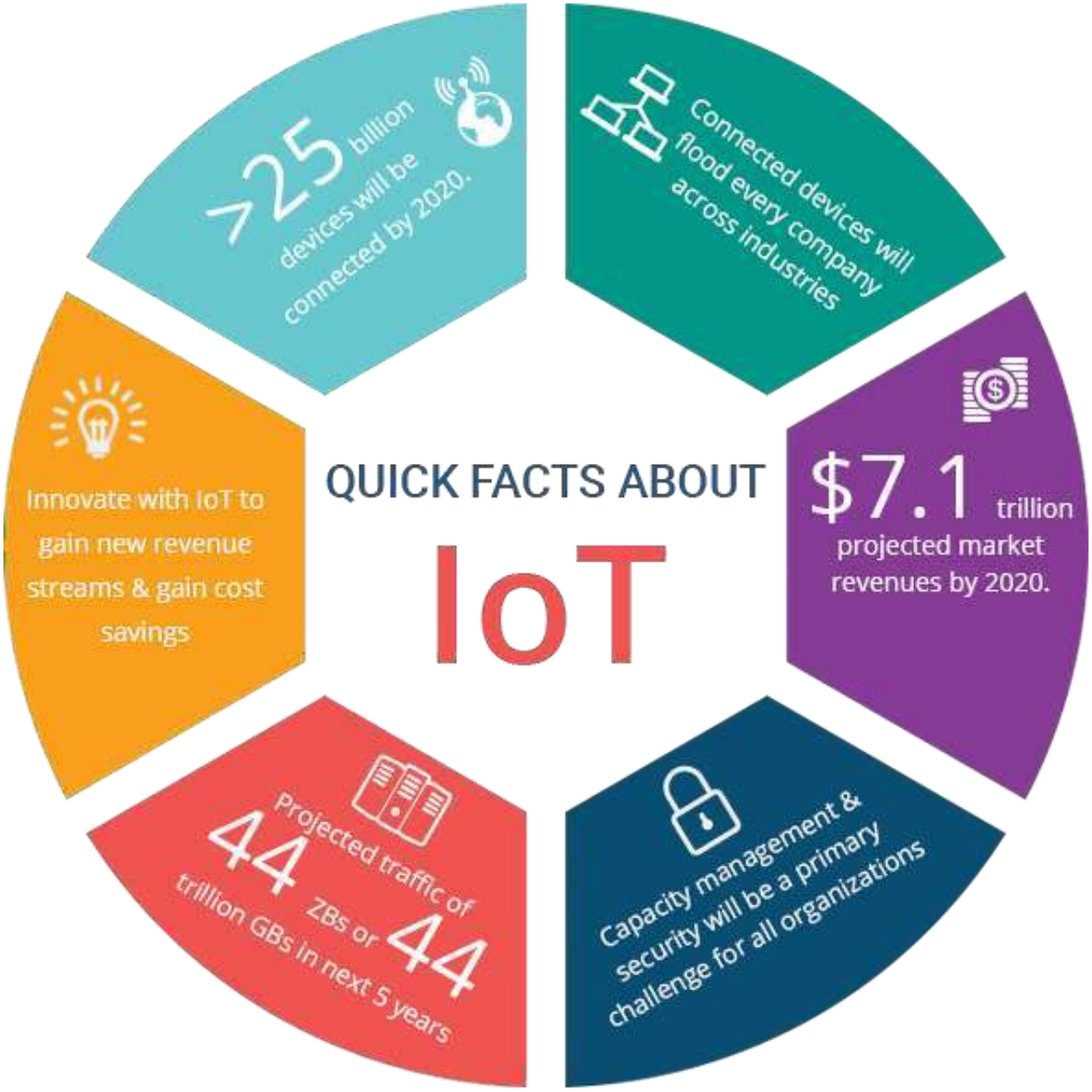
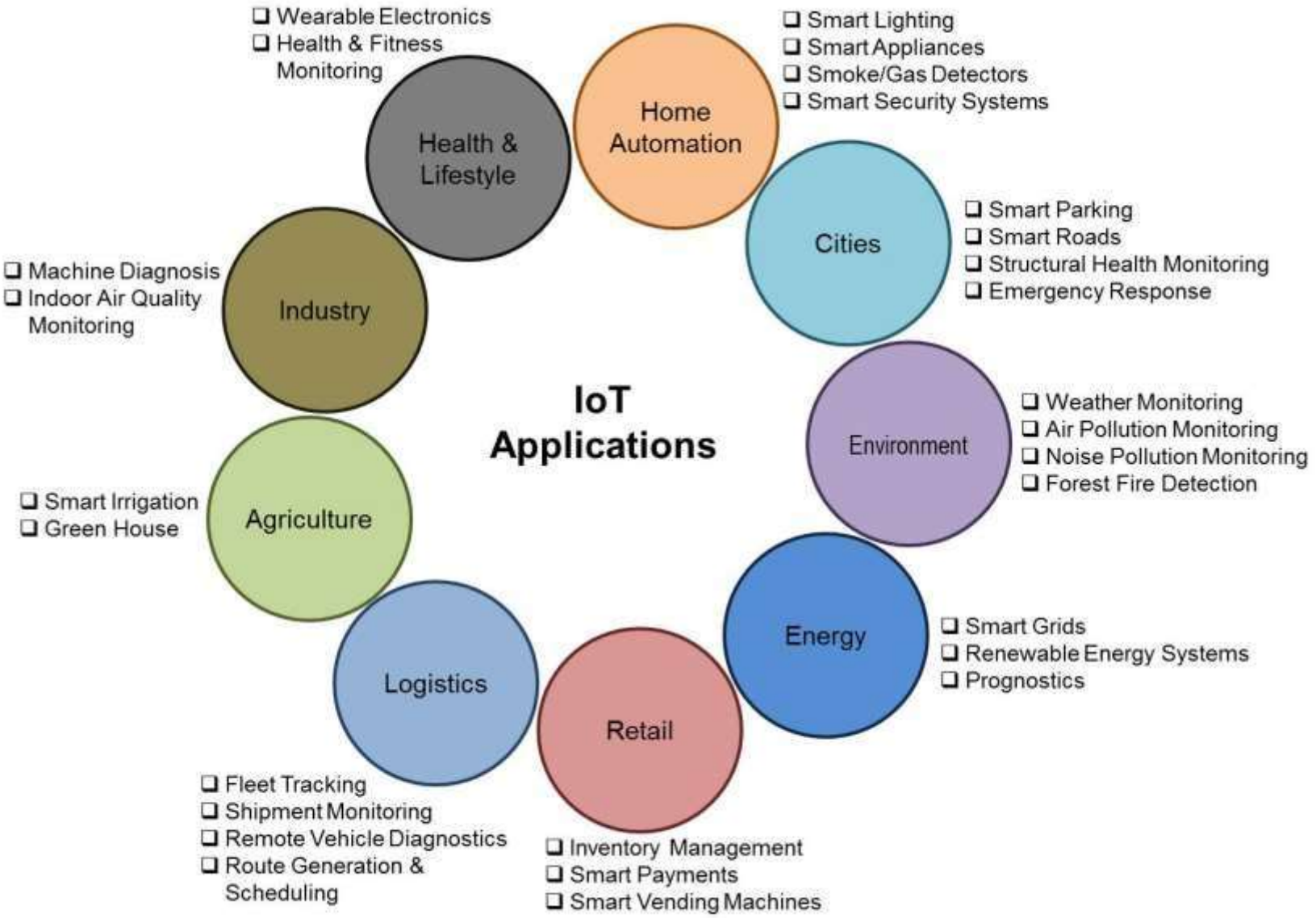
Unit – 2
IoT Protocols

Quick Facts about IoT


>25 billion devices will be connected by 2020.
Connected devices will flood every company across industries
$7.1 trillion projected market revenues by 2020.
Capacity management & security will be a primary challenge for all organizations
Projected traffic of 44 ZBs or 44 trillion GBs in next 5 years
Innovate with IoT to gain new revenue streams & gain cost savings
QUICK FACTS ABOUT
IoT

IoT Applications


IoT Applications
Health & Lifestyle
❑ Wearable Electronics
❑ Health & Fitness Monitoring
Home Automation
❑ Smart Lighting
❑ Smart Appliances
❑ Smoke/Gas Detectors
❑ Smart Security Systems
Cities
❑ Smart Parking
❑ Smart Roads
❑ Structural Health Monitoring
❑ Emergency Response
Environment
❑ Weather Monitoring
❑ Air Pollution Monitoring
❑ Noise Pollution Monitoring
❑ Forest Fire Detection
Energy
❑ Smart Grids
❑ Renewable Energy Systems
❑ Prognostics
Retail
❑ Inventory Management
❑ Smart Payments
❑ Smart Vending Machines
Logistics
❑ Fleet Tracking
❑ Shipment Monitoring
❑ Remote Vehicle Diagnostics
❑ Route Generation & Scheduling
Agriculture
❑ Smart Irrigation
❑ Green House
Industry
❑ Machine Diagnosis
❑ Indoor Air Quality Monitoring

Protocol Standardization for IoT

- IoT-Architecture one of the few efforts targeting a holistic architecture for all IoT sectors
- This consortium consists of 17 European organizations from nine countries
- Summarized current status of IoT standardization as
- Fragmented architectures
- No holistic approach to implement IoT has yet been proposed
- Many island solutions do exist (RFID, sensor nets, etc.)

- Little cross-sector reuse of technology and exchange of knowledge

M2M and WSN Protocols

- Most M2M applications are developed today in a highly customized fashion
- High-level M2M architecture from M2M Standardization Task Force (MSTF) does include fixed & other non cellular wireless networks
- Means it's generic, holistic IoT architecture even though it is M2M architecture
- M2M and IoT sometimes are used interchangeably in the United States.

