	2.1	Secure Simple Pairing
2009	3.0	High Speed with 802.11 Wi-Fi Radio
2010	4.0	Low-energy protocol
2013	4.1	Indirect IoT device connection
2014	4.2	IPv6 protocol for direct internet connection
2016	5.0	4x range, 2x speed, 8x message capacity + IoT

CROSSLAB
Innovation for industry 4.0

Bluetooth versions & compatibility



Wireless devices streaming rich content like video and audio

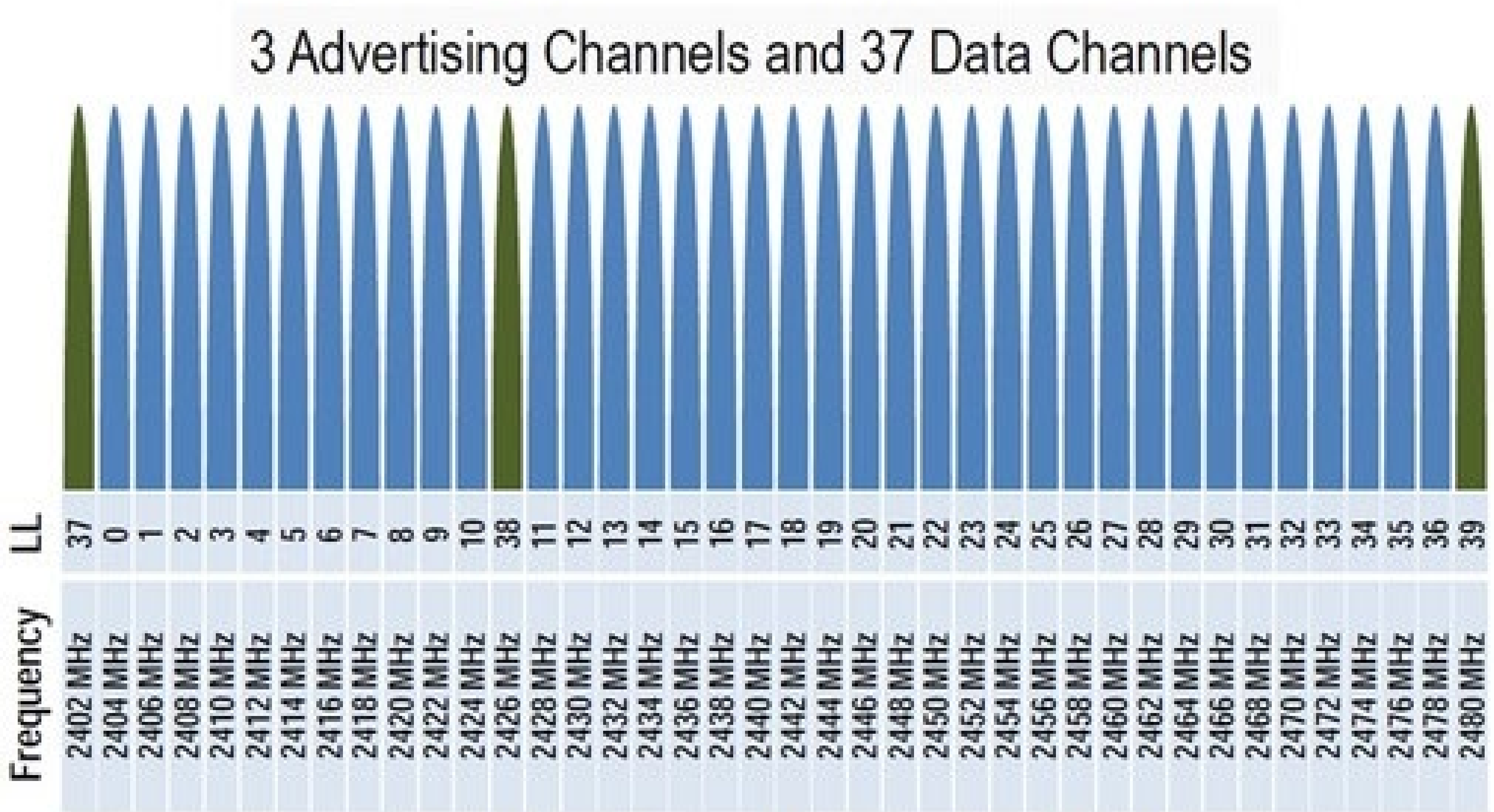
Devices that connect with both

Sensor devices sending small bits of data, using very little energy

BLE vs. Classic Bluetooth

	Bluetooth V2.1	Bluetooth Low Energy
Standardization Body	Bluetooth SIG	Bluetooth SIG
Range	~30 m (class 2)	~50 m
Frequency	2.4–2.5 GHz	2.4–2.5 GHz
Bit Rate	1–3 Mbit/s	~200 kbit/s
Set-Up Time	<6 s	<0.003 s
Voice Capable?	Yes	No
Max Output Power	+20 dBm	+10 dBm
Modulation Scheme	GFSK	GFSK
Modulation Index	0.35	0.5
Number of Channels	79	40
Channel Bandwidth	1 MHz	2 MHz

BLE Channels



Bluetooth Low Energy (BLE) Frequency Channels

