CSE 425: Internet of Things

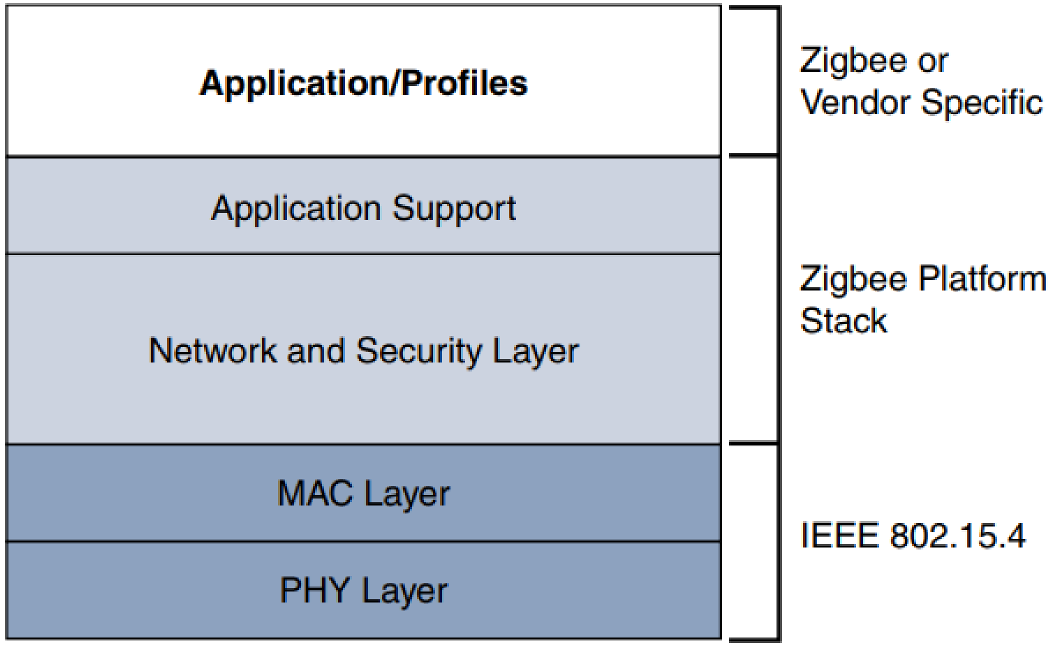
Dept. of CSE, BUBT| Summer 2021

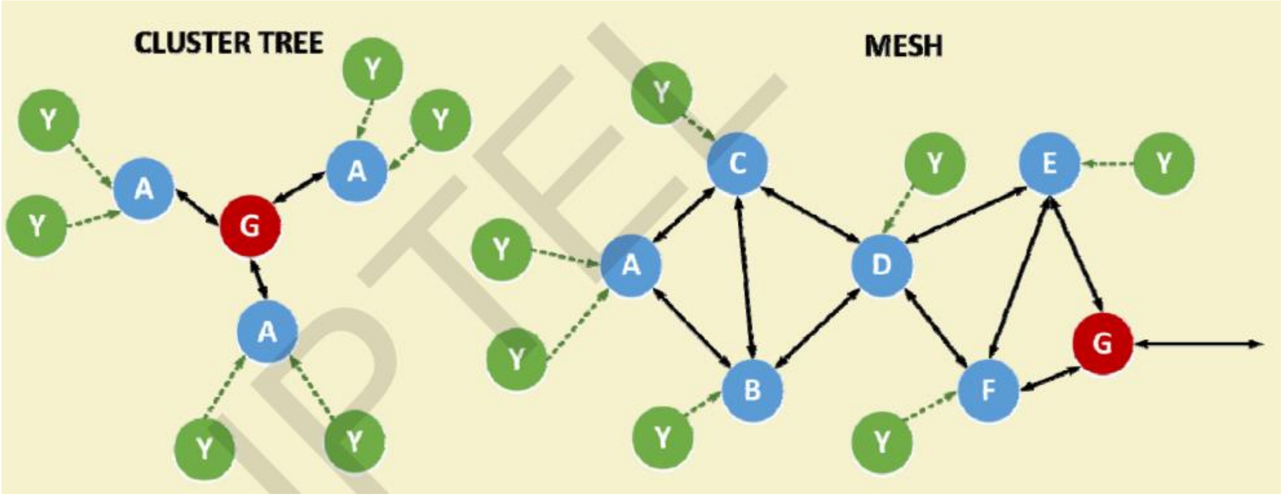
Md. Hasibur Rahman

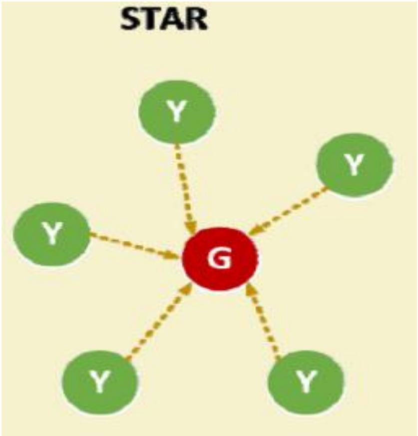
Connecting Smart Objects

Courtesy: David Hanes and Co.,Many Websites, IIT Kharagpur, and Google

ZigBee

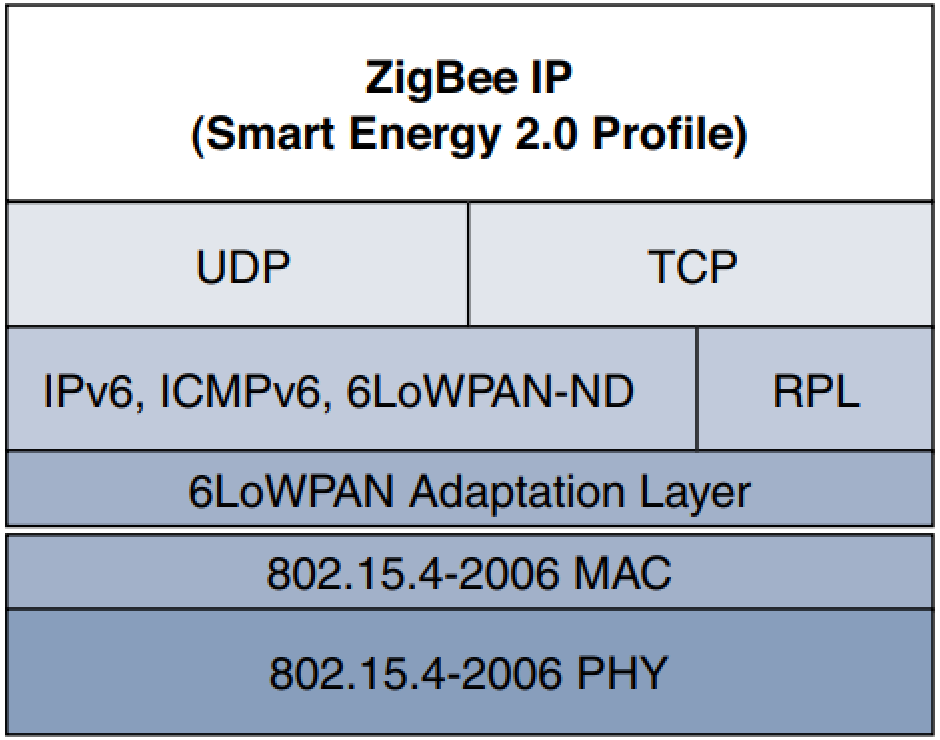






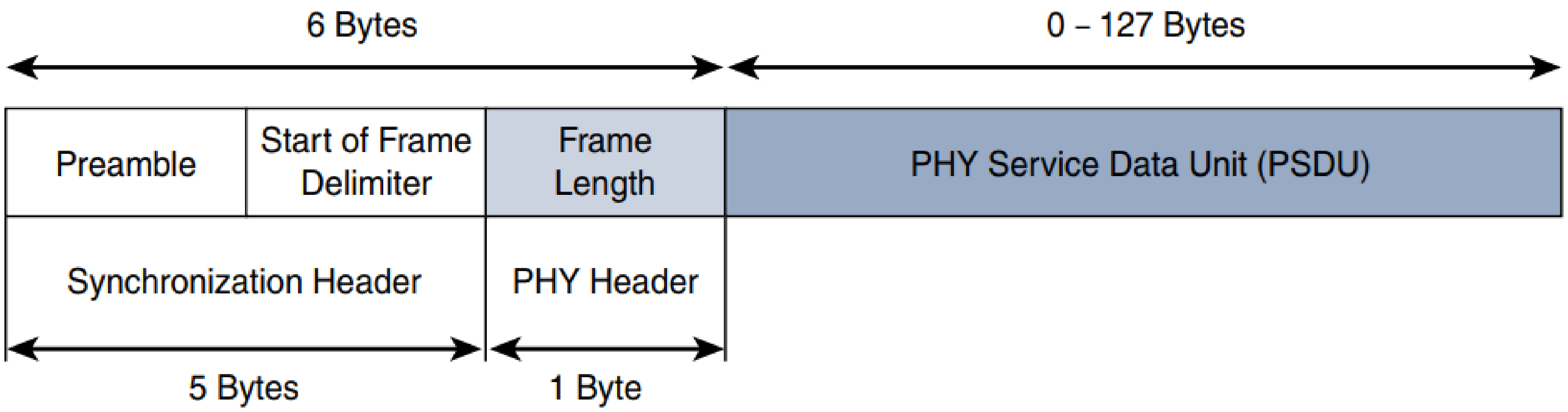
The network layer uses Ad Hoc On-Demand Distance Vector (AODV) routing.

ZigBee IP



Physical Layer:

- 2.4 GHz, 16 channels, with a data rate of 250 kbps
- 915 MHz, 10 channels, with a data rate of 40 kbps
- 868 MHz, 1 channel, with a data rate of 20 kbps
- OQPSK PHY
- BPSK PHY
- ASK PHY



ZigBee IP

MAC Layer

The IEEE 802.15.4 MAC layer manages access to the PHY channel by defining how devices in the same area will share the frequencies allocated. At this layer, the scheduling and routing of data frames are also coordinated. The 802.15.4 MAC layer performs the following tasks:

■ Network beaconing for devices acting as coordinators (New devices use beacons to join an 802.15.4 network)

■ PAN association and disassociation by a device

■ Device security

■ Reliable link communications between two peer MAC entities

The MAC layer achieves these tasks by using various predefined frame types. In fact, four types of MAC frames are specified in 802.15.4:

