Zigbee

Sachin Gajjar

sachin.gajjar@nirmauni.ac.in

Reading Material

Protocols and Architectures for Wireless Sensor Networks by Holger Karl

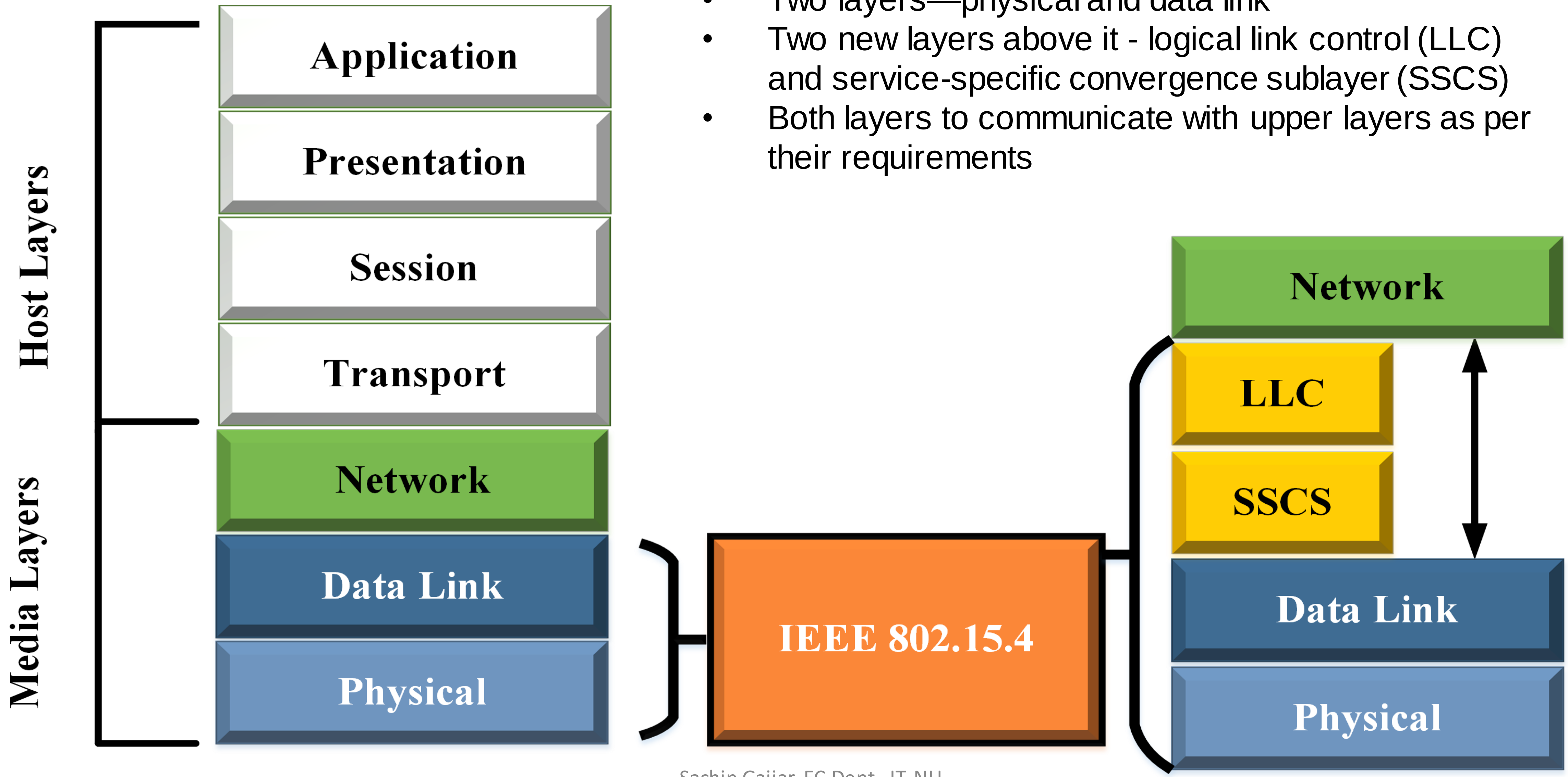
- Chapter 5
  - 5.5 The IEEE 802.15.4 MAC protocol

IEEE 802.15.4

- Standard for
  - low data rate (upto 250 kpbs),
  - low power consumption WPAN,
  - moderate delays without delay guarantees
- For monitoring and control applications in PAN
- Targeted applications are home automation, industrial automation, connecting devices in PAN

IEEE 802.15.4's protocol stack in comparison to OSI stack

- Two layers—physical and data link
- Two new layers above it - logical link control (LLC) and service-specific convergence sublayer (SSCS)
- Both layers to communicate with upper layers as per their requirements



IEEE 802.15.4 Physical Layer

- Operates in ISM (industrial, scientific, and medical) band
- No license required for usage of band
- Frequency Bands of Operation

	Channel	Center Frequency (MHz)	Availability
868 MHz Band	0	868.3	 *Europe*
915 MHz Band	1	906	 *Americas*
	2	908	
	3	910	
	4	912	
	5	914	
	6	916	
	7	918	
	8	920	
	9	922	
	10	924	
2.4 GHz Band	11	2405	 *World Wide*
	12	2410	
	13	2415	
	14	2420	
	15	2425	
	16	2430	
	17	2435	
	18	2440	
	19	2445	
	20	2450	
	21	2455	
	22	2460	
	23	2465	
	24	2470	
	25	2475	
	26	2480	

IEEE 802.15.4 Physical Layer

- Bitrates of 20 kbps (a single channel in frequency range 868–868.6 MHz), 40 kbps (ten channels in range between 905 and 928 MHz) and 250 kbps (16 channels in the 2.4 GHz band between 2.4 and 2.485 GHz with 5-MHz spacing between the center frequencies)
- To support MAC operation PHY layer includes features, as receiver energy detection (RED), link quality indicator (LQI), clear channel assessment (CCA)
- Direct Sequence Spread Spectrum (DSSS) modulation technique is used for communication purposes

IEEE 802.15.4 Physical Layer

- Utilizes infrequently occurring and very short packet transmissions with a low duty cycle (typically, < 1%) to minimize the power consumption.
- Minimum power level defined is -3dBm or 0.5mW for radios
- Transmission is Line of Sight (LOS), with range between 10 m to 75 m
- The best-case transmission range achieved outdoors can be up to 1000 m

IEEE 802.15.4 device
Full function device (FFD)

- Can communicate to all types of devices and supports full protocol stacks
- Network coordinator capability
- Equipped with adequate computational capability, memory
- Costly and energy-consuming due to increased requirements for support of full stacks
- Eg. Wireless Switch to operate Bulb

IEEE 802.15.4 device Reduced function device (RFD)

- Limited to being end device (sensor connected to it)
- Cannot become a network coordinator
- Communicates only to a network coordinator
- Limited computational capability, memory, limited power
- Eg. Bulb in the house operated with wireless switch

802.15.4 Device Definitions

- Coordinator
  - A Full Function Device (FFD)
  - Provides network coordination and related services
  - Coordinators can operate in a peer-to-peer fashion
  - Manages a list of associated network devices
  - Devices associate and disassociate with a coordinator using signalling packets.
  - All IEEE 802.15.4 nodes have a 64-bit device address