BLE Communication Modes

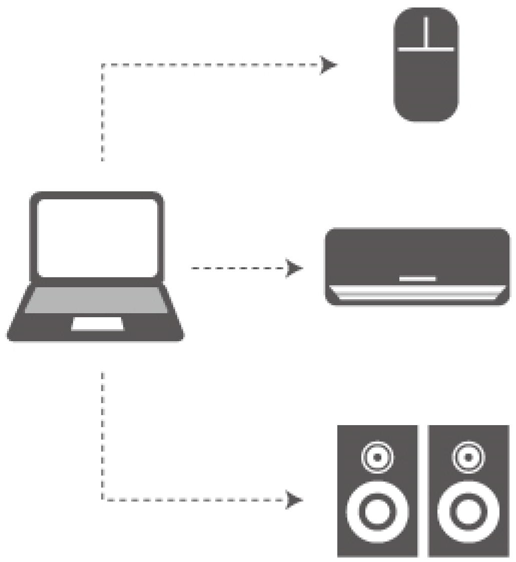
- Communication Mode
  - Device-to-device communication
  - Master-Slave approach
    - ⇨ Central (master)
    - ⇨ Peripheral (slave)
- Advertise Mode
  - Broadcast Communication
    - ⇨ Advertiser (Beacon)
    - ⇨ Observer

Bluetooth Topologies

- Hub and Spoke
  - Devices connects t a central hub
  - Communication is not possible if the central hub is out of coverage

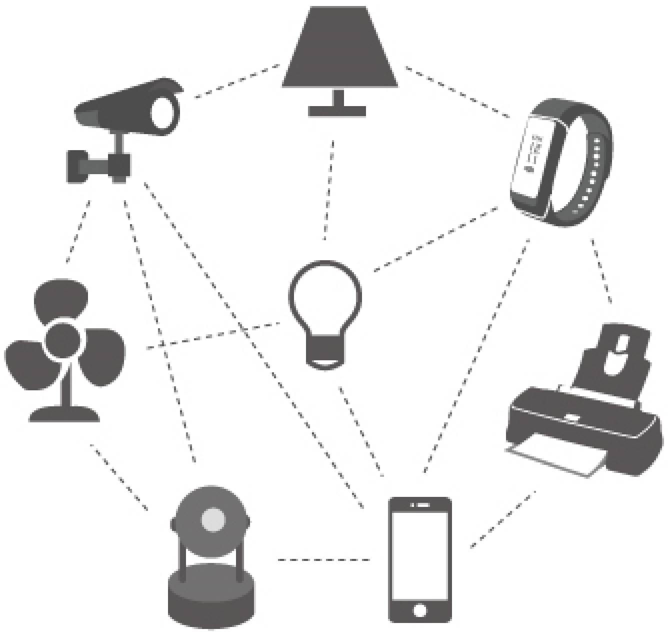
- Mesh Topology
  - Devices are connected directly without using the Internet to form a local network

Bluetooth Topologies



Hub-and-Spoke Topology

For the traditional Wi-Fi connection, all devices need to connect to a hub. Thus there is a limitation to the transmitting distance.



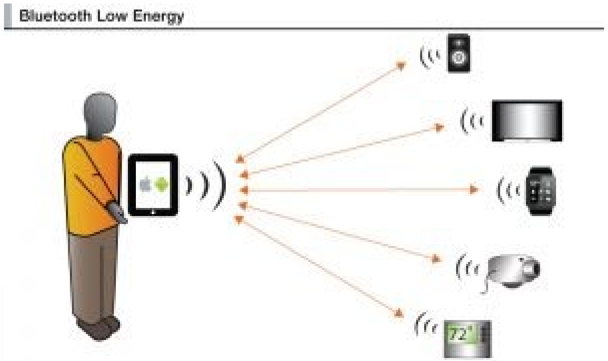
Mesh Network Topology

For the Bluetooth Mesh connection, the more devices connected on the same network, the further the transmitting distance.