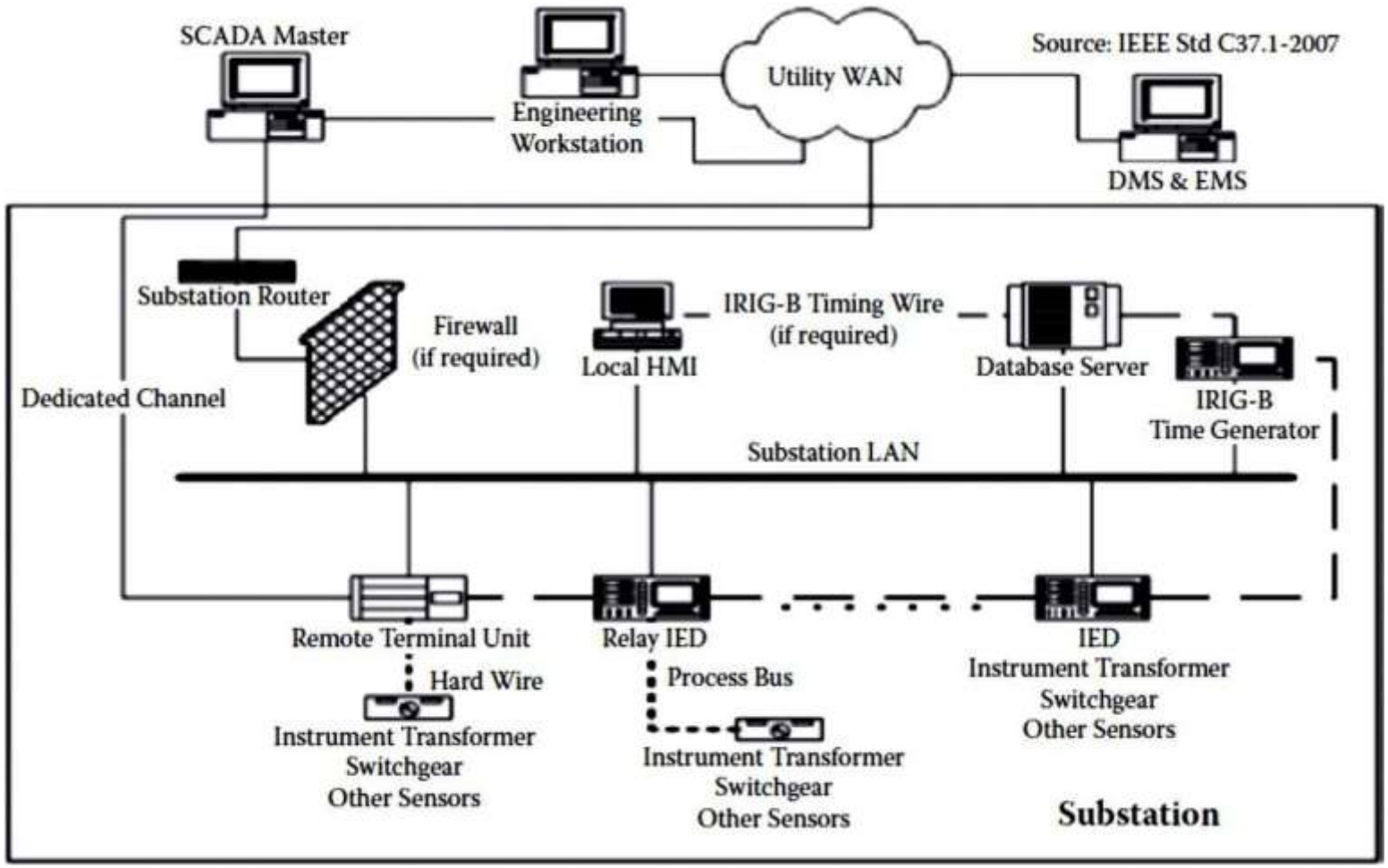
M2M and WSN Protocols

- Other M2M standards activities include:
- Data transport protocol standards - M2MXML, JavaScript Object Notation (JSON), BiTXML, WMMP, MDMP
- Extend OMA DM to support M2M devices protocol management objects
- M2M device management, standardize M2M gateway
- M2M security and fraud detection
- Network API's M2M service capabilities
- Remote management of device behind gateway/firewall
- Open REST-based API for M2M applications

SCADA and RFID Protocols

- Supervisory Control And Data Acquisition
- One of the IoT pillars to represent the whole industrial automation arena
- IEEE created standard specification called Std C37.1™, for SCADA & automation systems in 2007
- In recent years, network-based industrial automation has greatly evolved
- With the use of intelligent electronic devices (IEDs), or IoT devices in our terms, in substations and power stations

SCADA and RFID Protocols



SCADA and RFID Protocols

- The processing is now distributed
- Functions that used to be done at control center can now be done by IED i.e. M2M between devices
- Due to restructuring of electric industry, traditional vertically integrated electric utilities are replaced by many entities such as
- GENCO (Generation Company),
- TRANSCO (Transmission Company),
- DISCO (Distribution Company),
- ISO (Independent System Operator), etc.

Issues with IoT Standardization

- It should be noted that not everything about standardization is positive
- Standardization is like a double-edged sword:
- Critical to market development
- But it may threaten innovation and inhibit change when standards are accepted by the market
- Standardization and innovation are like yin & yang

Issues with IoT Standardization

- They could be contradictory to each other in some cases, even though this observation is debatable
- Different consortia, forums and alliances have been doing standardization in their own limited scope
- For example, 3GPP covers only cellular wireless networks while EPCglobal's middleware covers only RFID events

Issues with IoT Standardization

- Even within same segment, there are more than one consortium or forum doing standardization without enough communication with each other
- Some are even competing with each other
- Some people believe that the IoT concept is well established

Issues with IoT Standardization

- However, some gray zones remain in the definition, especially which technology should be included
- Following two issues for IoT standardization in particular and ICT standardization in general may never have answers:

1. ICT standardization is a highly decentralized activity. How can the individual activities of the

Issues with IoT Standardization

network of extremely heterogeneous standardssetting bodies be coordinated?

2. It will become essential to allow all interested stakeholders to participate in the standardization process toward the IoT and to voice their respective requirements and concerns. How can this be achieved?

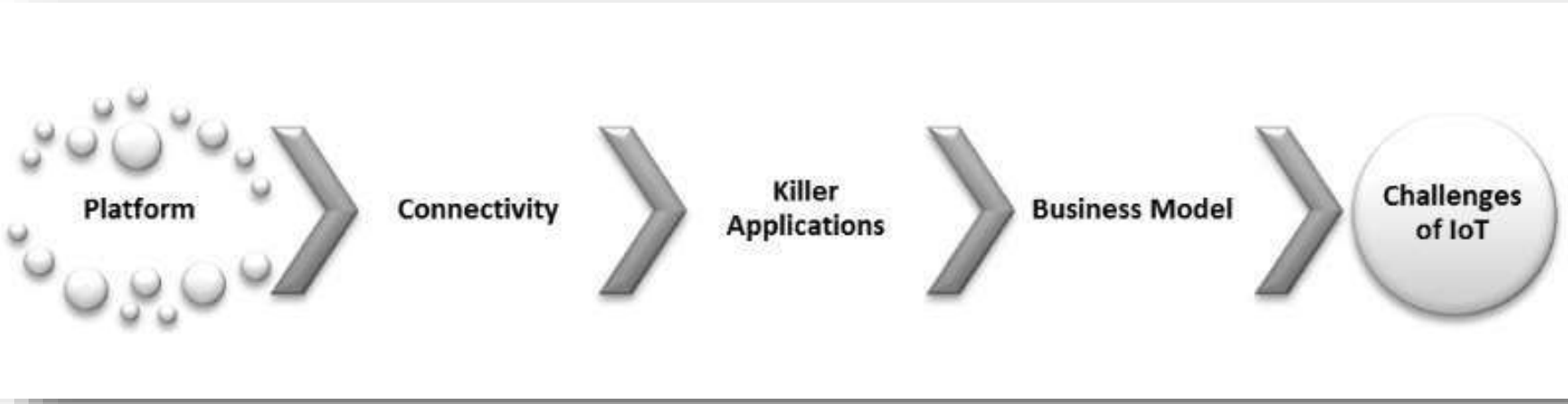
IoT Standardization and Implementation Challenges

- Creating that model will never be an easy task by any level of imagination, there are hurdles and challenges facing the standardization and implementation of IoT solutions and that model needs to overcome all of them.

IoT standardization

IoT standardization

- The hurdles facing IoT standardization can be divided into **4** categories;
- **Platform**
- **Connectivity**
- **Business Model**
- **Standard Applications**


Platform
Connectivity
Killer Applications
Business Model
Challenges of IoT

Platform

- This part includes the form and design of the products (UI/UX), analytics tools used to deal with the massive data streaming from all products in a secure way, and scalability which means wide adoption of protocols like IPv6 in all vertical and horizontal markets is needed.

Connectivity

- This phase includes all parts of the consumer's day and night routine, from using wearables, smart cars, smart homes, and in the big scheme, smart cities. From the business prospective we have connectivity using IIoT (Industrial Internet of Things) where M2M communications dominating the field.

Business Model

- The bottom line is a big motivation for starting, investing in, and operating any business, without a sound and solid business models for IoT we will have another bubble , this model must satisfied all the requirements for all kinds of e-commerce; vertical markets, horizontal markets and consumer markets. But this category is always a victim of regulatory and legal scrutiny.

Standard Applications

- In this category there are three functions needed to have standard applications: control “things”, collect “data”, and analyze “data”. IoT needs standard applications to drive the business model using a unified platform.

- All four categories are inter-related, you need all them to make all them work. Missing one will break that model and stall the standardization process.