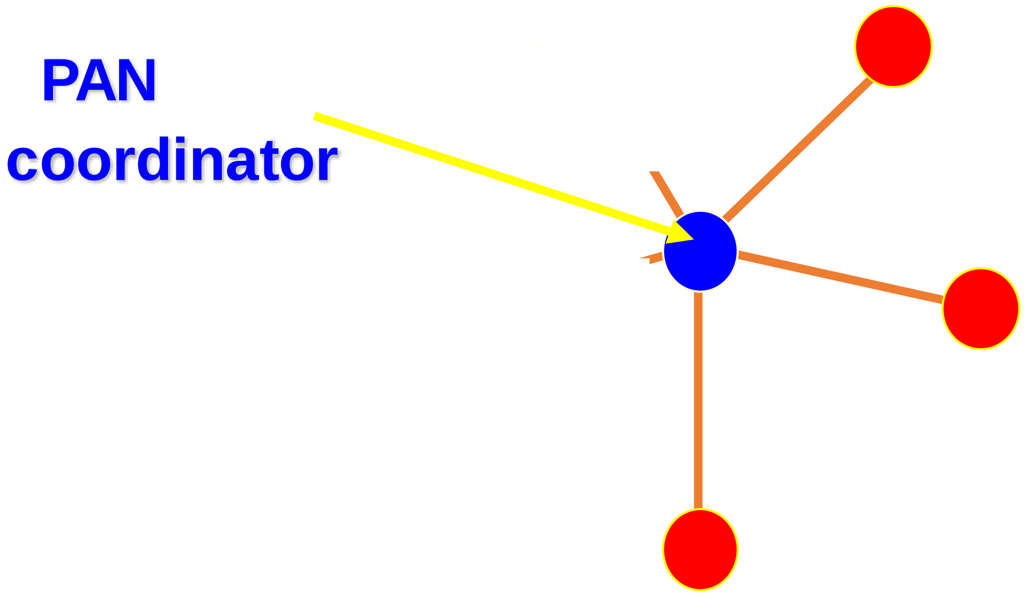
802.15.4 Device Definitions

- PAN Coordinator
  - Multiple coordinators can form a Personal Area Network (PAN)
  - PAN is identified by a 16-bit PAN Identifier
  - PAN has only one PAN coordinator, is controller of PAN
  - Exchanging data frames with network devices and a peer coordinator
  - Generating beacon frames on a periodic basis

IEEE 802.15.4 Topologies
Star Topology

- Supports a single coordinator, with up to 65,536 (2^{16}) devices.
- 1 FFD assumes role of PAN coordinator
- Other devices act as end devices
- Coordinator does initiating of the network
- End devices (RFD) can only communicate with the coordinator.

Star Topology



- Advantage
  - Easy implementation
- Disadvantage
  - Less scalable geographically

Full Function Device (FFD)

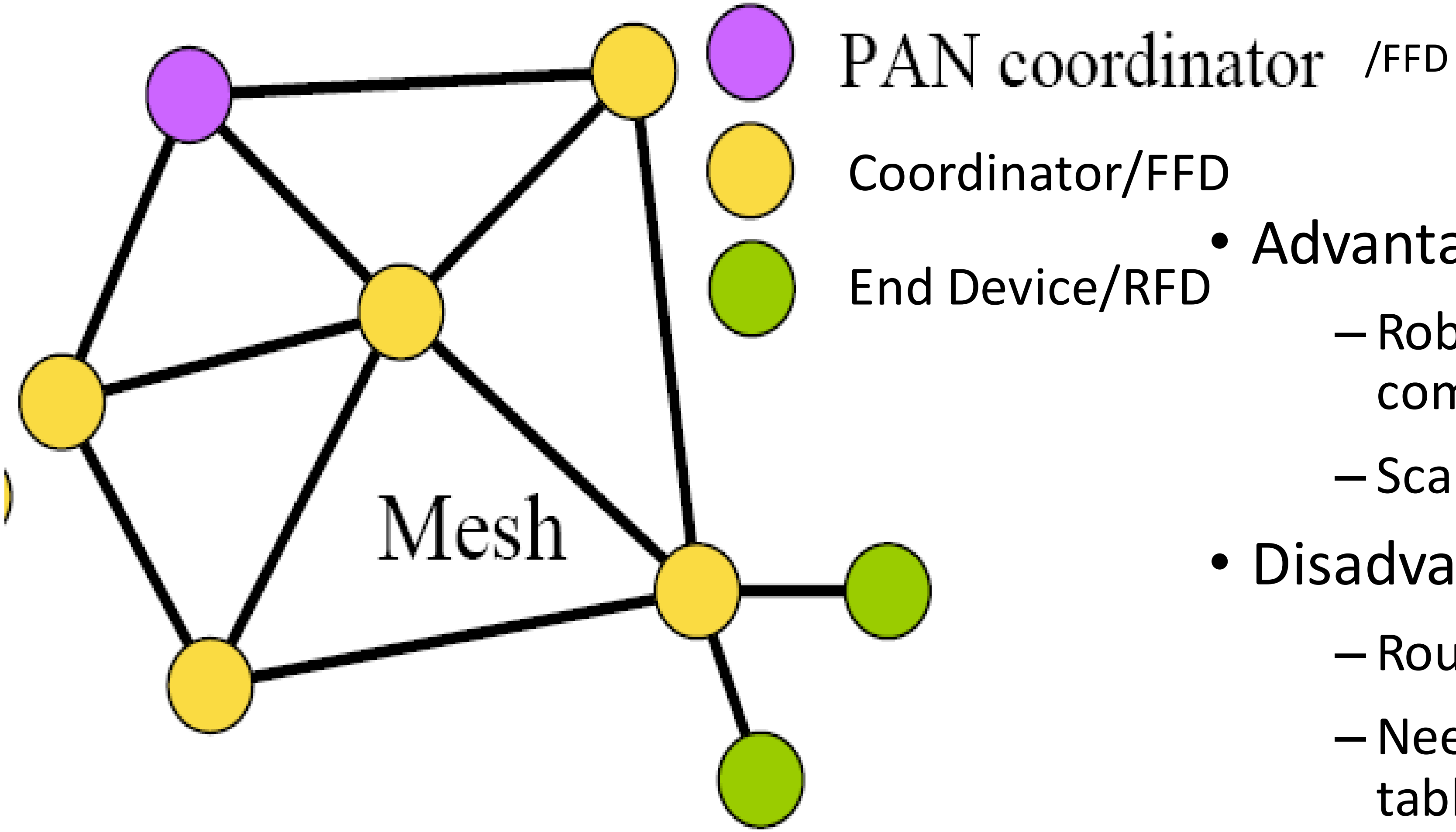
Reduced Function Device (RFD)/End Device with sensor

Communications Flow

IEEE 802.15.4 Topologies Mesh Topology

- Allows path formation from any source device to any destination device
- Using routing algorithms like simplified version of the Adhoc on-demand distance vector routing
- Radio receivers of the coordinator, PAN coordinator must always be on- Why?