How to connect to the Internet?

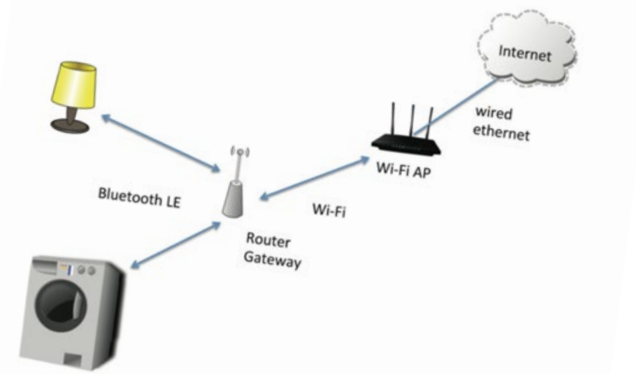
Bluetooth 4.0

- ➢Indirect Connection



Bluetooth 4.2

- ➢Application Gateway



- ➢Direct Connection

  Each device has an IPv6 address and connect directly

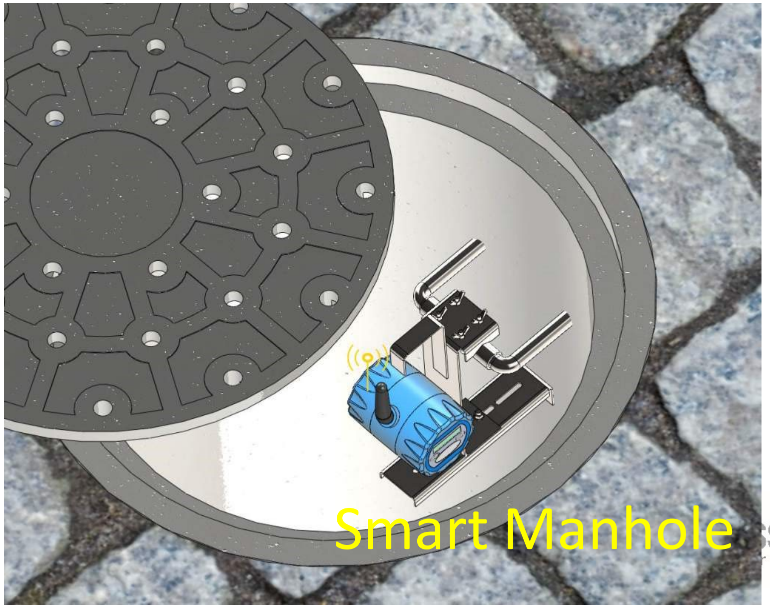
Other LLN Technologies

Limits of IEEE 802.15.4

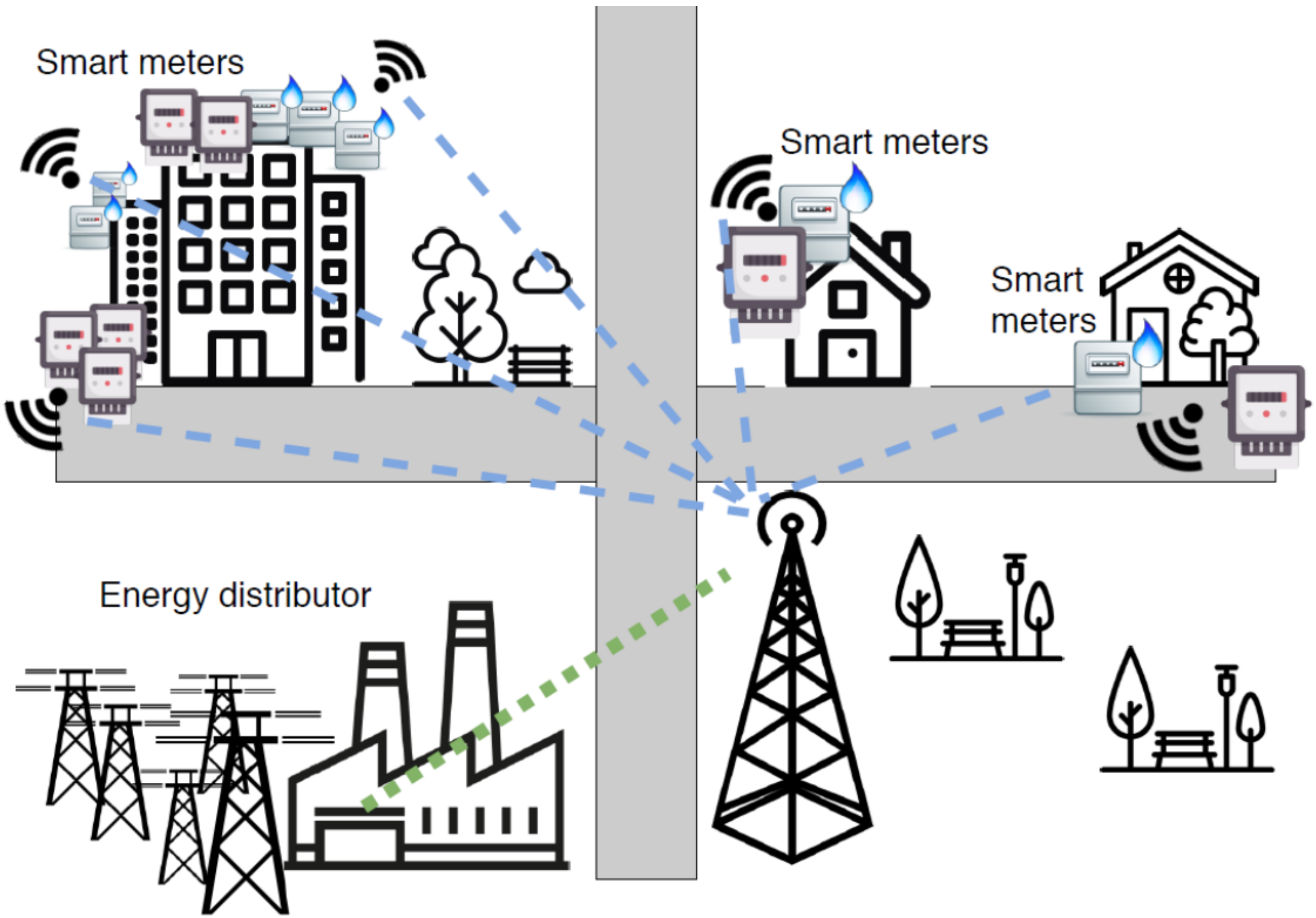
- Limited Communication Range
  - 100-200 m outdoors, 20-50 m indoors
  - Multi-hop communication for longer distances
    - ⇨ Lot of relay nodes to cover great distances increase the deployment cost
- Sensitivity to communication interferences
  - Due to wireless networks operating in the same range of frequencies (around 2.4 GHz)
    - ⇨ IEEE 802.11 (WiFi)
    - ⇨ IEEE 802.15.1 (Bluetooth)
    - ⇨ …
- Sensitivity to multi-path fading
  - several reflected signals taking different paths and arriving at the receiver at different times
  - e.g., due to obstacles

Sensory Data Collection

- Data are sent to a remote server (cloud)
- High power consumption
  - Due to the large distance
  - Solar panel or large battery required



Smart Utility Networks



Other LLN Technologies

- IEEE 802.15.4g
- Low-Power WiFi
- Low-Power Wide Area Networks
- Cellular communication (e.g., 5G)
- Power Line Communication
- Other wired technologies

Other LLN Technologies

- IEEE 802.15.4g
- Low-Power WiFi
- Low-Power Wide Area Networks
- Power Line Communication

IEEE 802.15.4g Standard

- Amendment to the IEEE 802.15.4 standard
  - Targeted to Wireless Smart Utility Networks
- Allows longer communication range
  - than IEEE 802.15.4
  - with similar emitted power
- Operates at sub GHz
  - Instead of 2.4 GHz

Enhancements introduced by IEEE 802.15.4g

- Sub-GHz Operations
  - longer distances with the same transmission power
  - less interference
    - ⇨ Compared to 2.4 GHz

- New Physical Layers (PHYs)
  - Frequency Shift Keying (**FSK**)
  - Offset Quadrature Phase-Shift Keying (**OQPSK**)
  - Orthogonal Frequency Division Multiplexing (**OFDM**)