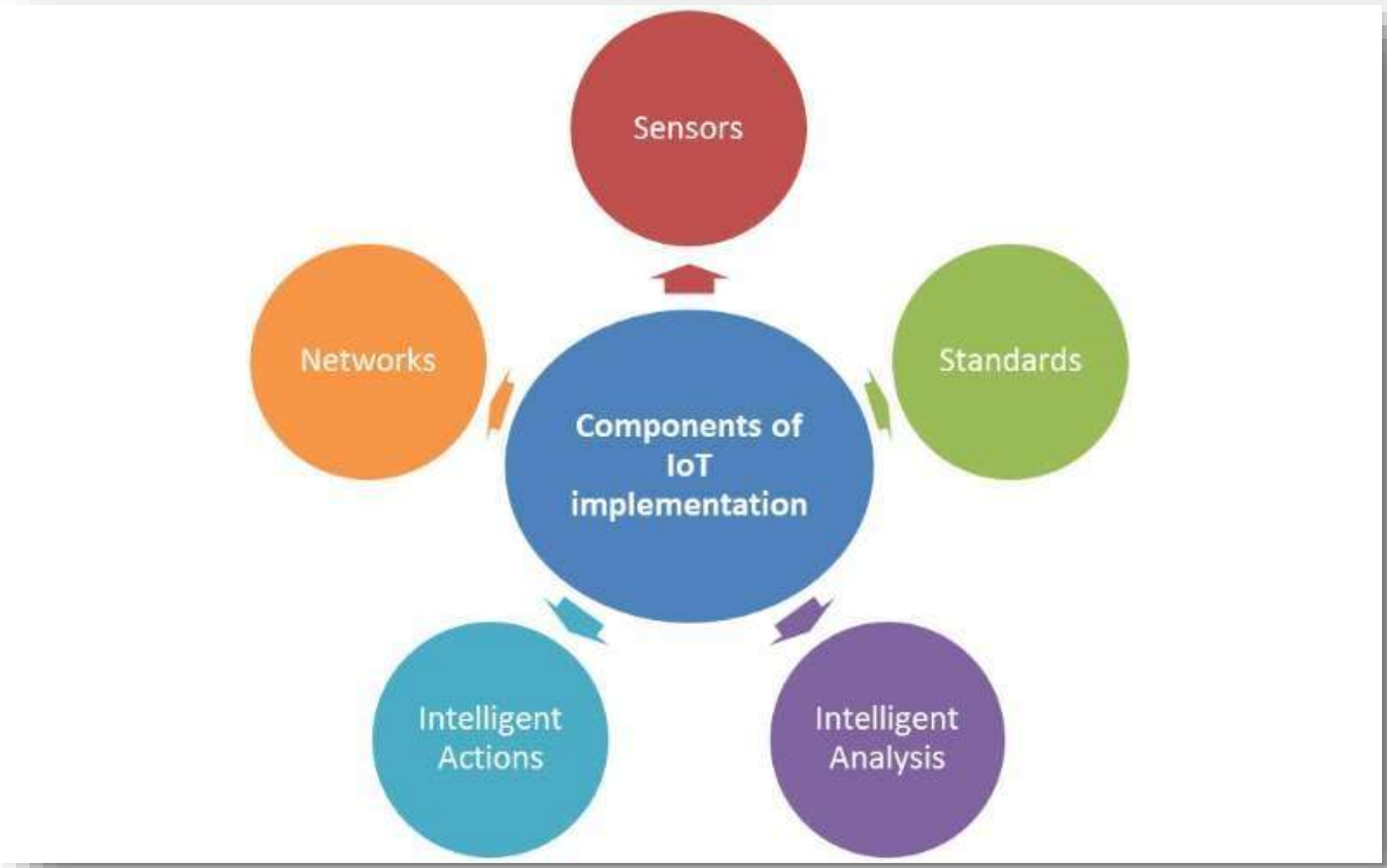
- A lot of work needed in this process, and many companies are involved in each of one of the categories, bringing them to the table to agree on a unifying model will be daunting task.

IoT implementation

IoT implementation

- The second part of the model is IoT implementations; implementing IoT is not an easy process by any measure for many reasons including the complex nature of the different components of the ecosystem of IoT.

- To understand the gravity of this process, we will explore all the **five** components of IoT Implementation:
- Sensors
- Networks
- Standards
- Intelligent Analysis
- Intelligent Actions


Sensors
Networks
Standards
Components of IoT implementation
Intelligent Actions
Intelligent Analysis

Sensors

- There two types of sensors: active sensors & passive sensors.
- *The driving forces for using sensors in IoT* today are new trends in technology that made sensors **cheaper, smarter** and **smaller**.
- *The Challenges facing IoT sensors are:* power consumption, security, and interoperability.

Networks

- The second component of IoT implantation is to transmit the signals collected by sensors over networks with all the different components of a typical network including routers, bridges in different topologies.

- Connecting the different parts of networks to the sensors can be done by different technologies including Wi-Fi, Bluetooth, Low Power Wi-Fi , Wi-Max, regular Ethernet , Long Term Evolution (LTE) and the recent promising technology of Li-Fi (using light as a medium of communication between the different parts of a typical network including sensors).

- *The driving forces for wide spread network adoption in IoT are h*igh data rate, low prices of data usage, virtualization (X - Defined Network trends), XaaS concept (SaaS, PaaS, and IaaS), and IPv6 deployment. B

- *The challenges facing network implementation in IoT are t*he enormous growth in number of connected devices, availability of networks coverage, security, and power consumption.

Standards

- The third stage in the implementation process includes the sum of all activities of handling, processing and storing the data collected from the sensors.

- This aggregation increases the value of data by increasing, *the scale, scope, and frequency* of data available for analysis but aggregation only achieved through the use of various standards depending on the IoT application in used.

- There are two types of standards relevant for the aggregation process:
- *Technology standards* (including network protocols, communication protocols, and data-aggregation standards)
- *Regulatory standards* (related to security and privacy of data, among other issues).

- *The Challenges facing the adoptions of standards within IoT are:* **standard for handling unstructured data, security and privacy issues** in addition to **regulatory standards for data markets**.

Intelligent Analysis

- The fourth stage in IoT implementation is extracting insight from data for analysis. IoT analysis is driven by *cognitive technologies* and the accompanying models that facilitate the use of cognitive technologies.

- With advances in cognitive technologies' the ability to process varied forms of information, vision and voice have also become usable, and open the doors for in-depth understanding of the none-stop streams of real-time data.

- *The Factors driving adoption intelligent analytics within the IoT;* **artificial intelligence models, growth in crowdsourcing and open-source analytics software, real-time data processing and analysis**.

- *The Challenges facing the adoption of analytics within IoT* **; Inaccurate analysis due to flaws in the data and/or model, legacy systems' ability to analyze** *unstructured data, and l***egacy systems' ability to manage real-time data**

Intelligent Actions

- Intelligent actions can be expressed as M2M (Machine to Machine) and M2H (Machine to Human) interfaces for example with all the advancement in UI and UX technologies.

- *TheFactors driving adoption of intelligent actions within the IoT;* lower machine prices, improved machine functionality, machines "influencing" human actions through behavioral-science rationale, and deep Learning tools.

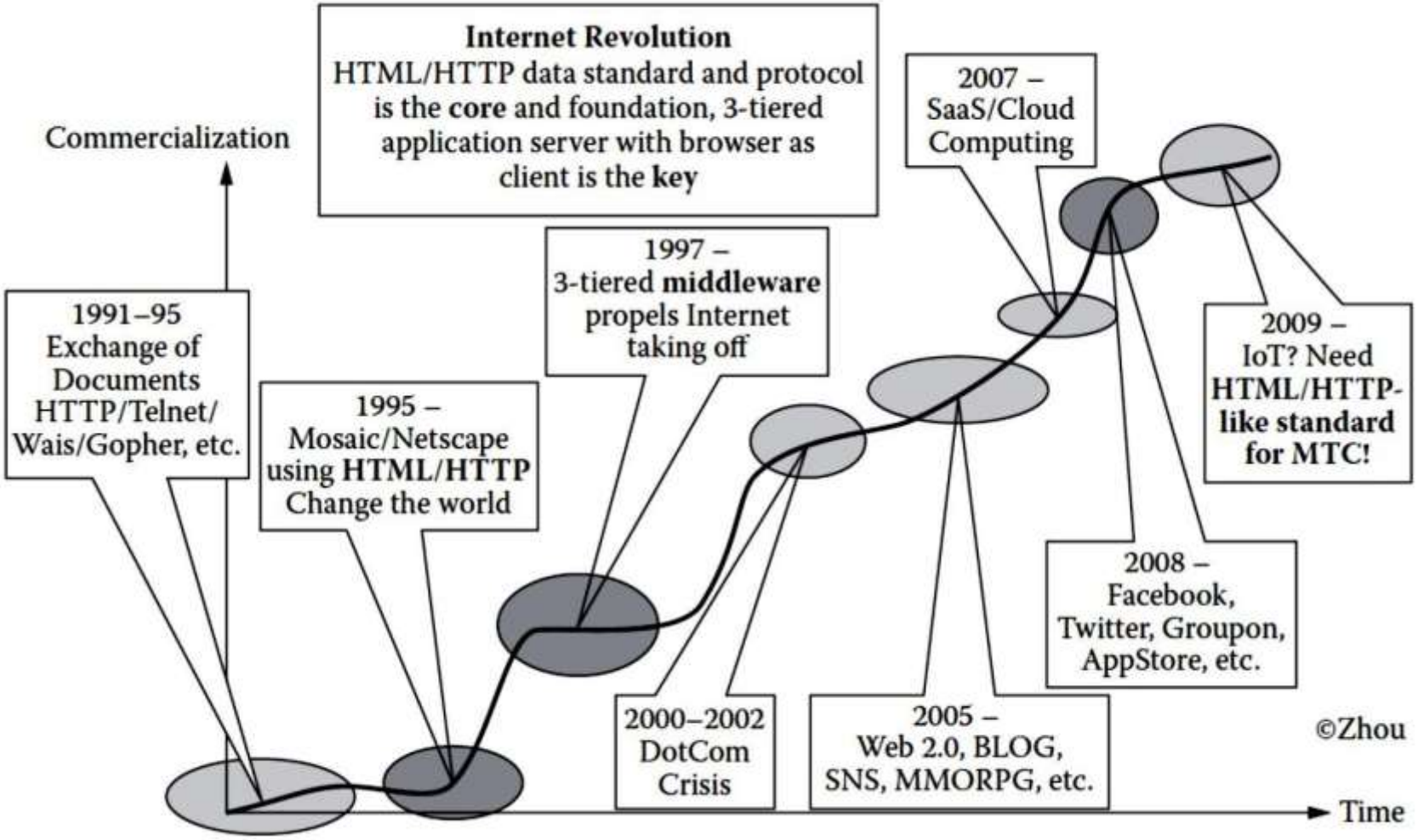
- *The Challenges facing the adoption of intelligent actions within IoT* **:** machines' actions in unpredictable situations, information security and privacy, machine interoperability, mean-reverting human behaviors, and slow adoption of new technologies

Unified Data Standards

- Already discussed about two pillars of the Internet
- HTML/HTTP combination of data format and exchange protocol is the foundation pillar of WWW
- Described great number of data standards and protocols proposed for four pillar domains of IoT
- Many issues still impede the development of IoT and especially WoT vision

Unified Data Standards

Evolution of web



Unified Data Standards

- Many standardization efforts have been trying to define unified data representation, protocol for IoT
- Before IoT, Internet was actually an Internet of documents or of multimedia documents
- Two pillars of Internet including HTML/HTTP turned the Internet into WWW
- We need to turn the IoT into the WoT
- What will it take to make this to happen?
- *Do we need a new HTML/HTTP-like standard for MTC and WoT? If there is no need to reinvent the*

Unified Data Standards

wheel, what extensions do we need to build on top of HTML/HTTP or HTML5?