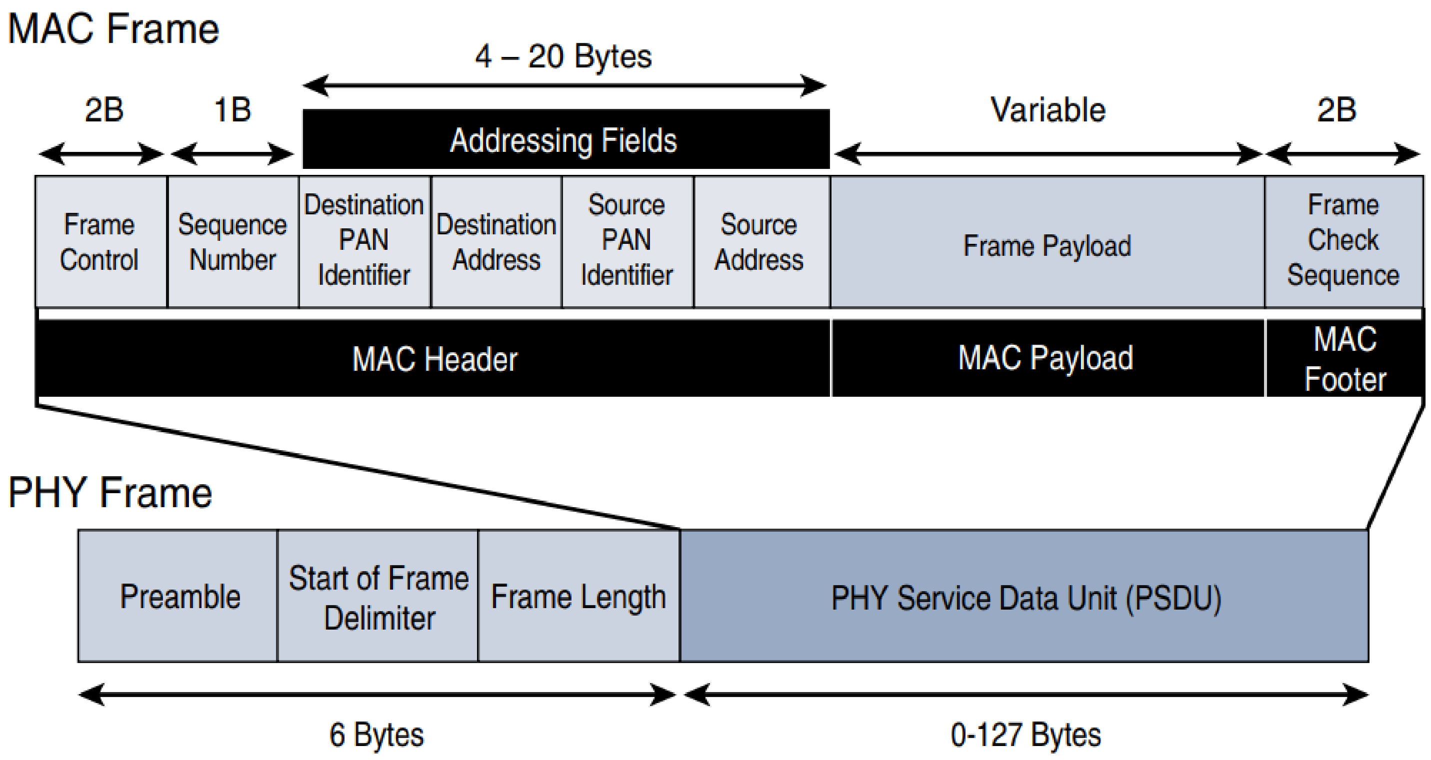
■ **Data frame:** Handles all transfers of data

■ **Beacon frame:** Used in the transmission of beacons from a PAN coordinator

■ **Acknowledgement frame:** Confirms the successful reception of a frame

■ **MAC command frame:** Responsible for control communication between devices

ZigBee IP



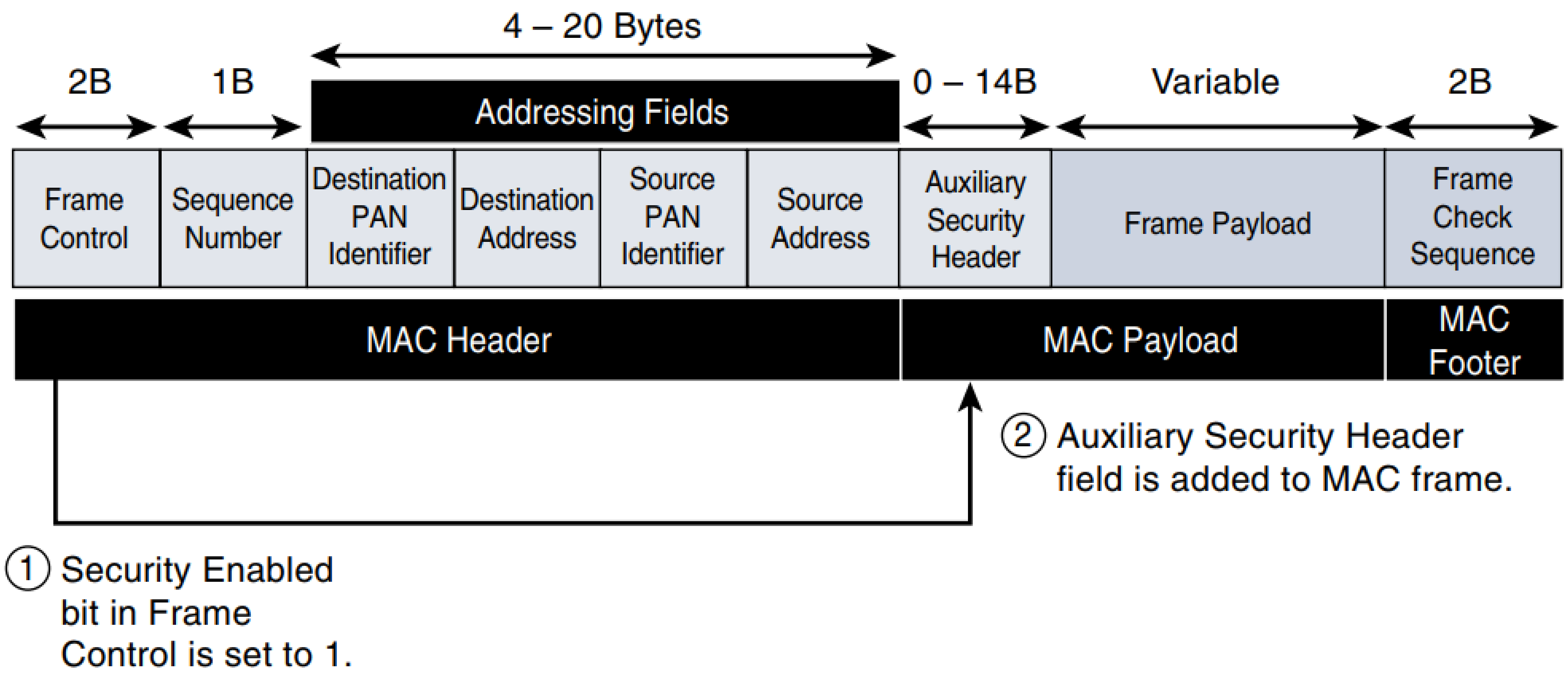
The MAC Header field is composed of the Frame Control, Sequence Number and the Addressing fields. The Frame Control field defines attributes such as frame type, addressing modes, and other control flags. The Sequence Number field indicates the sequence identifier for the frame. The Addressing field specifies the Source and Destination PAN Identifier fields as well as the Source and Destination Address fields.