IEEE 802.15.4g PHYs

- Frequency Shift Keying (FSK)
  - data rates in the range **5-400 Kbps**
    - ⇨ depending on the radio parameter setting
  - Forward Error Correction (FEC) to reduce the bit error rate
    - ⇨ reduces the # of re-transmissions
- Offset Quadrature Phase-Shift Keying (OQPSK)
  - shares some characteristics with the original IEEE802.15.4 standard
  - data rates in the range **6–500 Kbps**
- Orthogonal Frequency Division Multiplexing (OFDM)
  - data rates in the range **50–800 Kbps**
  - in challenging environments with multi-path fading

IEEE 802.15.4g Operating Modes

- Many Operating Modes for each PHY
  - Depending on the parameter setting
  - Up to 31 different modes
  - Data rates from **6.25 Kbps** to **800 Kbps**
- Default Mode
  - FSK at 50 Kbps
  - The default mode is mandatory
    - ⇨ must be implemented in any IEEE 802.15.4g compliant product
- Maximum frame size is always 2047 bytes

Question

Is 802.15.4g suitable to IoT applications requiring a long range

Experimental Results

Urban Scenario

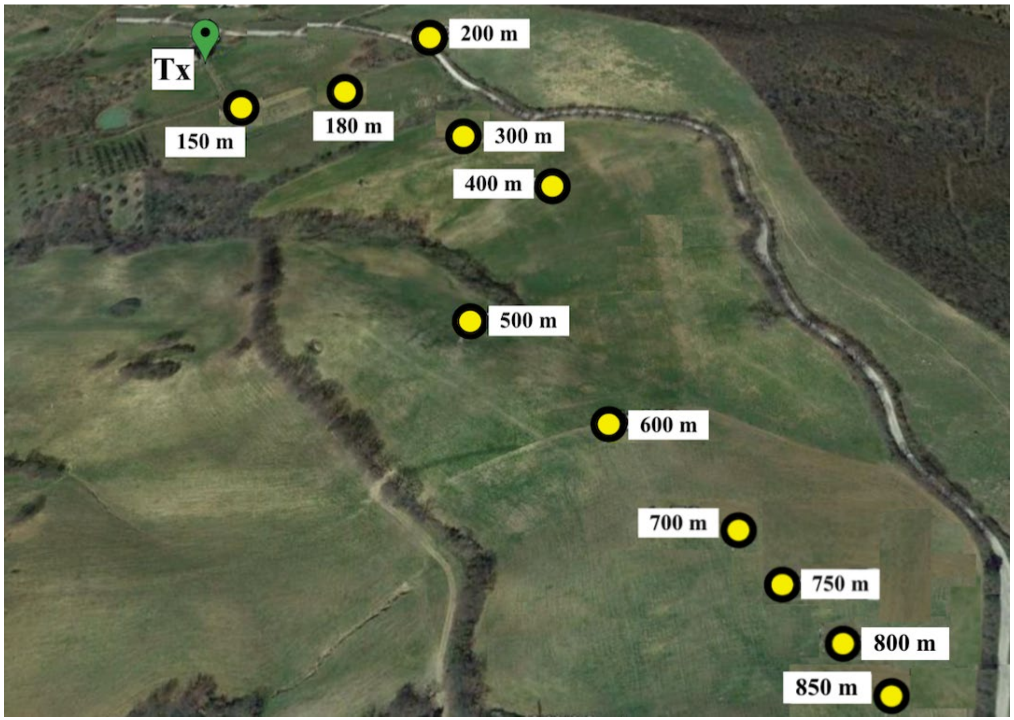
Path	Distance	PDR
1	100m	60%
	120m	90%
	150m	80%
	200m	0%
2	100m	30%
	150m	40%
	200m	0%
3	50m	90%
	100m	70%
	150m	30%
	200m	0%

F. Righetti, C. Vallati, D. Comola, G. Anastasi, **Performance Measurements of IEEE 802.15.4g Wireless Networks**, Proceedings of the *IEEE International Workshop on Internet of Things – Smart Objects and Services (IoT-SoS 2019)*, Washington DC, USA, June 10, 2019.

CROSSLAB Innovation for industry 4.0

Experimental Results

Rural Scenario



Distance	PDR
150m	100%
180m	90%
200m	100%
300m	100%
400m	80%
500m	30%
600m	60%
700m	65%
750m	90%
800m	30%
850m	0%

F. Righetti, C. Vallati, D. Comola, G. Anastasi, **Performance Measurements of IEEE 802.15.4g Wireless Networks**, Proceedings of the *IEEE International Workshop on Internet of Things – Smart Objects and Services (IoT-SoS 2019)*, Washington DC, USA, June 10, 2019.