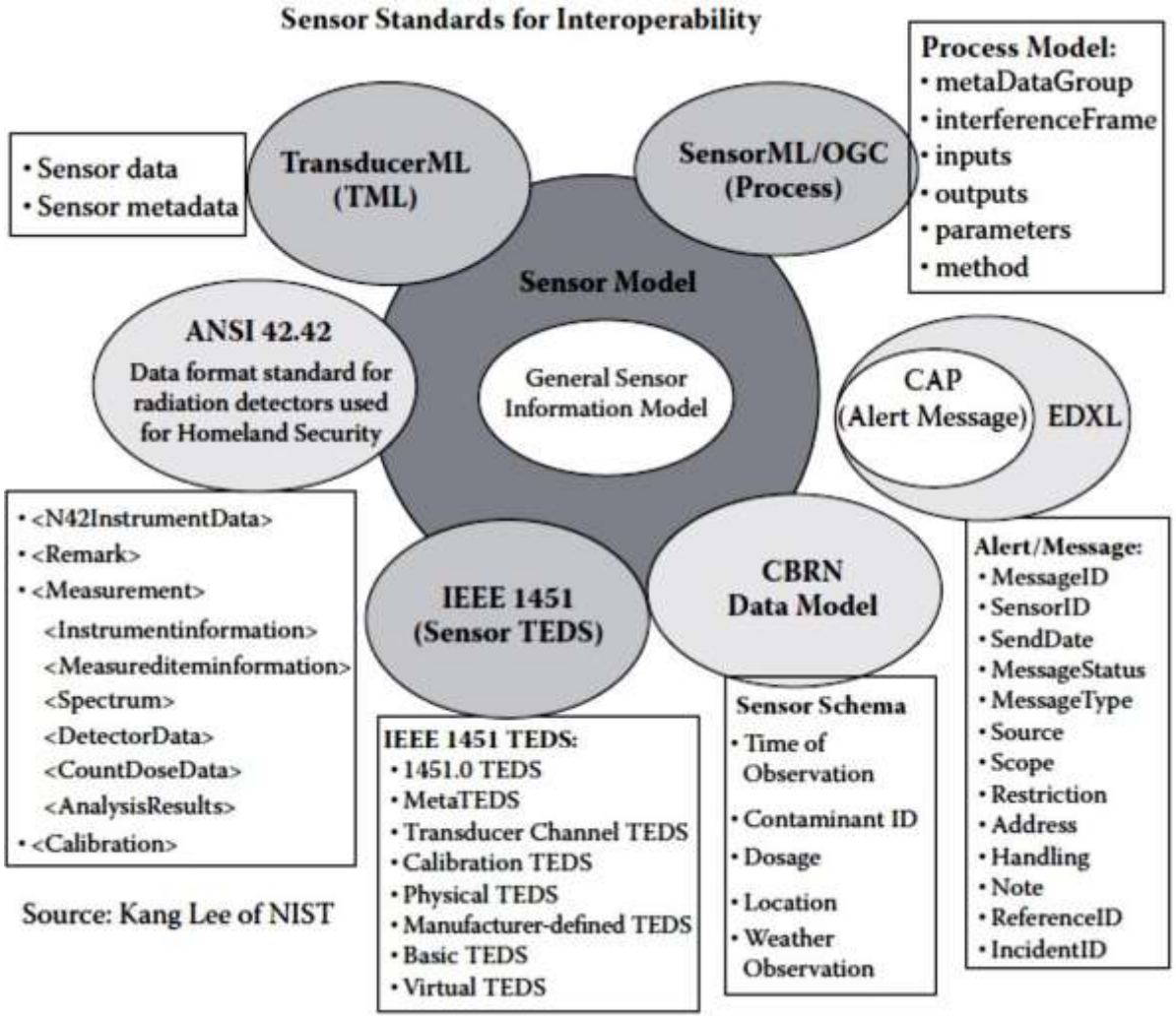
- *Browser is intended for humans, so do we need new browser for machines to make sense of ocean of machine-generated data? If not, what extensions do we need to make to the existing browsers?*
- *Today, most new protocols are built on top of XML. For OS there must be XML-based data format standards or a metadata standard to represent the machine-generated data (MGD). Is it possible to define such a metadata standard that covers everything?*

Unified Data Standards

- There are many different levels of protocols
- But the ones that most directly relate to business and social issues are the ones closest to the top
- so-called application protocols such as HTML/HTTP for the web
- Web has always been visual medium, but restricted
- Until recently, HTML developers were limited to CSS

  & JavaScript in order to produce animations
- Or they would have to rely on a plug-in like Flash

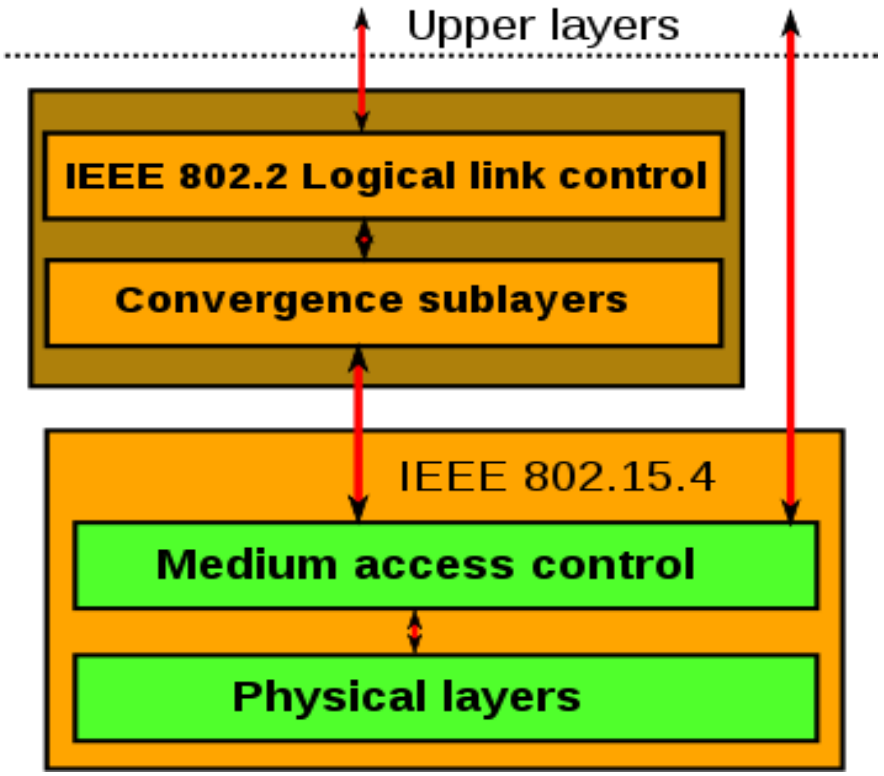
Unified Data Standards



Protocols – IEEE 802.15.4

- Defines operation of low-rate wireless personal area networks (LR-WPANs)
- Specifies physical layer and media access control for LR-WPANs
- Maintained by IEEE 802.15 working group, which defined the standard in 2003
- Basic framework conceives a 10m communications range with a transfer rate of 250 kbit/s

Protocols – IEEE 802.15.4



- *Physical Layer* (PHY) provides data transmission service & interface to *physical layer management entity*
- MAC enables transmission of MAC frames through the use of the physical channel

BACNet Protocol

- Communications protocol for Building Automation and Control (BAC) networks
- Provides mechanisms for computerized building automation devices to exchange information
- Designed to allow communication of building automation & control system for application like
- Heating, Ventilating and Air-conditioning Control (HVAC)
- Lighting Control, Access Control
- Fire Detection Systems and their Associated Equipment

BACNet Protocol

- Defines a number of services that are used to communicate between building devices
- Protocol services include Who-Is, I-Am, Who-Has, IHave which are used for Device & Object discovery
- Services such as Read-Property and Write-Property are used for data sharing
- Defines 60 object types that are acted upon by services
- Defines no. of data link/physical layers including
- ARCNET,

- Ethernet,
- BACnet/IP,
- BACnet/IPv6,
- Point-To-Point over RS-232,
- Master-Slave/Token-Passing over RS-485,
- ZigBee
- LonTalk

Modbus

- Serial communications protocol originally published by Modicon (now Schneider Electric) in 1979
- Commonly available for connecting industrial electronic devices
- Reasons for use of Modbus in industrial environment:
- Developed with industrial applications in mind
- Openly published and royalty-free
- Easy to deploy and maintain

- Enables communication among many devices connected to the same network

Modbus Object Types

Object type	Access	Size
Coil	Read-write	1 bit
Discrete input	Read-only	1 bit
Input register	Read-only	16 bits
Holding register	Read-write	16 bits

Protocol Versions

- Modbus RTU
- Modbus ASCII
- Modbus TCP/IP or Modbus TCP
- Modbus over TCP/IP or Modbus over TCP or Modbus RTU/IP
- Modbus over UDP
- Modbus Plus (Modbus+, MB+ or MBP)
- Pemex Modbus
- Enron Modbus

KNX Protocol

- Standardized (EN 50090, ISO/IEC 14543), OSI-based network communications protocol for automation
- Defines several physical communication media:
- Twisted pair wiring (inherited from the BatiBUS and EIB Instabus standards)
- Powerline networking (inherited from EIB and EHS similar to that used by X10)
- Radio (KNX-RF)
- Infrared
- Ethernet (also known as EIBnet/IP or KNXnet/IP)

KNX System Components

- All the devices for a KNX installation are connected together by a two wire bus to exchange data
- Sensors
- Actuators
- System devices and components

ZigBee/IEEE 802.15.4

ZigBee/IEEE 802.15.4

Why ZigBee ?

- Wireless communication standards:
  - IEEE 802.11 a/b/g
  - Bluetooth
  - GSM
- What makes them unattractive for WSN:
  - Power hungry (need big batteries)
  - Complexity (need lots of clock cycles and memory)
- New protocol for WSN:
  - 802.15.4 and Zigbee (ratified in Dec 14, 2004)
  - Low Cost
  - Low Power Consumption
  - Scalability and Reliability

Origin Of Name ZigBee

- The technique that honey bees use to communicate new-found food sources to other members of the colony is referred to as the ZigBee Principle.