IEEE 802.15.4 Topologies
Mesh Topology

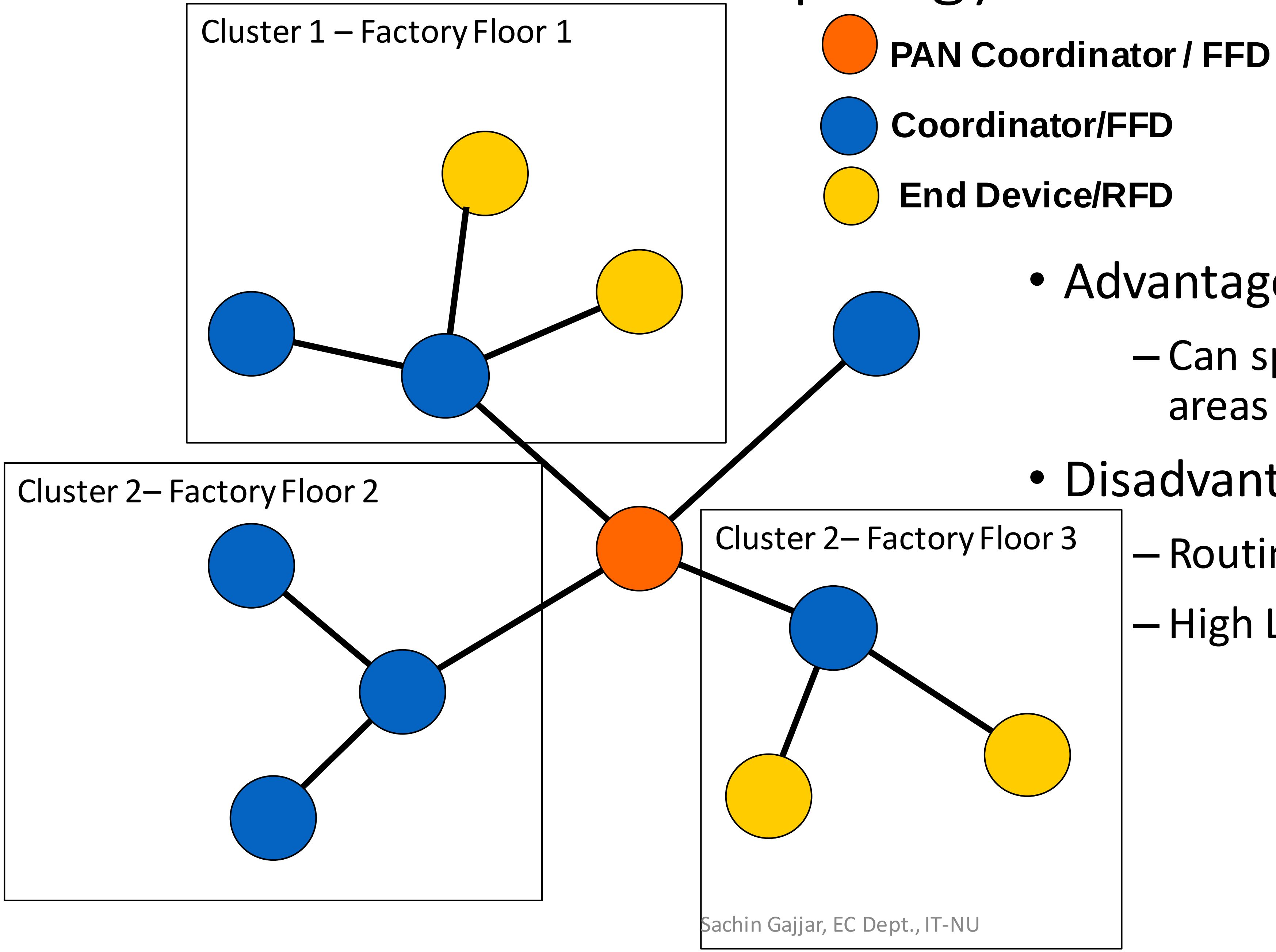


- Advantage
  - Robust multi-hop communication
  - Scalable
- Disadvantage
  - Routing is costly
  - Needs storage for routing table

IEEE 802.15.4 Topologies Cluster tree networks

- Any FFD can be a PAN coordinator.
- One coordinator is selected for the PAN
- It forms the first cluster and assigns it a cluster identity (CID) of value zero
- Subsequent clusters are then formed with a designated cluster head for each cluster.
- Each PAN is uniquely identified by a 16-bit identifier.
- Cluster comprises up to 255 clusters of up to 254 nodes each, for a total of 64,770 nodes
- Clustering
  - geographically adjacent nodes form clusters
  - reduces information transfers, offers scalability

Cluster-Tree Topology



- Advantage
  - Can span large physical areas
- Disadvantage
  - Routing is costly
  - High Latency

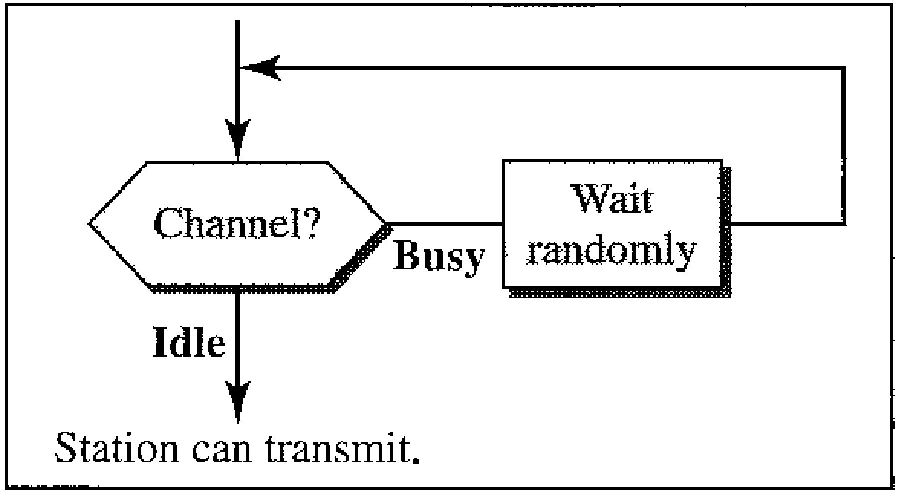
MAC Traffic Types

- Periodic Data
  - Sensor data transmission at regular intervals
  - Eg. Temperature Map generating network
- Intermittent Data
  - Application/External stimulus defined sensor data
  - Eg. A wireless light switch controlling a lamp, the lamp, typically mains powered, can monitor the channel in a continuous manner. Switch remains idle until it is toggled, in which case it transmits the information to the lamp
- Repetitive low-latency data
  - Repetitive in nature and requires minimum latency for its transfer
  - For critical applications such as security monitoring systems
  - Requires guaranteed access to channel within its latency tolerance
  - Eg. Video based intrusion detection systems

IEEE 802.15.4 MAC Layer

- Medium Access Control
- Carrier Sense Multiple Access (CSMA) with Collision Avoidance (CA)
  - Slotted CSMA/CA (Beacon enabled mode)
    - Periodic data and Repetitive low latency data
  - Un-slotted CSMA/CA (Non-Beacon enabled mode)
    - Intermittent data (Stimulus data)