CROSSLAB Innovation for industry 4.0

Experimental Results

Semi-rural Scenario

Distance	PDR
50m	100%
100m	75%
150m	70%
200m	40%
250m	60%
300m	0%

F. Righetti, C. Vallati, D. Comola, G. Anastasi, **Performance Measurements of IEEE 802.15.4g Wireless Networks**, Proceedings of the *IEEE International Workshop on Internet of Things – Smart Objects and Services (IoT-SoS 2019)*, Washington DC, USA, June 10, 2019.

IEEE 802.15.4g

- The communication range strongly depends on the external environment
  - Buildings, trees, and other objects that attenuate the signal strength
  - Obstacle that may prevent the signal propagation
- The communication range is lower than 1 km
  - Rural scenario: 800 m
  - Semi-rural scenario: 250 m
  - Urban scenario: 150 m
- May not be enough
  - Wireless Smart Utility Networks
  - Other IoT applications where a long communication range is required
- Multi-hop communication required in such cases

Other LLN Technologies

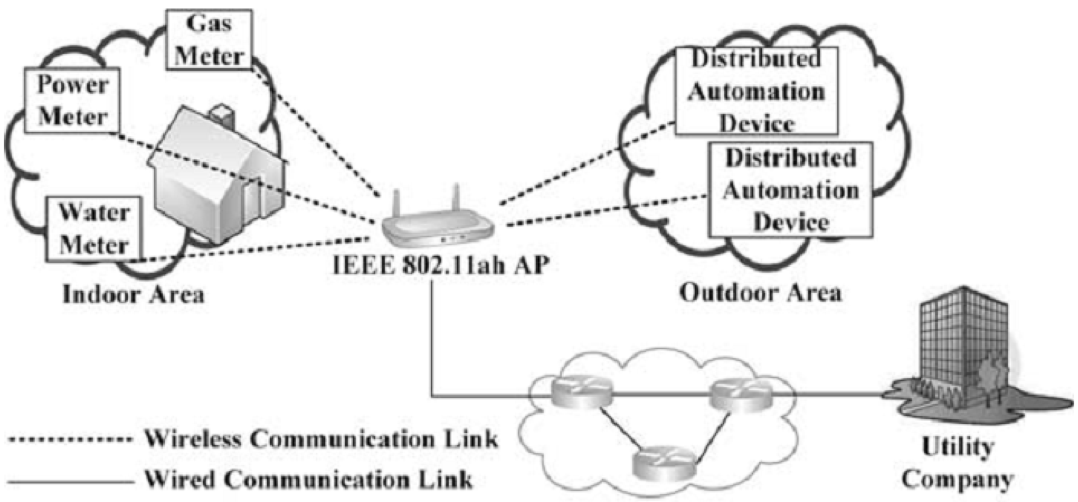
- IEEE 802.15.4g
- Low-Power WiFi
- Low-Power Wide Area Networks
- Power Line Communication

IEEE 802.11ah

- New amendment of the .11 family
  - based on IEEE 802.11ac (high thtroughput)
- Uses sub 1 GHz license-exempt bands
- Indoor and outdoor communications
  - over small or large areas
- Energy efficiency
- Increased aggregate throughput
- Scalability
  - support for large numbers of stations

802.11.ah Application Areas

- Smart meters
- Home/building automation
- Indoor healthcare/fitness systems
- Elderly care systems



- Smart grids
- Environmental monitoring
- Agricultural monitoring
- Automation of industrial processes

WiFi HaLow

- Wi-Fi HaLow extends Wi-Fi into the 900 MHz band
  - enabling the low power connectivity necessary for applications including sensors and wearables
- Wi-Fi HaLow's range is nearly twice that of today's Wi-Fi
  - Provides a robust connection in challenging environments where the ability to more easily penetrate walls or other barriers is an important consideration.
- Wi-Fi HaLow will broadly adopt Wi-Fi protocols
  - deliver many of the benefits that consumers have come to expect from Wi-Fi today
    - ⇨ including multi-vendor interoperability
    - ⇨ strong government-grade security
    - ⇨ easy setup