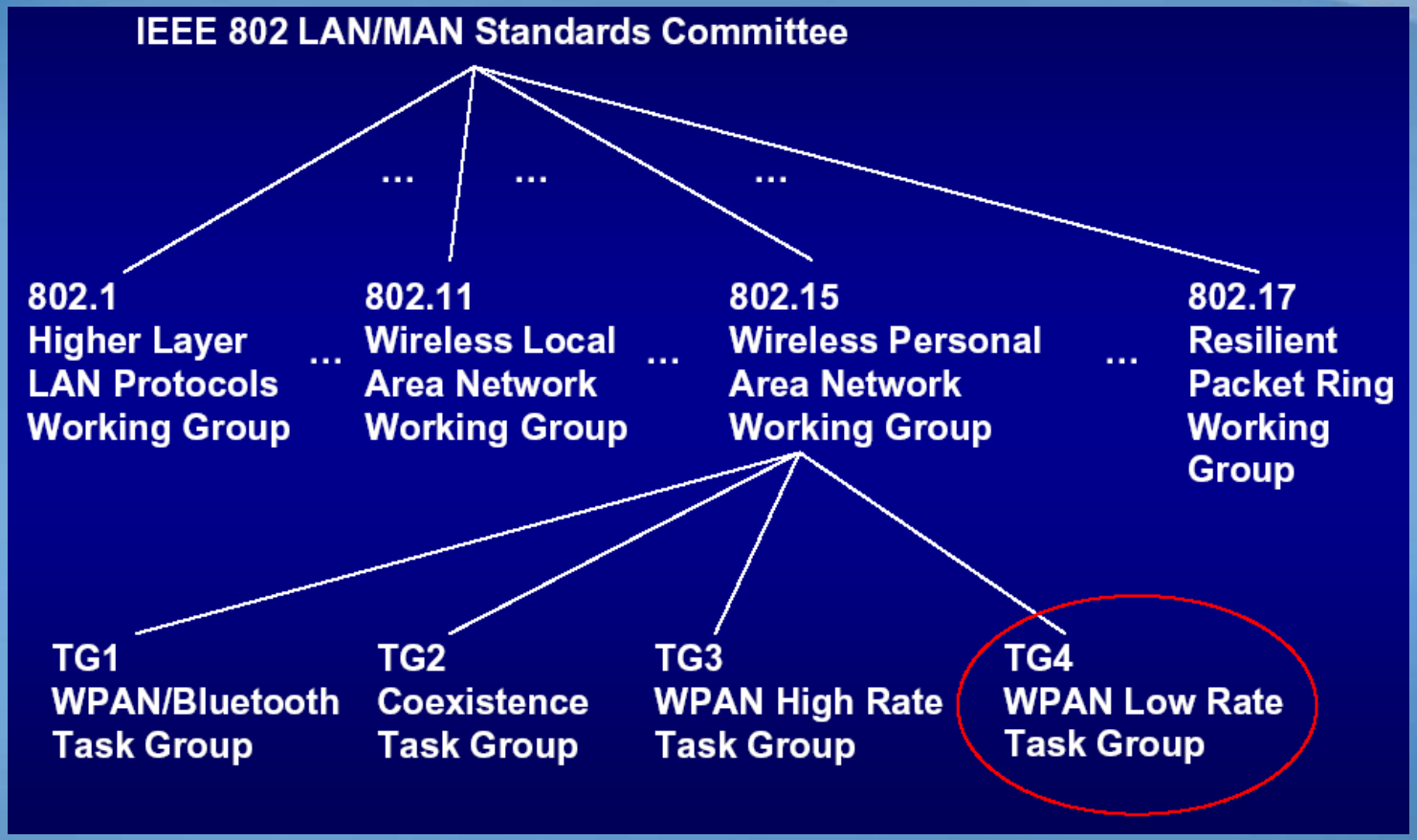
- Using this silent, but powerful communication system, whereby the bee dances in a zig-zag pattern, she is able to share information such as the location, distance, and direction of a newly discovered food source to her fellow colony members. Instinctively implementing the ZigBee Principle.

802.15.4 Standard (WPAN)

Within the broad organization of the Institute of Electrical and Electronics Engineers (IEEE), the 802 group is the section that deals with network operations and technologies. Group 15 works more specifically with *wireless* networking, and Task Group 4 drafted the 802.15.4 standard for a low data rate wireless personal area network (WPAN).

The ZigBee standard is currently an ‘open’ standard only to those that are a part of the ZigBee Alliance. For this reason, the ZigBee standard was not used to implement the application layer.

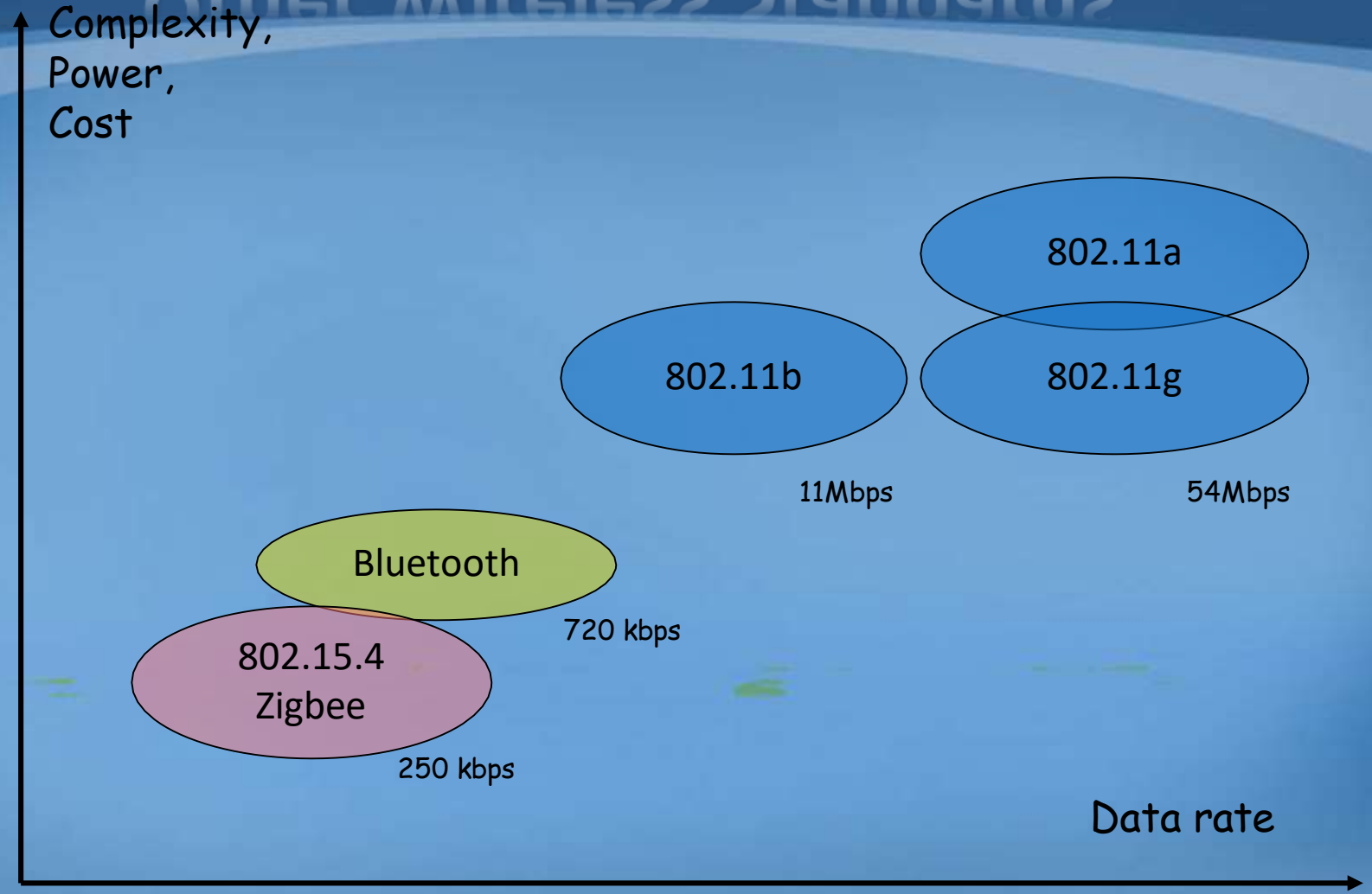
IEEE 802.15 working group



ZigBee General Characteristics

- Data rates of 20 kbps and up to 250 kbps
- Intended for 2.45 Ghz , 868 Mhz and 915 Mhz Band
- Data rates touch 250Kbps for 2.45Ghz ,40 Kbps 915Mhz and 20Kbps for 868Mhz band
- Star or Peer-to-Peer network topologies
- Support for Low Latency Devices
- CSMA-CA Channel Access
- Handshaking
- Low Power Usage consumption
- 3 Frequencies bands with 27 channels
- Extremely low duty-cycle (<0.1%)

Comparision Graph with Other Wireless Standards



Why NOT 802.11 ?

The Cost of Throughput

- High data rates
  - up to 11Mbps for b and
  - up to 54Mbps for g and a)
- Distance up to 300 feet, or more with special antennas
- **High power consumption**
  - Sources about **1800mA** when transceiver is operational.

ZigBee Aims Low

- Low data rate
- Low power consumption
- Small packet devices

What Does ZigBee Do?

- Designed for wireless controls and sensors
- Operates in Personal Area Networks (PAN's) and device-to-device networks
- Connectivity between small packet devices
- Control of lights, switches, thermostats, appliances, etc.

How ZigBee Works

- Devices
  - Zigbee Coordinator Node
  - Zigbee Full Function Node
  - Zigbee Reduced Function Node
- Modes of operation
  - Beacon
  - Non-beacon

Device Types and Roles

- **Zigbee Coordinator Node (ZCN):**
  - It is the root of the network tree
  - Acts as a bridge to other networks.
  - Stores Information about the Network
  - There is only one ZCN for the complete Network