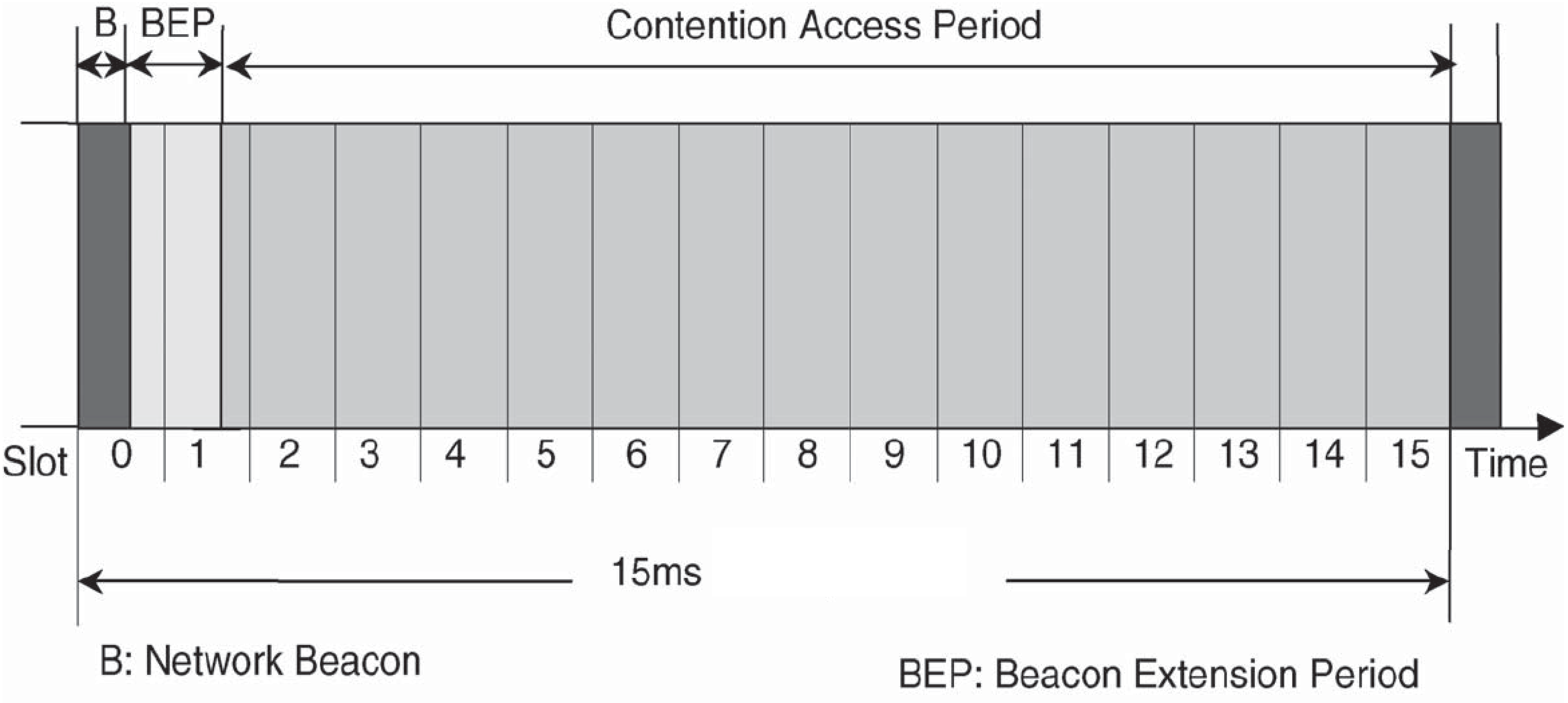
CSMA



MAC Superframe Structure for network transmission and reception

- Superframe is formed by PAN coordinator
- Bounded by network beacons
- Divided into 16 equally sized time slots.
- 1^{st} time slot of each superframe is used to transmit the beacon
- Beacon synchronizes attached devices, identifies the PAN, describes superframe structure
- BEP used to transmit pending node messages to be delivered by coordinator
- Remaining time slots are used by competing devices for communications during the contention access period (CAP)
- Devices use slotted CSMA-CA-based protocol to compete for the time slots

MAC Superframe structure

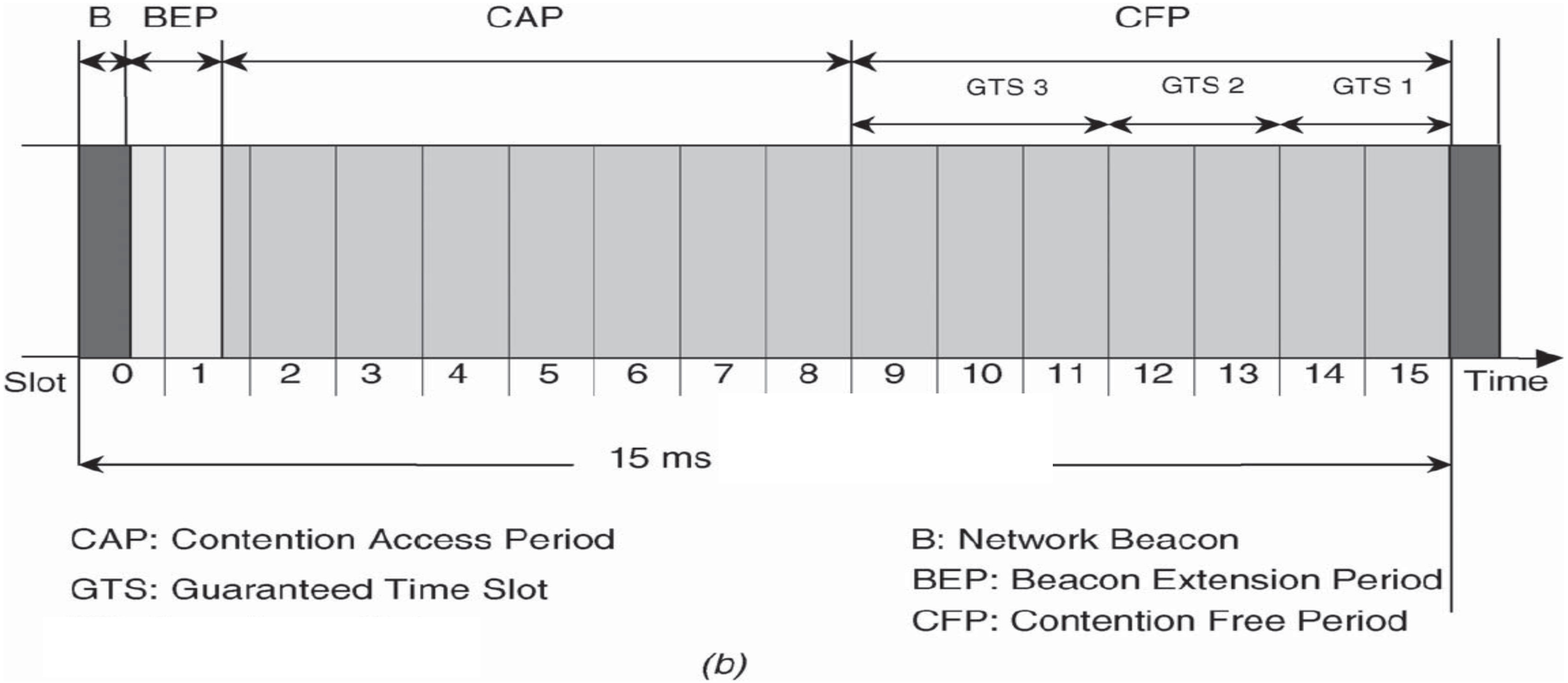


(a)