www.wi-fi.org/discover-wi-fi/wi-fi-halow

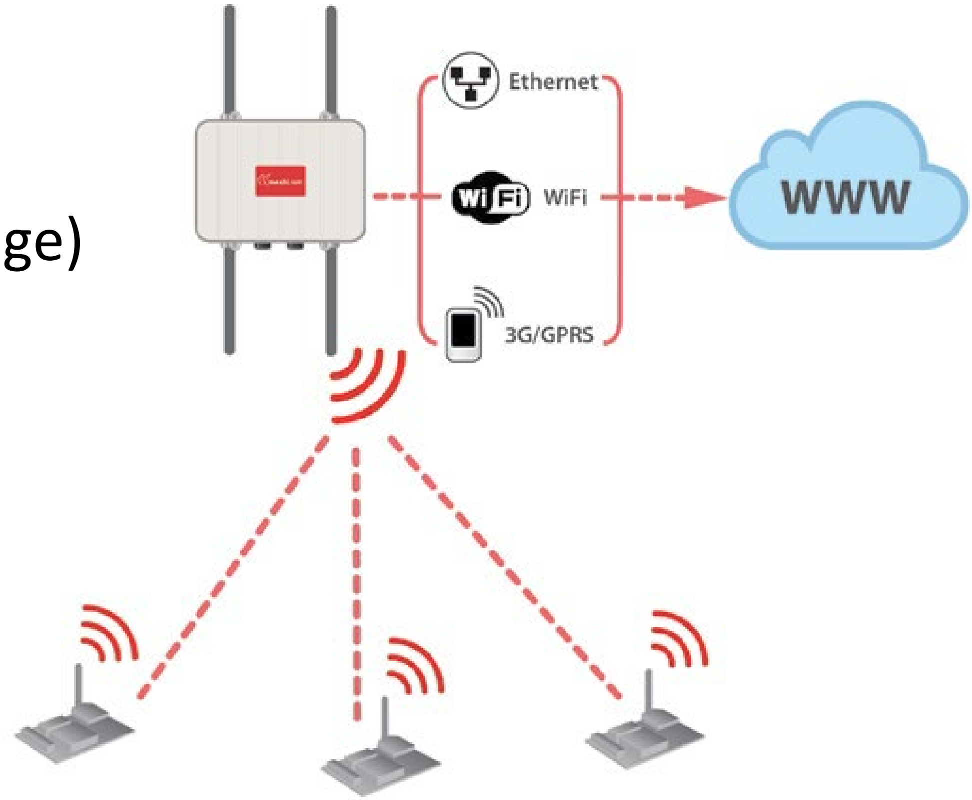
CROSSLAB Innovation for industry 4.0

Low-Power Wide-Area (LPWA)

- **LPWA networks**
  - communication technologies with very low power consumption, long range and very low costs
- **enable IoT services**
  - for which traditional mobile and short range networks cannot afford completely
    - ⇨ Smart Metering, Smart City, Asset Management and Tracking
  - Sigfox and LoRa (proprietary solutions)
    - ⇨ The gaining popularity of those proprietary solutions has forced standardization bodies to accelerate.