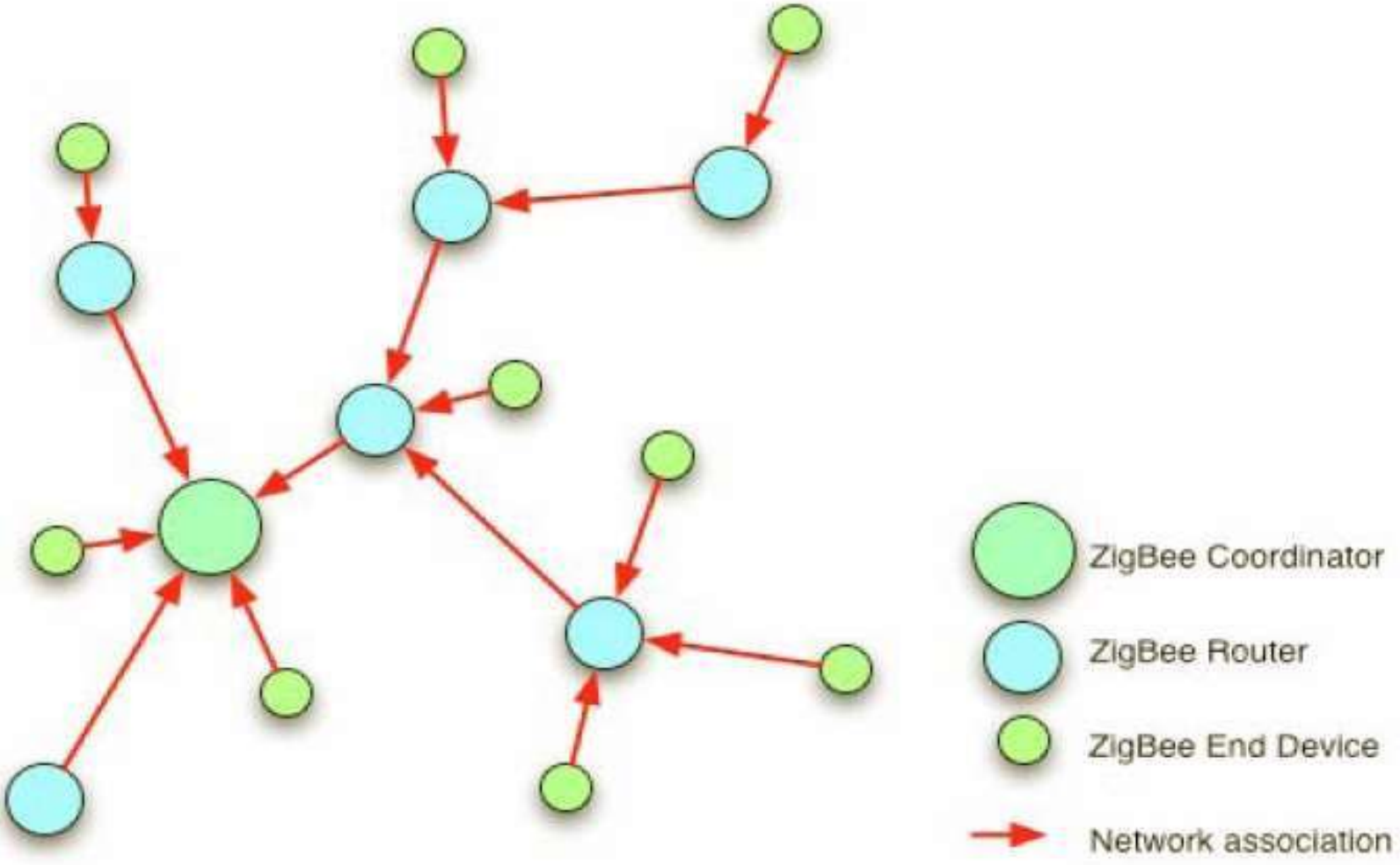
Device Types and Roles

- **Zigbee Full Functional Device (FFD):**
  - An Intermediate router in the Network
  - Transmitting and Receiving data from other devices
  - Needs less memory than Zigbee Coordinator Node
  - Lesser Manufacturing cost
  - Can operate on all topologies

Device Types and Roles

- **Zigbee Reduced Function Device (RFD):**
  - Also called the End Device
  - Device capable of talking in the Network
  - Can’t relay data from other devices
  - Cheaper than FFD
  - Lesser Manufacturing cost
  - Talks only to the Network Coordinator

Device Types and Roles



Modes of Operation

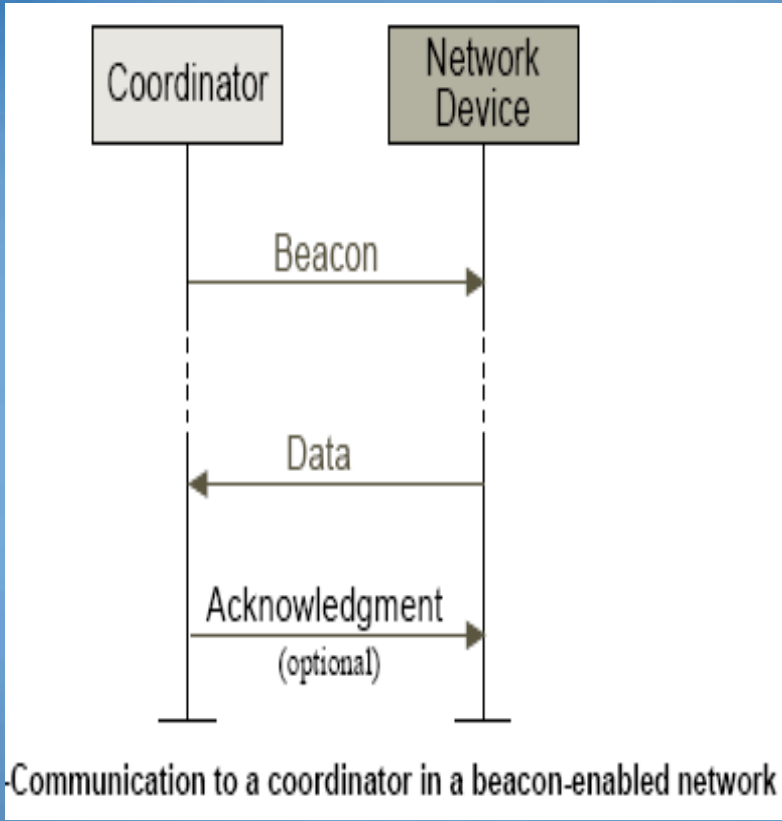
- **Beacon Mode :**

In beacon-enabled networks, the special network nodes called ZigBee Routers transmit periodic beacons to confirm their presence to other network nodes. Nodes may sleep between beacons, thus lowering their duty cycle and extending their battery life.

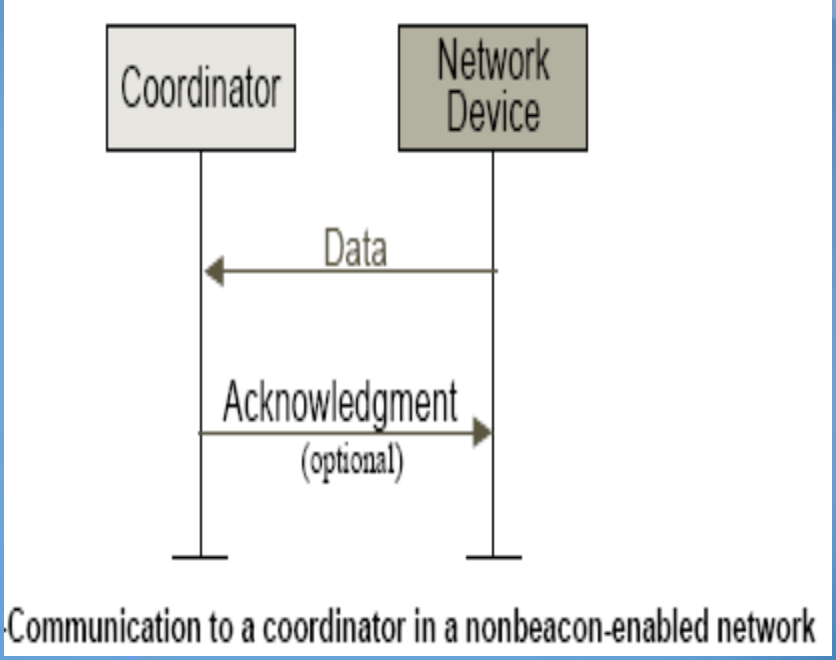
- **Non Beacon Mode**

In non-beacon-enabled networks, an unslotted CSMA/CA channel access mechanism is used. In this type of network, ZigBee Routers typically have their receivers continuously active, requiring a more robust power supply.

Modes of Operation



Communication to a coordinator in a beacon-enabled network

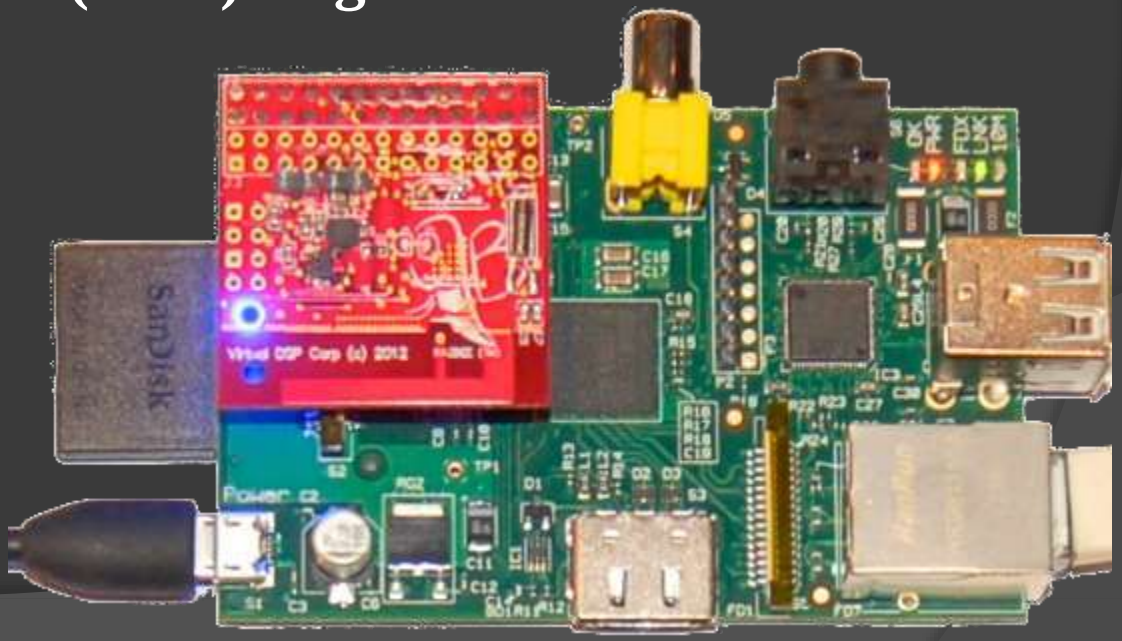


Communication to a coordinator in a nonbeacon-enabled network

Device types

There are three different types of ZigBee device:

- **ZigBee coordinator (ZC)**
- ***ZigBee Router (ZR)/ Zigbee FFD***
- **ZigBee End Device (ZED)/ Zigbee RFD**



Types Explained…

- **ZigBee coordinator (ZC):** The most capable device, the coordinator forms the root of the network tree and might bridge to other networks.

There is exactly one ZigBee coordinator in each network. It is able to store information about the network, including acting as the repository for security keys.

Types Explained…

- **ZigBee Router (ZR):** Routers can act as an intermediate router, passing data from other devices.

- **ZigBee End Device (ZED):** Contains just enough functionality to talk to its parent node (either the coordinator or a router); it cannot relay data from other devices. It requires the least amount of memory, and therefore can be less expensive to manufacture than a ZR or ZC.