GTS (Guaranteed Time Slot) Concepts

- To satisfy the low latency and bandwidth requirements of applications
- Devices requiring low latency or specific data rate issue request to the PAN coordinator for GTS allocation during CFP
- PAN coordinator may dedicate groups of contiguous time slots labeled as guaranteed time slots (GTSs)
- The number of GTSs cannot exceed seven
- A single GTS allocation, may occupy more then one time slot.
- Together the GTSs form the contention free period (CFP)
- All GTS-based transactions finish within their allocated time slots and before end of CFP
- CFP starts at a slot boundary immediately following the CAP
- For repetitive low latency data

MAC Superframe structure with CAP and CFP

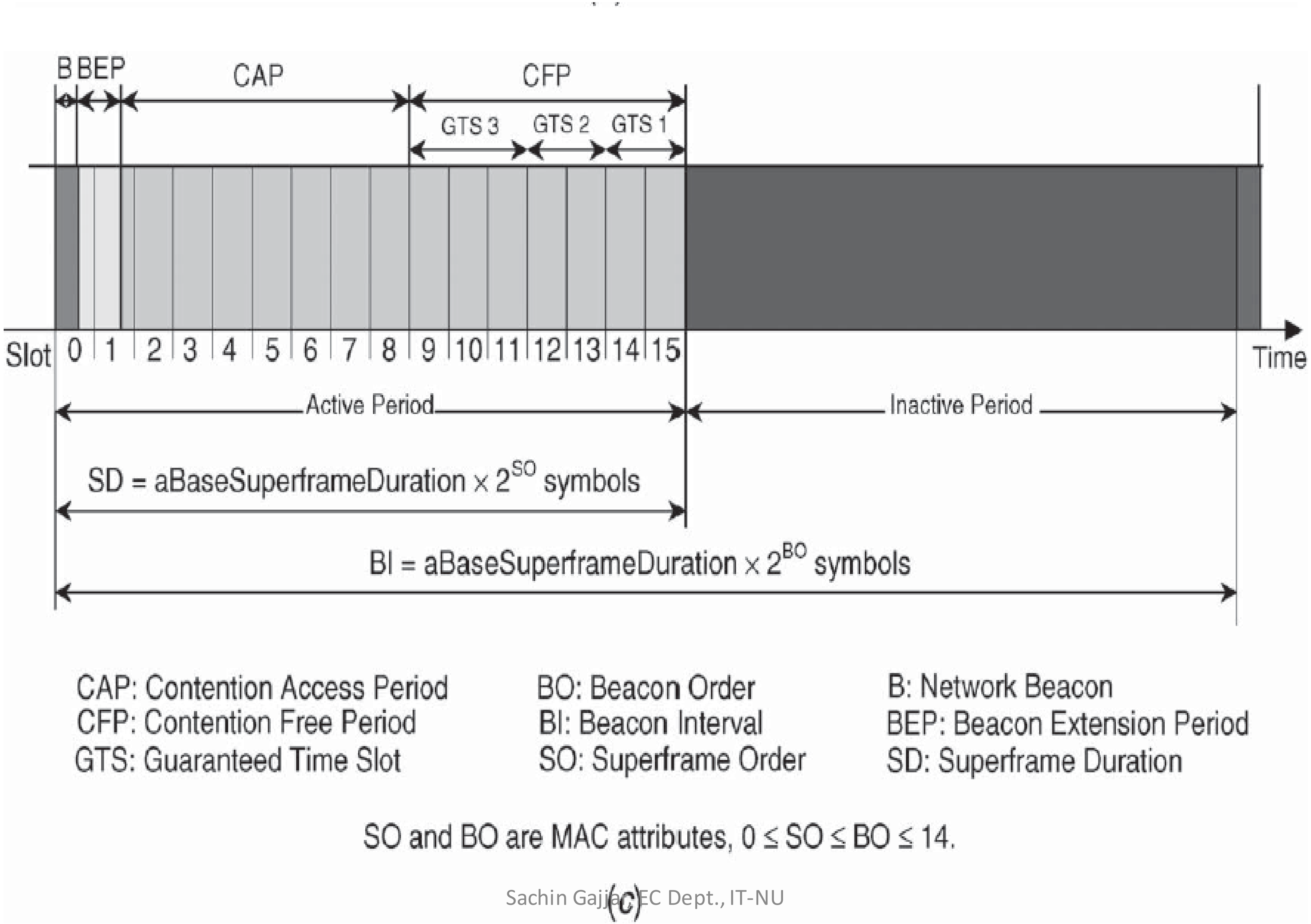


Network beacon	Transmitted by PAN coordinator. Beacon synchronizes attached devices, identifies the PAN, describes superframe structure
Beacon extension period	Space reserved for beacon growth due to pending node messages to be delivered by coordinator
Contention period	Access by any node using CSMA-CA
Guaranteed Time Slot	Reserved for nodes requiring guaranteed bandwidth, it can be zero

MAC Superframe structure with inactive period

- Coordinator may issue a superframe containing both an active period and an inactive period
- Active period = 16 time slots, contains frame beacon, CAP time slots, and if applicable, the CFP slots.
- Inactive period - a time period during which all network nodes and coordinator, can go to sleep mode for energy saving
- In inactive network devices switch off their power and set timer to wake up just before announcement of beacon frame

MAC Superframe structure with CAP, CFP and inactive period



MAC Superframe structure with CAP, CFP and inactive period

- Length of the active/inactive periods, time slot duration, number/usage of GTS slots are configurable network parameters
- To accommodate A wide range of application requirements and network deployment
- Length of the inactive period varies and may be set to zero

Un-slotted CSMA/CA (Non-Beacon enable mode)

- Absence of a synchronization mechanism, such as the beacon
- For applications where remote units like intrusion sensors/motion detectors wake up random basis to report on events as they occur.
- Network coordinator, mains powered, is continuously awake waiting to hear from each of these units.
- Does not support GTS
- Devices compete for channel access using an unslotted, CSMA/CA protocol

IEEE 802.15.4 MAC Layer frames

- Frame Types
  - Data Frame
    - used for all transfers of data
  - Beacon Frame
    - used by a coordinator to transmit beacons
  - Acknowledgment Frame
    - used for confirming successful frame reception
  - MAC Command Frame
    - used for handling all MAC peer entity control transfers

IEEE 802.15.4 Variants

- There are seven variants identified with in IEEE 802.15.4—A, B, C, D, E, F, and G.
- Variants A/B are the base versions, C is assigned for China, and D for Japan
- Variants E, F, and G are assigned respectively for industrial applications, and smart utility systems

What is ZigBee Alliance?

- An alliance with a mission to define reliable, cost effective, low-power, wirelessly networked, monitoring and control products based on an open global standard
- https://zigbeealliance.org/about/
- Certify products to help ensure interoperability through Certified program
- Zigbee Alliance is now the Connectivity Standards Alliance
- https://csa-iot.org/

ZigBee™ Alliance
Wireless Control That Simply Works

csa connectivity standards alliance

ZigBee Alliance

and many more....