Topology

Mesh Network Topology

ZigBee IP

Security



IEEE 802.15.4 Conclusions

The IEEE 802.15.4 wireless PHY and MAC layers are mature specifications that are the foundation for various industry standards and products. The PHY layer offers a maximum speed of up to 250 kbps, but this varies based on modulation and frequency. The MAC layer for 802.15.4 is robust and handles how data is transmitted and received over the PHY layer. Specifically, the MAC layer handles the association and disassociation of devices to/from a PAN, reliable communications between devices, security, and the formation of various topologies.

The topologies used in 802.15.4 include star, peer-to-peer, and cluster trees that allow for the formation of mesh networks. From a security perspective, 802.15.4 utilizes AES encryption to allow secure communications and also provide data integrity.

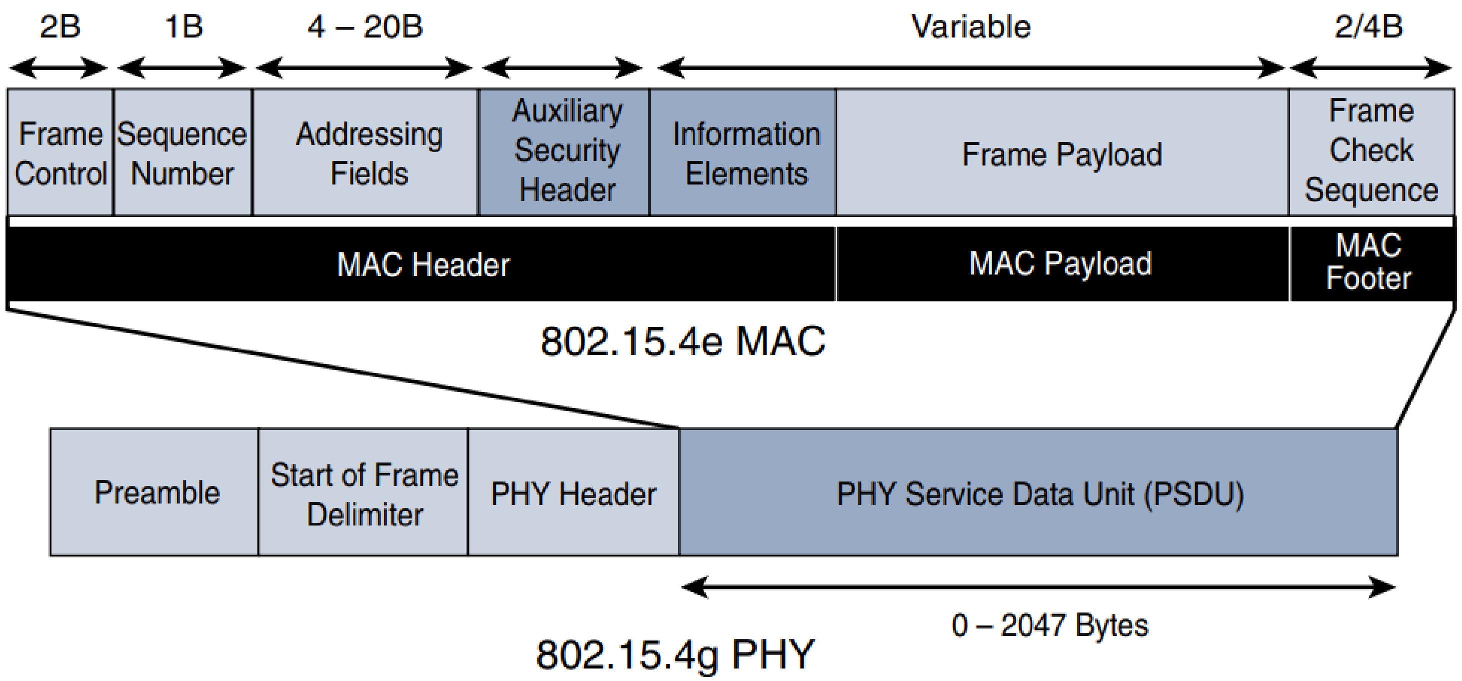
The main competitor to IEEE 802.15.4 is DASH7, another wireless technology that compares favorably. However, IEEE 802.15.4 has an edge in the marketplace through all the different vendors and organizations that utilize its PHY and MAC layers.