1.Zigbee Coordinator Node

- It is the root of network tree and a bridge to other network
- Able to store information about the network
- Only one ZCN for a network
- It act as a repositary for other security keys

2.The full Function Device

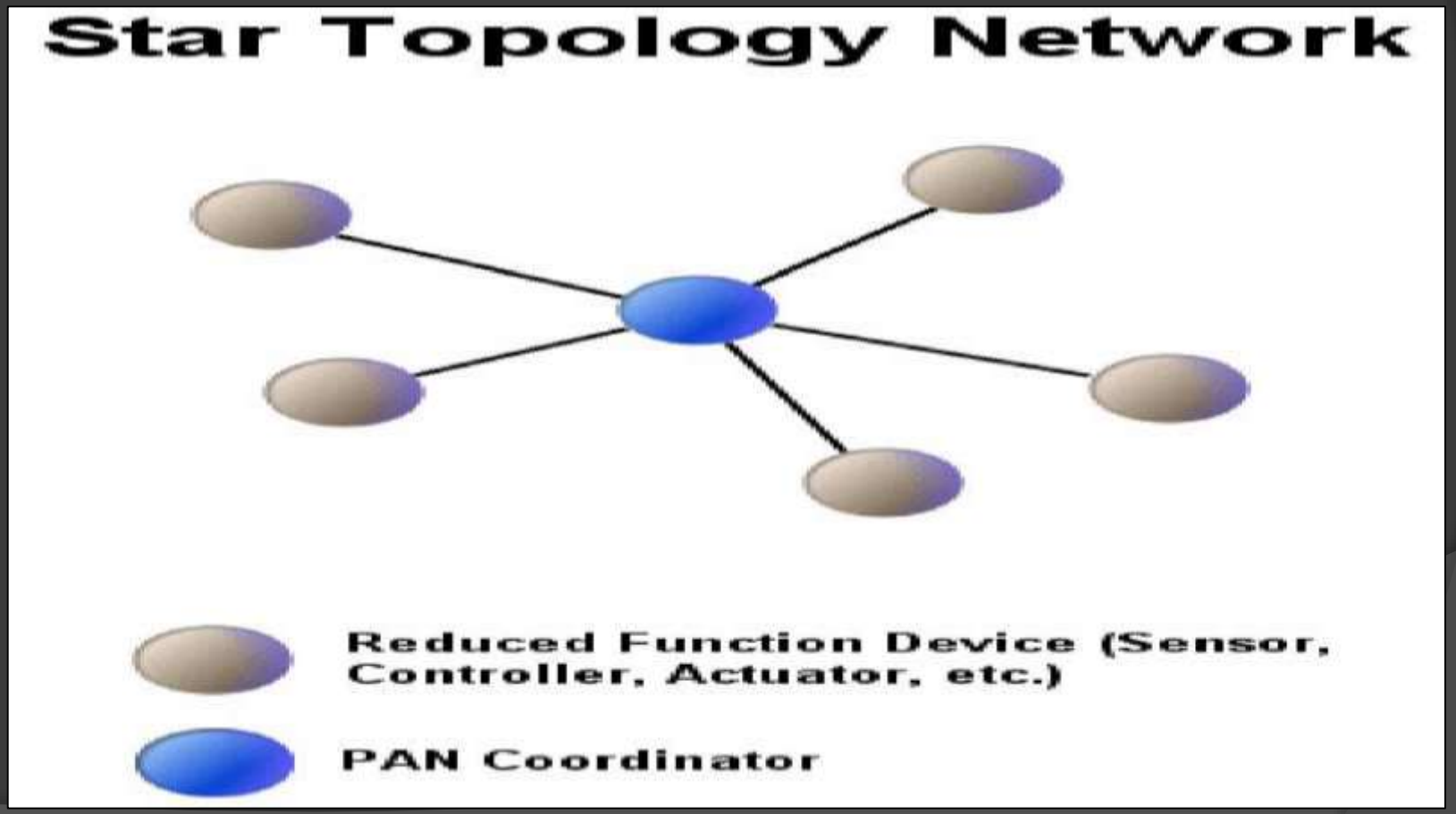
- An intermediatory router transmitting data from other devices
- Needs lesser memory than Zigbee coordinator node
- Lesser manufacturing cost
- Can operate on all topologies
- Also act as a coordinator

3.The Reduced Function Device

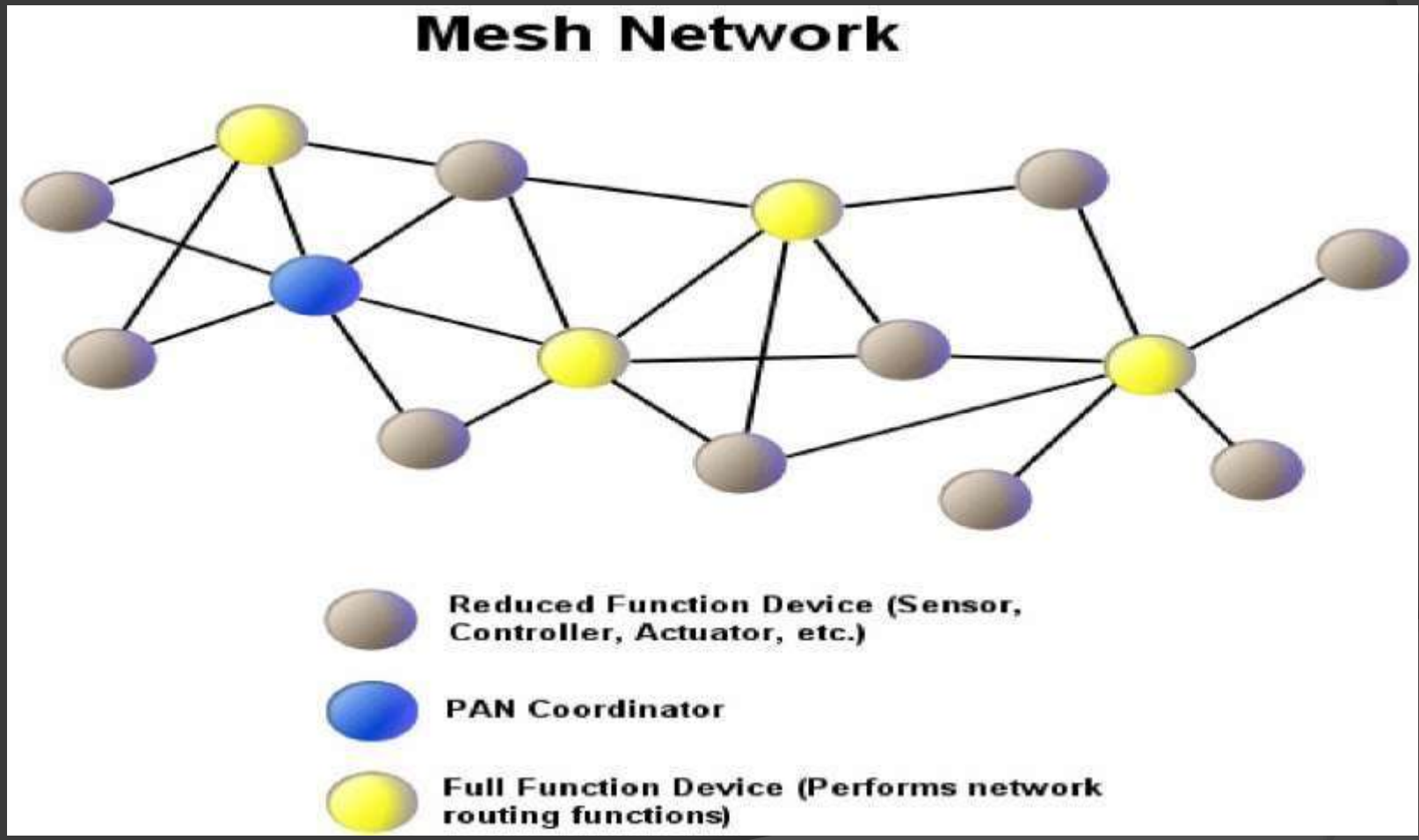
- Device capable of talking in the network
- It cannot relay data from other devices
- Less memory
- Cheaper than FFD
- It talks only to the n/w coordinator

NETWORK TOPOLOGIES

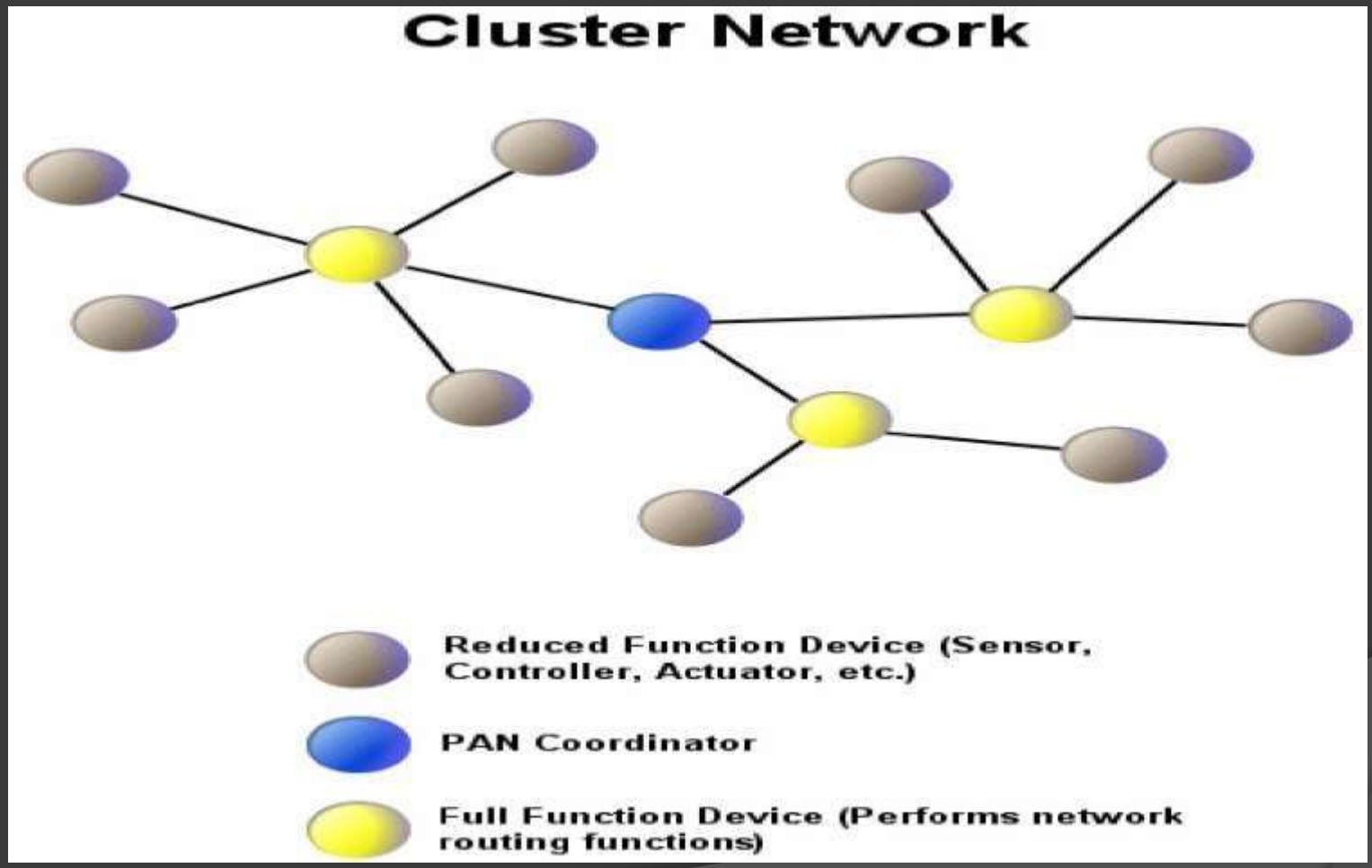
1.Star Topology



2.Peer-to-Peer Topology



3.Cluster Network



Characteristics

- Low power consumption with battery life ranging from months to years
- High density of nodes per network
- Low cost
- Simple implementation
- Low data rate
- Small packet devices