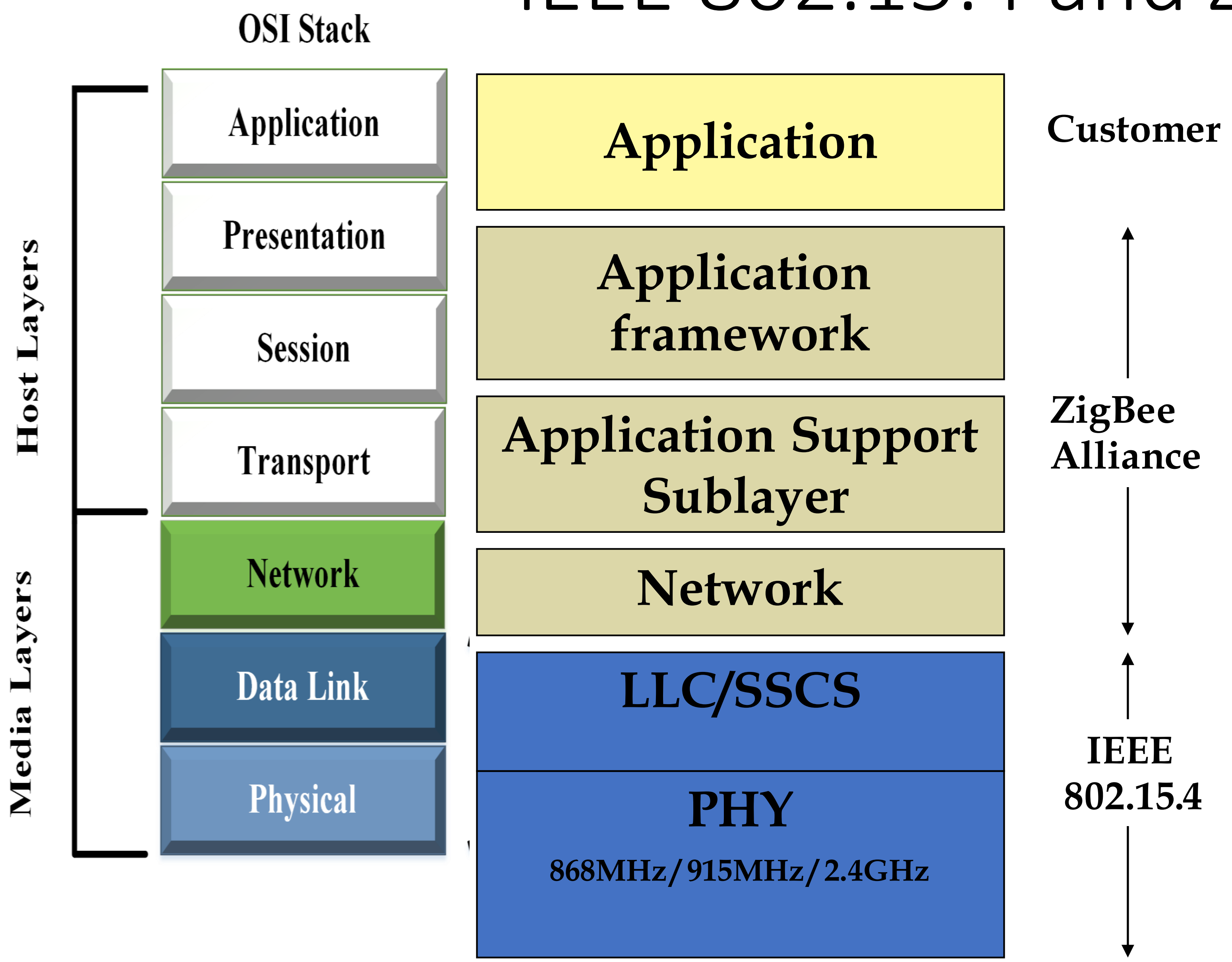
ZigBee Aims Low

- Low-data rate (Upto 250 kbps)
- Small amounts of data
- Low power consumption, devices turned off most of the time (<1% duty cycle)
- Low cost
- Low offered message throughput
- Low to no QoS guarantees
- Less Complex. 32kB protocol stack vs 250kB for Bluetooth

Zigbee Technical Specifications

Solution	Description Ref: *https://csa-iot.org/*
Network Protocol	Zigbee PRO 2015 (or newer)
Network Topology	Self-Forming, Self-Healing MESH , Star, Cluster Tree
Network Device Types	Coordinator (routing capable), Router, End Device, Zigbee Green Power Device
Network Size (theoretical # of nodes)	Up to 65,000
Radio Technology	IEEE 802.15.4-2011
Frequency Band / Channels	2.4 GHz (ISM band) 16-channels (2 MHz wide)
Data Rate	250 Kbits/sec
Security Models	Centralized (with Install Codes support) Distributed
Encryption Support	AES-128 at Network Layer Advanced Encryption Standard AES-128 available at Application Layer
Communication Range (Average)	Up to 300+ meters (line of sight) Up to 75-100 meter indoor
Low Power Support	Sleeping End Devices Zigbee Green Power Devices (energy harvesting)
Legacy Profile Support	Zigbee 3 devices can join legacy Zigbee profile networks. Legacy devices may join Zigbee 3 networks (based on network's security policy)
[illegible]	[illegible]

IEEE 802.15.4 and ZigBee



ZigBee Alliance

- Defines Software part of the protocol stack
- Takes care of Network, Security & Application layers
- Brand management, Runs in host

IEEE 802.15.4

- Released in October 2003
- Defines Physical & Data Link layer

ZigBee Logical Device Type

- A typical Zigbee network consist of three different device types, Zigbee coordinator, Router, and End device
- ZigBee coordinator (ZC)
    - IEEE 802.15.4 FFD
    - Starts network originally
    - Stores info about network - repository for security keys
    - Only one in a network
    - All devices communicate with ZBC
    - May do routing functionality
    - Bridge to other networks
    - Mains powered

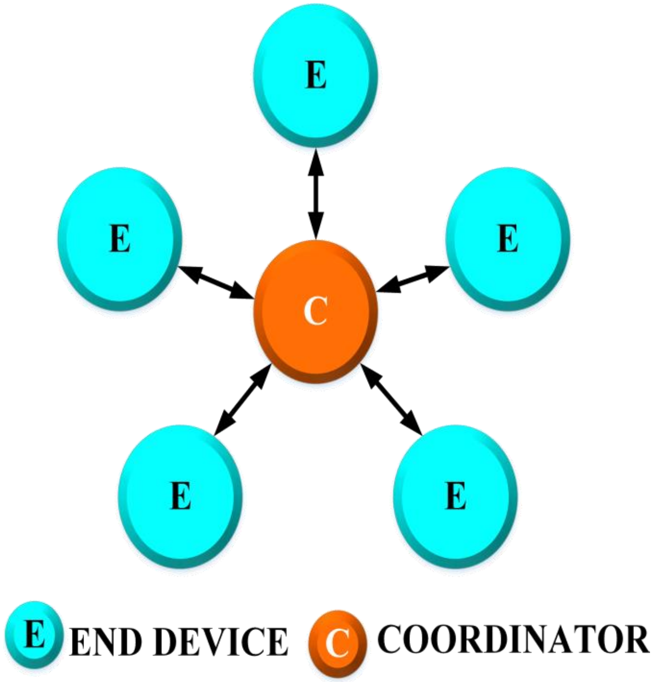
ZigBee Logical Device Type

- ZigBee Router (ZR):
  - IEEE 802.15.4 FFD
  - Optional network component
  - Intermediate router passing data in multihop paths
  - Can communicate with ZC, ZR, ZED
  - Extends network coverage
  - Scans to find a network to join