IEEE 802.15.4g and 802.15.4e

The IEEE 802.15.4e amendment of 802.15.4-2011 expands the MAC layer feature set to remedy the disadvantages associated with 802.15.4, including MAC reliability, unbounded latency, and multipath fading. In addition to making general enhancements to the MAC layer, IEEE 802.15.4e also made improvements to better cope with certain application domains, such as factory and process automation and smart grid.

Standardization and Alliances

Wi-SUN (SUN stands for *smart utility network*.)



IEEE 1901.2a

While most of the constrained network technologies relate to wireless, IEEE 1901.2a-2013 is a wired technology that is an update to the original IEEE 1901.2 specification. This is a standard for Narrowband Power Line Communication (NB-PLC). NB-PLC leverages a narrowband spectrum for low power, long range, and resistance to interference over the same wires that carry electric power. NB-PLC is often found in use cases such as the following:

Smart metering: NB-PLC can be used to automate the reading of utility meters, such as electric, gas, and water meters. This is true particularly in Europe, where PLC is the preferred technology for utilities deploying smart meter solutions.

Distribution automation: NB-PLC can be used for distribution automation, which involves monitoring and controlling all the devices in the power grid.

Public lighting: A common use for NB-PLC is with public lighting—the lights found in cities and along streets, highways, and public areas such as parks.

Electric vehicle charging stations: NB-PLC can be used for electric vehicle charging stations, where the batteries of electric vehicles can be recharged.

Microgrids: NB-PLC can be used for microgrids, local energy grids that can disconnect from the traditional grid and operate independently.

Renewable energy: NB-PLC can be used in renewable energy applications, such as solar, wind power, hydroelectric, and geothermal heat.

IEEE 802.11ah

In unconstrained networks, IEEE 802.11 Wi-Fi is certainly the most successfully deployed wireless technology. This standard is a key IoT wireless access technology, either for connecting endpoints such as fog computing nodes, high-data-rate sensors, and audio or video analytics devices or for deploying Wi-Fi backhaul infrastructures, such as outdoor Wi-Fi mesh in smart cities, oil and mining, or other environments. However, Wi-Fi lacks sub-GHz support for better signal penetration, low power for battery powered nodes, and the ability to support a large number of devices. For these reasons, the IEEE 802.11 working group launched a task group named IEEE 802.11ah to specify a sub-GHz version of Wi-Fi. Three main use cases are identified for IEEE 802.11ah:

Sensors and meters covering a smart grid: Meter to pole, environmental/agricultural monitoring, industrial process sensors, indoor healthcare system and fitness sensors, home and building automation sensors

Backhaul aggregation of industrial sensors and meter data: Potentially connecting IEEE 802.15.4g subnet works

Extended range Wi-Fi: For outdoor extended-range hotspot or cellular traffic offloading when distances already covered by IEEE 802.11a/b/g/n/ac are not good enough.

Named as WiFi Hallow.

IEEE 802.11ah

Physical Layer

IEEE 802.11ah essentially provides an additional 802.11 physical layer operating in unlicensed sub-GHz bands. For example, various countries and regions use the following bands for IEEE 802.11ah: 868–868.6 MHz for EMEAR, 902–928 MHz and associated subsets for North America and Asia-Pacific regions, and 314–316 MHz, 430–434 MHz, 470–510 MHz, and 779–787 MHz for China.

MAC Layer

■ **Number of devices:** Has been scaled up to 8192 per access point.

■ **MAC header:** Has been shortened to allow more efficient communication.

■ **Null data packet (NDP) support:** Is extended to cover several control and management frames. Relevant information is concentrated in the PHY header and the additional overhead associated with decoding the MAC header and data payload is avoided. This change makes the control frame exchanges efficient and less power consuming for the receiving stations.

■ **Grouping and sectorization:** Enables an AP to use sector antennas and also group stations (distributing a group ID). In combination with RAW and TWT, this mechanism reduces contention in large cells with many clients by restricting which group, in which sector, can contend during which time window. (Sectors are described in more detail in the following section.)

IEEE 802.11ah

■ **Grouping and sectorization:** Enables an AP to use sector antennas and also group stations (distributing a group ID). In combination with RAW and TWT, this mechanism reduces contention in large cells with many clients by restricting which group, in which sector, can contend during which time window. (Sectors are described in more detail in the following section.)

■ **Restricted access window (RAW):** Is a control algorithm that avoids simultaneous transmissions when many devices are present and provides fair access to the wireless network. By providing more efficient access to the medium, additional power savings for battery-powered devices can be achieved, and collisions are reduced.

■ **Target wake time (TWT):** Reduces energy consumption by permitting an access point to define times when a device can access the network. This allows devices to enter a low-power state until their TWT time arrives. It also reduces the probability of collisions in large cells with many clients.

■ **Speed frame exchange:** Enables an AP and endpoint to exchange frames during a reserved transmit opportunity (TXOP). This reduces contention on the medium, minimizes the number of frame exchanges to improve channel efficiency, and extends battery life by keeping awake times short.

IEEE 802.11ah

Topology

While IEEE 802.11ah is deployed as a star topology, it includes a simple hops relay operation to extend its range. This relay option is not capped, but the IEEE 802.11ah task group worked on the assumption of two hops. It allows one 802.11ah device to act as an intermediary and relay data to another. In some ways, this is similar to a mesh, and it is important to note that the clients and not the access point handle the relay function.

Security

No additional security has been identified for IEEE 802.11ah compared to other IEEE 802.11 specifications. (The other IEEE protocols are discussed earlier in this chapter.) These protocols include IEEE 802.15.4, IEEE 802.15.4e, and IEEE 1901.2a, and the security information for them is also applicable to IEEE 802.11ah.