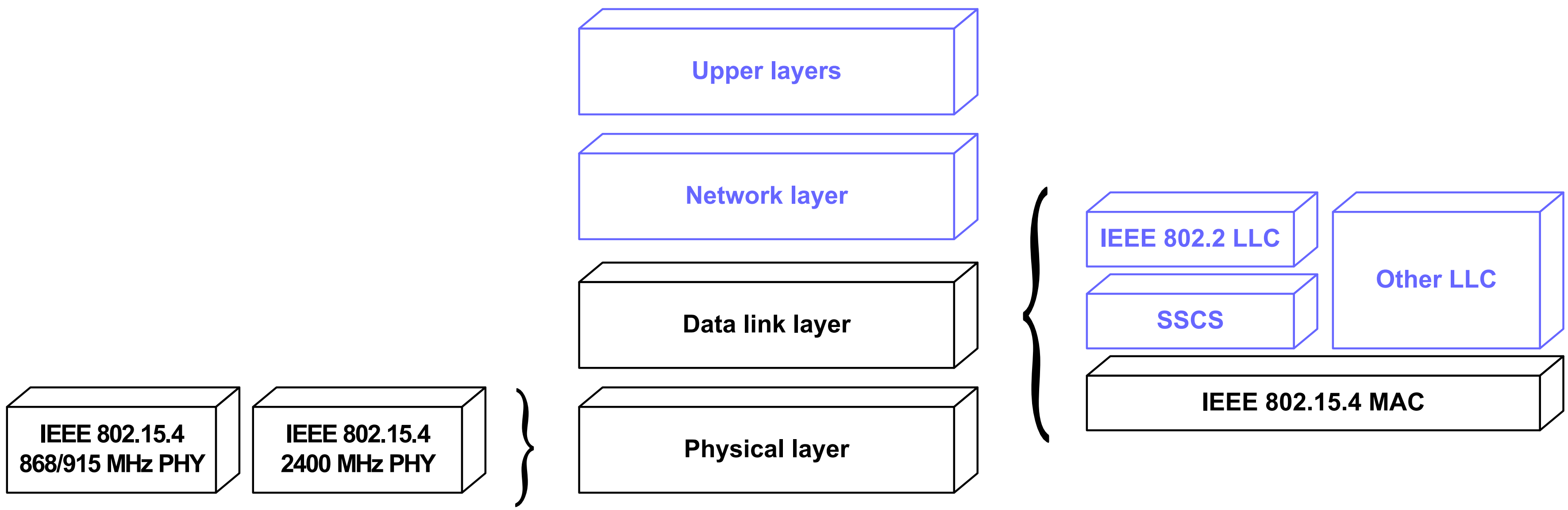
Infrastructure-based capillary networks

- Two-hop communication (through an intermediate gateway)
  - Device-gateway (short range)
    - ⇨ 802.15.4/ZigBee
    - ⇨ Bluetooth
    - ⇨ …
  - Gateway-Server (long-range)
    - ⇨ Ethernet
    - ⇨ GPRS/UMTS
    - ⇨ WiFi
    - ⇨ …



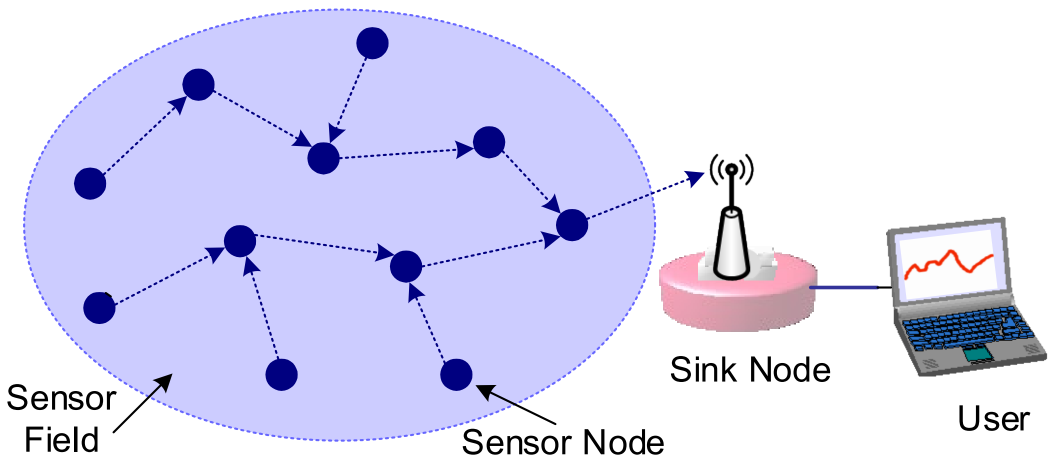
Summary

- IEEE 802.15.4 covers
  - Physical Layer
  - Data Link Layer



Key Question

How to do multi-hop communication?



Higher-layer protocols

- Routing
- Forwarding
- End-to-end transport protocol
  - ⇨ May not be required
- Application
- Cross-layer aspects
  - Security
  - Power Management

Two possible approach

- Non-IP Solution
- IP-based Solution
  - based on IPv6 and IoT protocols

Readings

- P. Baronti, P. Pillai, V. Chook, S. Chessa, A. Gotta, Y. Hu, **Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards,** *Computer Communications*, Vol. 30 (2007), pp. 1655–1695.
- Ed Callaway, Paul Gorday, Lance Hester, Jose A. Gutierrez, Marco Naeve, Bob Heile, **Home Networking with IEEE 802.15.4: Developing Standard for Low-Rate Wireless Personal Area Networks,** *IEEE Communications Magazine*, August 2002.
- G. Anastasi, M. Conti, M. Di Francesco, **A Comprehensive Analysis of the MAC Unreliability Problem in 802.15.4 Wireless Sensor Networks**, *IEEE Transactions on Industrial Informatics,* Vol.7, N.1, pp.52-65, February 2011.
- F. Righetti, C. Vallati, D. Comola, G. Anastasi, **Performance Measurements of IEEE 802.15.4g Wireless Networks**, Proceedings of the *IEEE International Workshop on Internet of Things – Smart Objects and Services (IoT-SoS 2019*), Washington DC, USA, June 10, 2019.

Questions