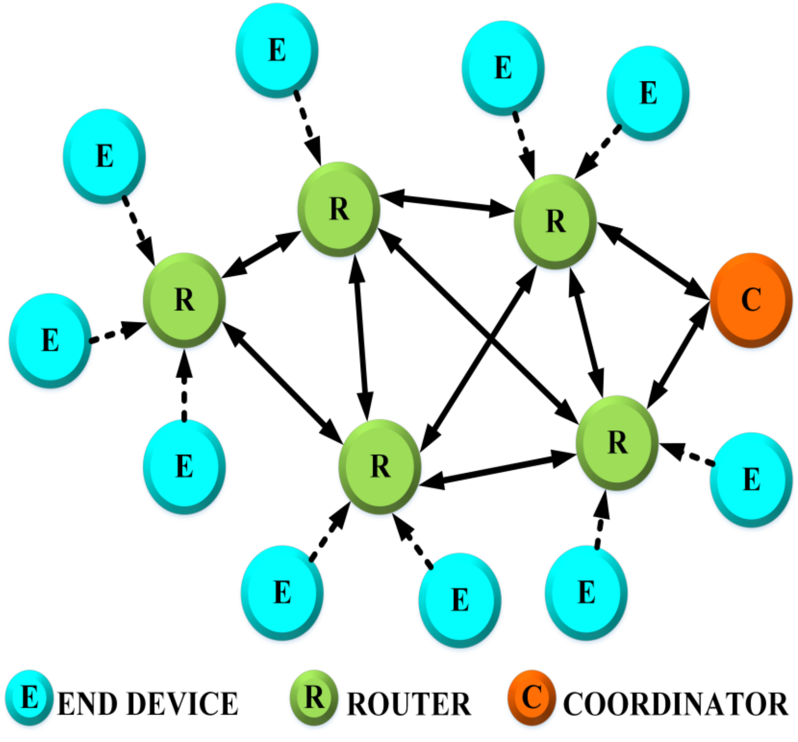
Zigbee Logical Device Type

- ZigBee End Device (ZED):
  - IEEE 802.15.4 RFD
  - Enough functionality to communicate with ZC or ZR
  - Node can sleep for significant amount of the time
  - Requires the least amount of memory
  - Cheapest device type
  - Sensor would be deployed here
  - Usually battery powered

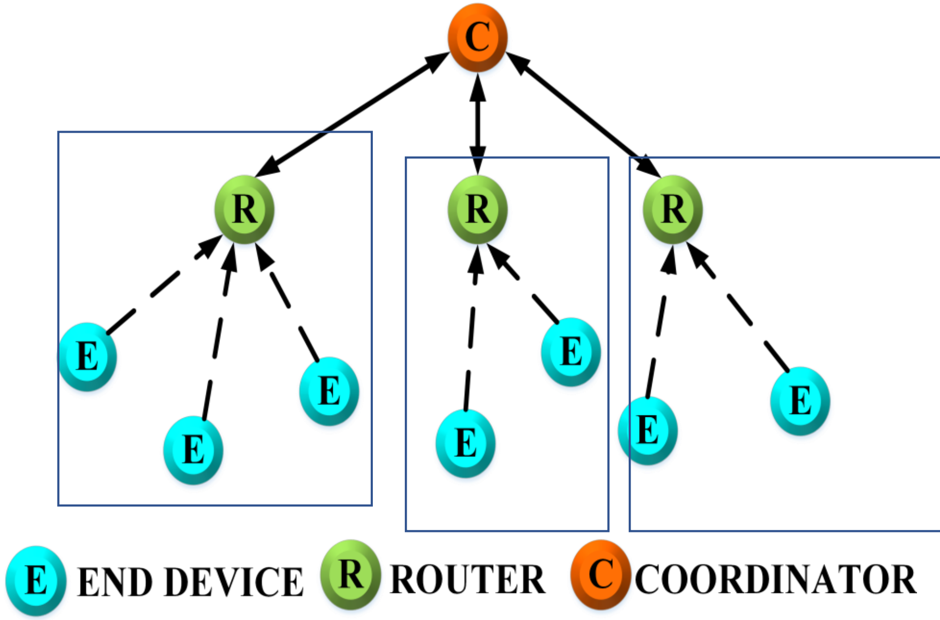
ZIGBEE Topologies



(a) Star



(b) Mesh



(c) cluster-tree

Various communication topologies in Zigbee

Network layer

- Handles operations such as, connecting and disconnecting the devices, configuring the devices
- Routing according to topology
- Setting up the network - Discover new neighbors and routers
- Distance vector based routing algorithm used

Application layer

- Interface of ZigBee system to its end user
- Application Support Sub-Layer:
  - Maintaining tables for binding devices together, based on their services and their needs (remote profiles, Garage Door and its opener) and forwarding messages between bound devices.
  - ZDO is a special application object that is resident on all ZigBee devices.
  - It has its own profile, ZigBee device profile (ZDP), which user application endpoints and other ZigBee devices can access.
  - ZDO is responsible for device management, security, defining role of device within network
- Application Framework:
  - Two types of data services are provided: provision of a key-value pair and generation of generic messages.
  - A key-value pair is used for getting attributes within the application objects, whereas a generic message is a developer-defined structure

Zigbee Power Consumption

- The power required to transmit a bit in Zigbee is 180 μW/bit.
- An implementation has 200 Zigbee end devices (where each device is attached to four sensors)
- Each device periodically transmits data to coordinator at intervals of 120 seconds.
- Packet from each node consists of: 64-bit node identifier, 64-bit destination identifier, 8-bit sensor values, 8-bit sensor identifier from each sensor
- How much power will be consumed by the implementation (except at the coordinator) for 1 hour of network operation
- Find no. of bits in each packet
- Find no. of packets transmitted by each device in one hour
- Find total packets transmitted by 200 devices
- Find number of bits in all those packets
- Find power consumption of all those bits
- Ans 207.36 W