6LoWPAN

NPTEL

Introduction

- ✓ Low-power Wireless Personal Area Networks over IPv6.
- ✓ Allows for the smallest devices with limited processing ability to transmit information wirelessly using an Internet protocol.
- ✓ Allows low-power devices to connect to the Internet.
- ✓ Created by the Internet Engineering Task Force (IETF) - RFC 5933 and RFC 4919.

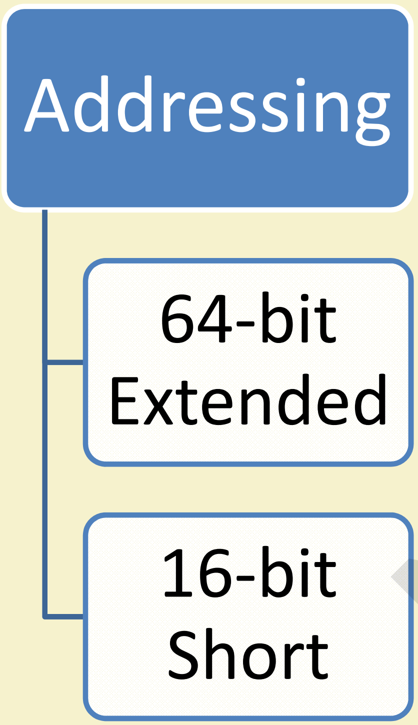
Source: T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik , JP. Vasseur, R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", IETF, Standards Track, Mar. 2012

Features of 6LoWPANs

- ✓ Allows IEEE 802.15.4 radios to carry 128-bit addresses of Internet Protocol version 6 (IPv6).
- ✓ Header compression and address translation techniques allow the IEEE 802.15.4 radios to access the Internet.
- ✓ IPv6 packets compressed and reformatted to fit the IEEE 802.15.4 packet format.
- ✓ Uses include IoT, Smart grid, and M2M applications.

NPTEL

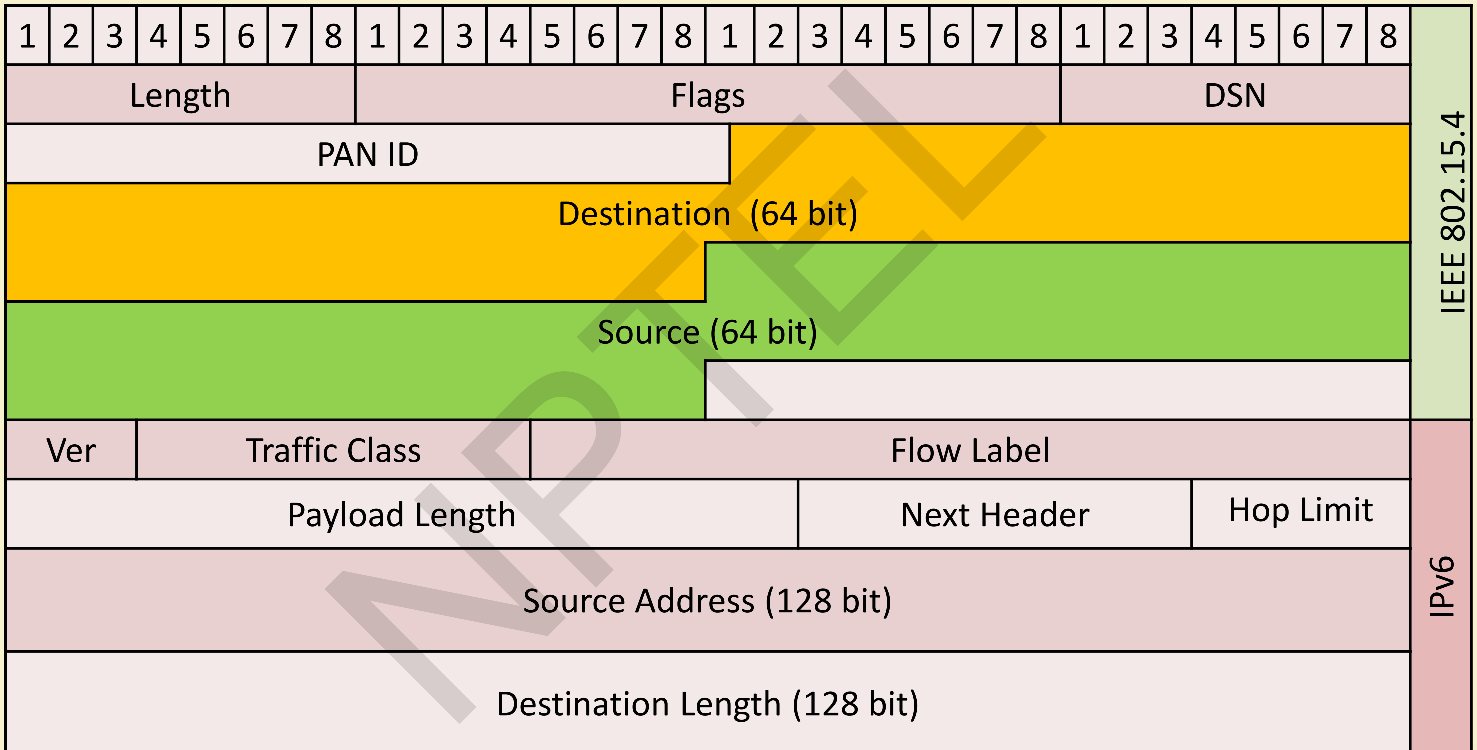
Addressing in 6LoWPAN



- <u>64-bit addresses</u>: globally unique
- <u>16 bit addresses</u>: PAN specific; assigned by PAN coordinator
- IPv6 multicast not supported by 802.15.4
- IPv6 packets carried as link layer broadcast frames

NPTEL

6LowPAN Packet Format



Header Type: Dispatch Header

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
0 1		Dispatch						Type Specific Header																							

- **Dispatch:** Initiates communication
- **0,1**: Identifier for Dispatch Type
- **Dispatch**:
  - 6 bits
  - Identifies the next header type
- **Type Specific Header:**
  - Determined by Dispatch header

NPTEL

Header Type: Mesh Addressing Header

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
1 0		V	F	Hops Left				Originator Address												Final Address											

- **1,0**: ID for Mesh Addressing Header
- **V**: ‘0’ if originator is 64-bit extended address, ‘1’ if 16-bit address
- **F**: ‘0’ if destination is 64-bit addr., ‘1’ if 16-bit addr.
- **Hops Left**: decremented by each node before sending to next hop

NPTEL

Header Type: Fragmentation Header

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
1 1 0 0				Datagram Size														Datagram Tag													

(a) First Fragment

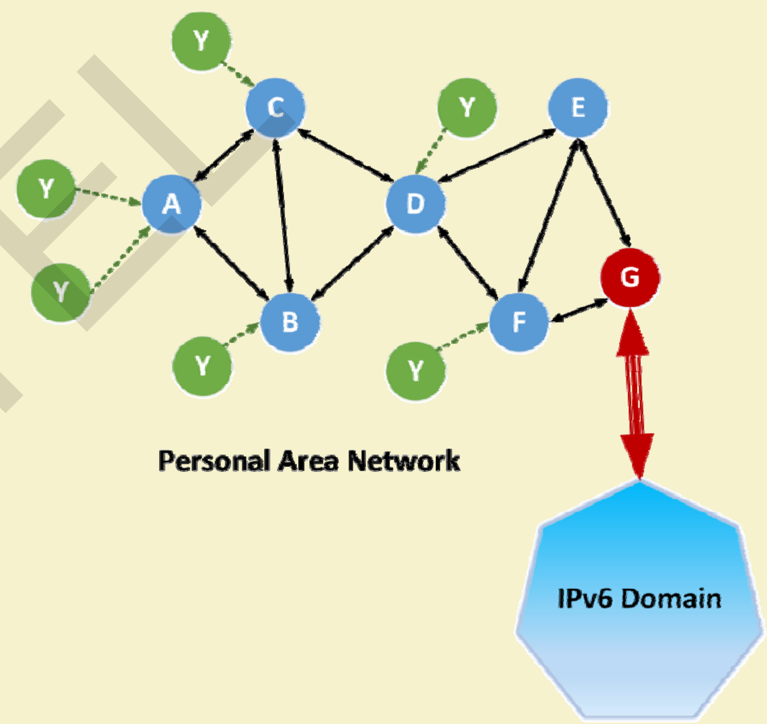
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
1 1 0 0				Datagram Size														Datagram Tag													
Datagram Offset																															

(b) Subsequent Fragment

NPTEL

6LoWPAN Routing Considerations

- ✓ Mesh routing within the PAN space.
- ✓ Routing between IPv6 and the PAN domain
- ✓ Routing protocols in use:
  - **LOADng**
  - **RPL**



NPTEL

LOADng Routing

- ✓ Derived from AODV and extended for use in IoT.
- ✓ Basic operations of LOADng include:
  - Generation of **Route Requests (RREQs)** by a LOADng Router (originator) for discovering a route to a destination,
  - **Forwarding of such RREQs** until they reach the destination LOADng Router,
  - Generation of **Route Replies (RREPs)** upon receipt of an RREQ by the indicated destination, and unicast hop-by-hop forwarding of these RREPs towards the originator.

Source: Clausen, T.; Colin de Verdiere, A.; Yi, J.; Niktash, A.; Igarashi, Y.; Satoh, H.; Herberg, U.; Lavenu, C. et al. (January 2016). *The Lightweight On-demand Ad hoc Distance-vector Routing Protocol - Next Generation (LOADng)*. IETF. I-D draft-clausen-lln-loadng-14

NPTEL

- If a route is detected to be broken, a **Route Error (RERR)** message is returned to the originator of that data packet to inform the originator about the route breakage.
- **Optimized flooding** is supported, reducing the overhead incurred by RREQ generation and flooding.
- Only the destination is permitted to respond to an RREQ.
- Intermediate LOADng Routers are explicitly prohibited from responding to RREQs, even if they may have active routes to the sought destination.
- RREQ/RREP messages generated by a given LOADng Router share a single unique, monotonically increasing sequence number.

Source: Clausen, T.; Colin de Verdiere, A.; Yi, J.; Niktash, A.; Igarashi, Y.; Satoh, H.; Herberg, U.; Lavenu, C. et al. (January 2016). *The Lightweight On-demand Ad hoc Distance-vector Routing Protocol - Next Generation (LOADng)*. IETF. I-D draft-clausen-lln-loadng-14

NPTEL

RPL Routing

- ✓ Distance Vector IPv6 **routing protocol for lossy and low power networks.**
- ✓ Maintains routing topology using low rate beaconing.
- ✓ Beaconing rate increases on detecting inconsistencies (e.g. node/link in a route is down).
- ✓ Routing information included in the datagram itself.
- ✓ **Proactive**: Maintaining routing topology.
- ✓ **Reactive**: Resolving routing inconsistencies.