Zigbee Power Consumption

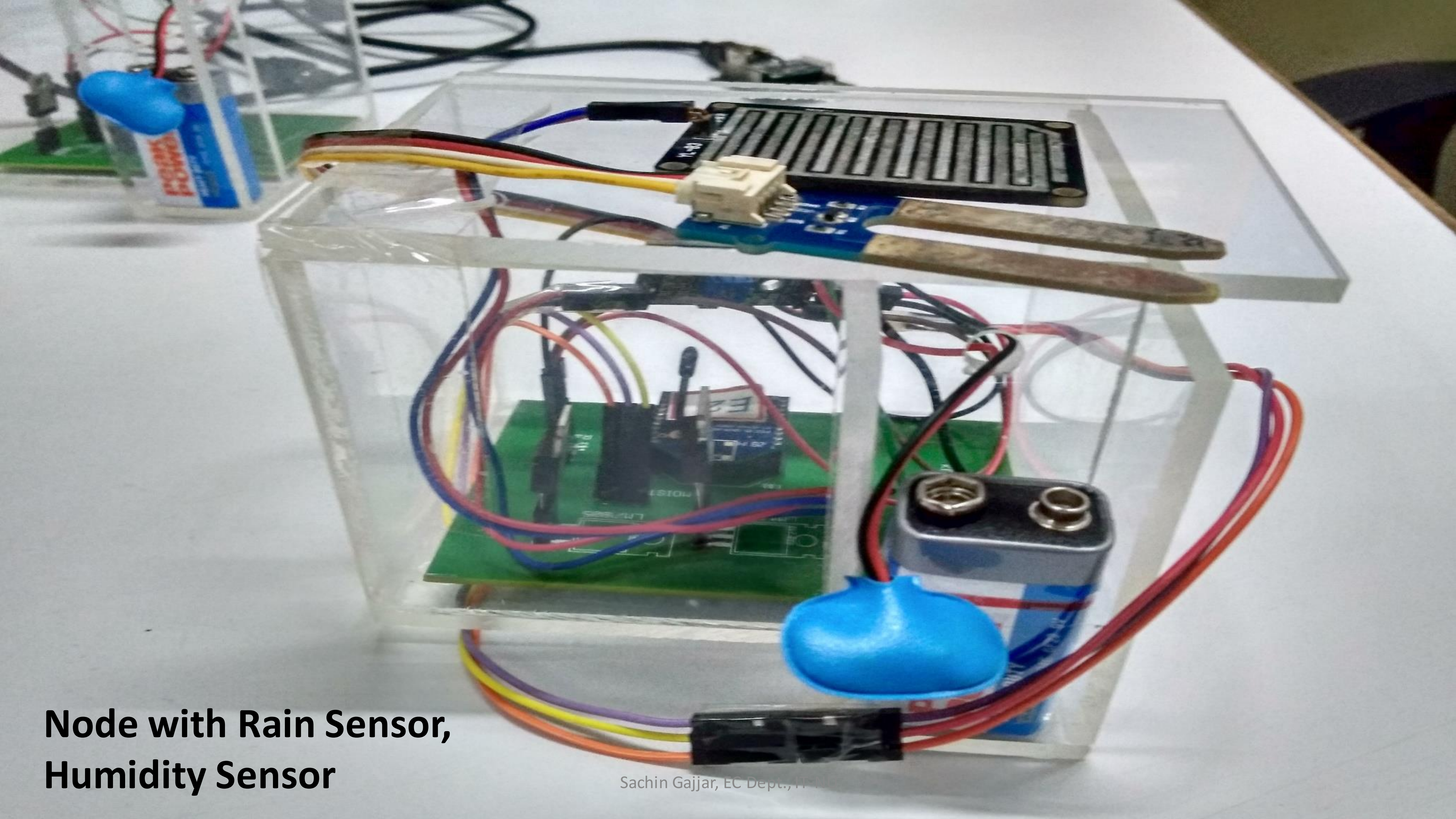
- For 1 end device, each packet consist of: 64 bits (sender id)+ 64 bits (destination id) + [(8 bits (sensor id) + 8 bits (sensor data)) x 4 (number of sensors per node)] = 192 bits
- 1 end device transmits 1 packet in 120 seconds
- Thus in 1 hour, each end device transmits = 3600x1/120=30 packets
- For 1 hour of operation, packets transmitted to coordinator = 30 (packets) × 200 (end devices) = 6000packets
- Number of bits transmitted to coordinator = 6000×192bits= 11,52,000 bits.
- Power consumption of 1 bit = 180 µW/bit
- Power consumption for the whole network for 1 hour of operation = 11, 52, 000 × 180 × 10^{-6} µW = 207.36 W

Hardware and Software

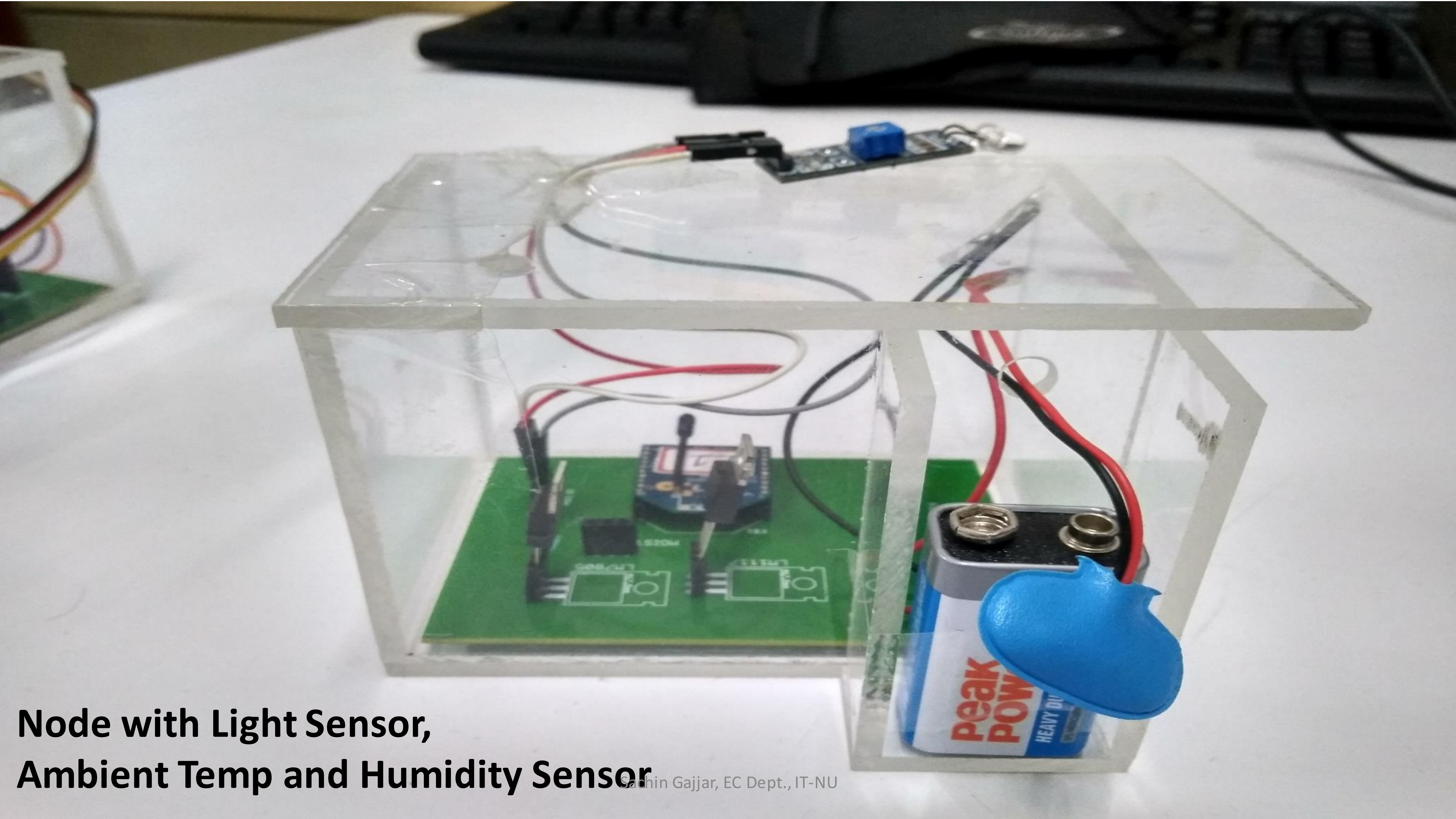
- Simpler and cheaper
- Chip has Integrated radio and microcontroller with 60K-28K flash memory
- Freescale, Ember, Texas, Digi International Instruments
- Radio available as stand-alone can be used with any processor or microcontroller
- Vendors offer ZigBee software stack, although independent ones are also available
- XBEE from Digi International (https://www.digi.com/xbee)

XBee - a wireless way of Serial line replacement

- XBee – Transmitter transmits data received through serial input over the air
- XBee – Receiver receives data from air, sent through serial interface



Node with Rain Sensor, Humidity Sensor



Node with Light Sensor,
Ambient Temp and Humidity Sensor

The End