Source: T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik , JP. Vasseur, R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", IETF, Standards Track, Mar. 2012

NPTEL

- RPL separates packet processing and forwarding from the routing optimization objective, which helps in Low power Lossy Networks (LLN).
- RPL supports message confidentiality and integrity.
- Supports Data-Path Validation and Loop Detection
- Routing optimization objectives include
  - minimizing energy
  - minimizing latency
  - satisfying constraints (w.r.t node power, bandwidth, etc.)

Source: T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik , JP. Vasseur, R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", IETF, Standards Track, Mar. 2012

- ✓ RPL operations require bidirectional links.
- ✓ In some LLN scenarios, those links may exhibit asymmetric properties.
- ✓ It is required that the reachability of a router be verified before the router can be used as a parent.

Source: T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik , JP. Vasseur, R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", IETF, Standards Track, Mar. 2012

NPTEL

RFID

NPTEL

Introduction

- ✓ RFID is an acronym for "radio-frequency identification"
- ✓ Data digitally encoded in RFID tags, which can be read by a reader.
- ✓ Somewhat similar to barcodes.
- ✓ Data read from tags are stored in a database by the reader.
- ✓ As compared to traditional barcodes and QR codes, RFID tag data can be read outside the line-of-sight.

Source: "How does RFID work?" AB&R (Online)

NPTEL

RFID Features

- ✓ RFID tag consists of an integrated circuit and an antenna.
- ✓ The tag is covered by a protective material which also acts as a shield against various environmental effects.
- ✓ Tags may be passive or active.
- ✓ Passive RFID tags are the most widely used.
- ✓ Passive tags have to be powered by a reader inductively before they can transmit information, whereas active tags have their own power supply.

Source: "How does RFID work?" AB&R (Online)

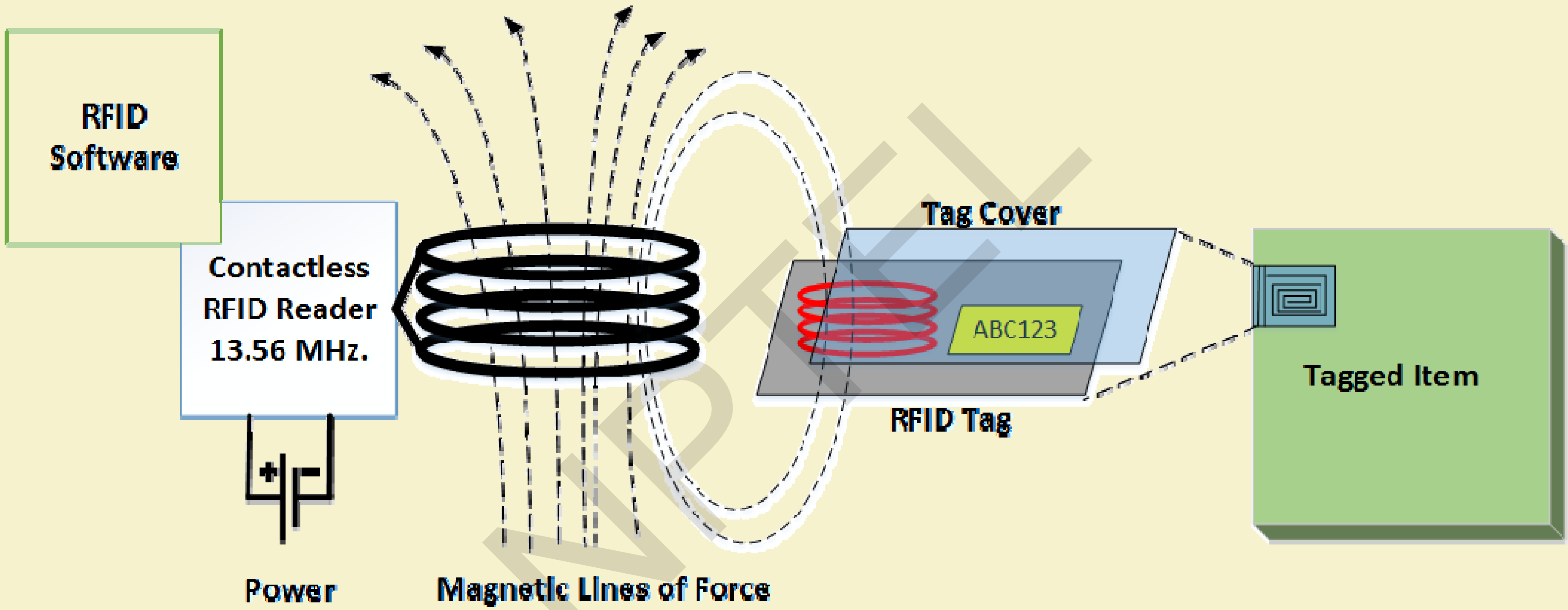
NPTEL

Working Principle

- ✓ Derived from Automatic Identification and Data Capture (AIDC) technology.
- ✓ AIDC performs object identification, object data collection and mapping of the collected data to computer systems with little or no human intervention.
- ✓ AIDC uses wired communication
- ✓ RFID uses radio waves to perform AIDC functions.
- ✓ The main components of an RFID system include an RFID tag or smart label, an RFID reader, and an antenna.

Source: "How does RFID work?" AB&R (Online)

NPTEL



RFID Software
Contactless RFID Reader 13.56 MHz.
Power
Magnetic Lines of Force
Tag Cover
ABC123
RFID Tag
Tagged Item

Applications

- ✓ Inventory management
- ✓ Asset tracking
- ✓ Personnel tracking
- ✓ Controlling access to restricted areas
- ✓ ID badging
- ✓ Supply chain management
- ✓ Counterfeit prevention (e.g. in the pharmaceutical industry)

Source: "How does RFID work?" AB&R (Online)

NPTEL

Thank You!!

NPTEL