Applications

- Home Entertainment and Control
- Wireless sensor networks
- Industrial control
- Embedded sensing
- Medical data collection
- Smoke and intruder warning
- Building automation

Applications

- The ZigBee Alliance targets applications Across consumer, commercial, industrial and government markets worldwide
- Home networking
- Industrial control and management

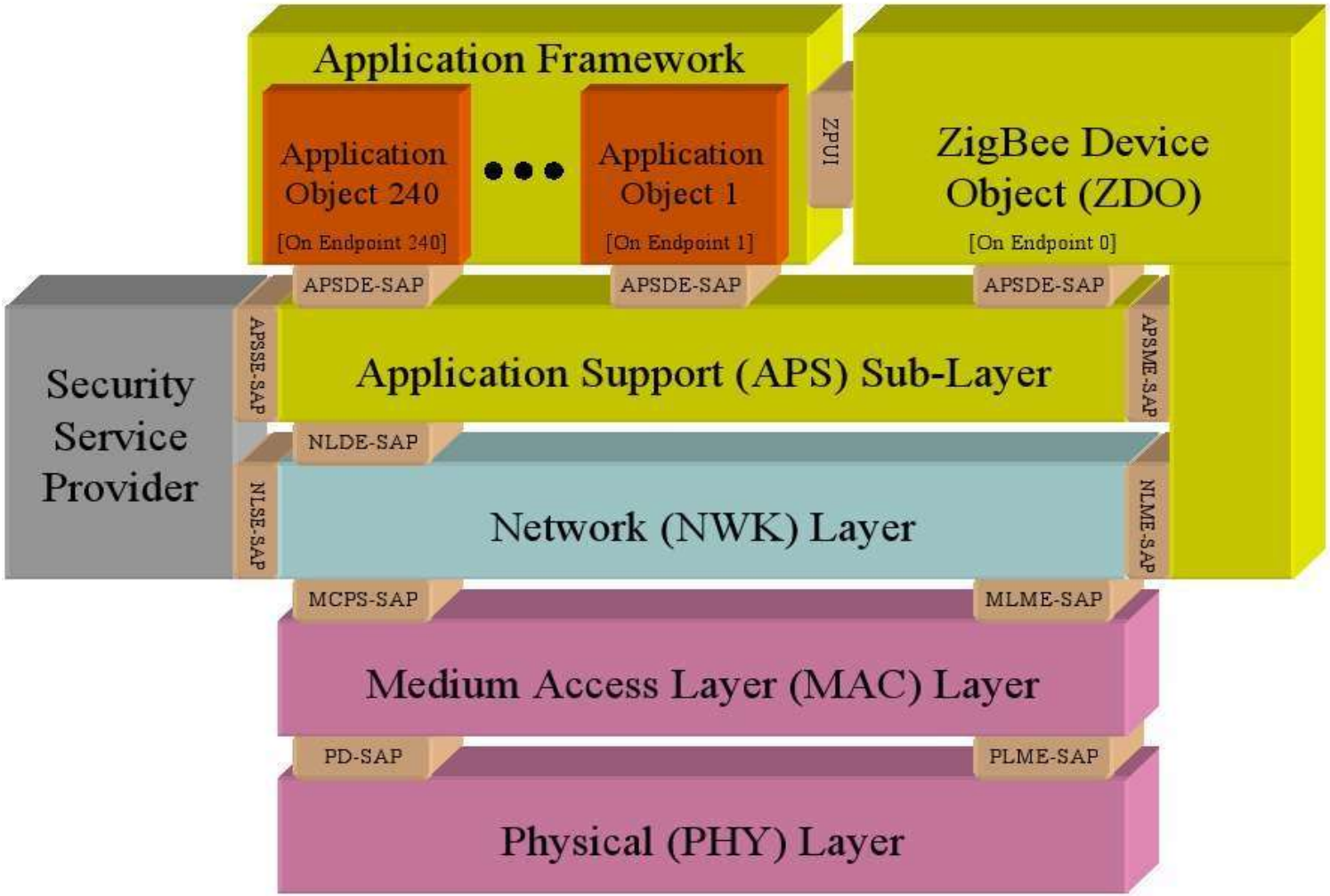
ADVANTAGES

- All Zigbee compliant appliances compatibly operate on the same network
- Setting up Zigbee wireless home management system is relatively inexpensive
- Ability to manage home appliance network remotely
- Eliminates dependence on Infrared device
- No central control point - dispersal of workload

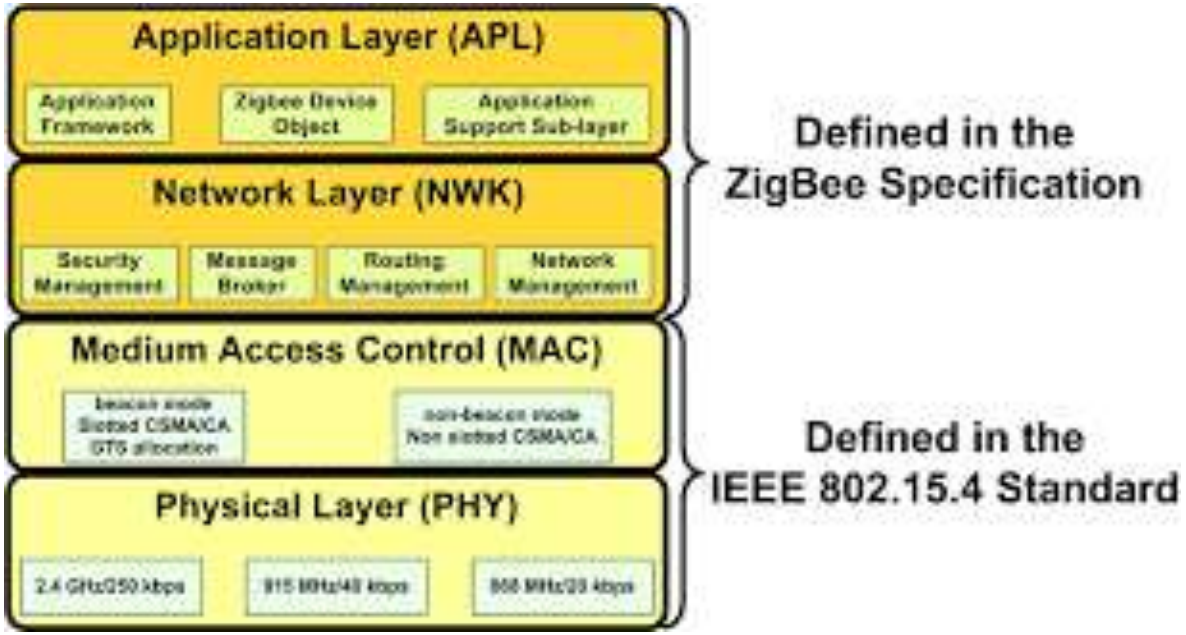
Conclusion

In future all devices and their controls will be based on this standard. Since Wireless personal Area Networking applies not only to household devices, but also to individualised office automation applications, ZigBee is here to stay. It is more than likely the basis of future home-networking solutions……

Zigbee Architecture



ZigBee Architecture



1. Physical Layer: This is the lowest protocol layer, and is responsible for controlling and activating the radio transceiver, and also for selecting the channel frequency and monitoring the channel. It is also responsible for communication with the radio devices. Communication of data or commands is done using Packets. Each PHY Packet consists of a Synchronization Header (SHR)(responsible for receiver synchronization), Physical Header (PHR)(contains information about Frame length) and PHY payload (provided by upper layers as a frame and includes data or command).
2. Medium Access Control or MAC n interface between the Physical layer and the Network layers. It is responsible for generation of Beacons and synchronization of devices in the Beacon enabled network. A MAC frame can be a Beacon Frame (used by Coordinator to transmit Beacons), Data Frame, Acknowledge Frame or a Command Frame. It consists of a MAC Header (contains information about security and addressing), Variable length size MAC Payload (contains data or command) and a MAC Footer (contains 16 bit Frame check sequence for data verification).
3. Network Layer: This layer connects the Application layer with the MAC layer. It manages the network formation and routing. It establishes a new network and selects the network topology. The NWK frame consists of the NWK Header and NWK Payload. The Header contains information regarding network level addressing and control. The NWK Payload contains the Application sublayer frame.
4. Application Support Sub Layer: It provides a set of services through two entities – Application SupportData Entity and Application Support Management Entity, to the application and network layers. These entities are accessed through their respective Service Access Points (SAP)
5. Application Layer: This is the highest layer in the network and is responsible for hosting the application objects which holds user applications and ZigBee Device Objects (ZDOs). A single ZigBee device can contain up to 240 application objects which control and manage the protocol layers. Each application object can consist of one application profile or program, developed by the user or the ZigBee alliance. The application profile is responsible for transmission and reception of data in the network. The type of devices and function of each device is defined in an application profile. The ZigBee Device Objects act as a interface between application objects, device profiles and the Application sub layer.

ZigBee Architecture

- Divided into three sections
- IEEE 802.15.4 which consists of MAC and physical layers
- ZigBee layers, which consist of the network layer, the ZigBee device object (ZDO), the application sublayer, and security management
- Manufacturer application: Manufacturers of ZigBee devices can use the ZigBee application profile or develop their own application profile

Network Layer

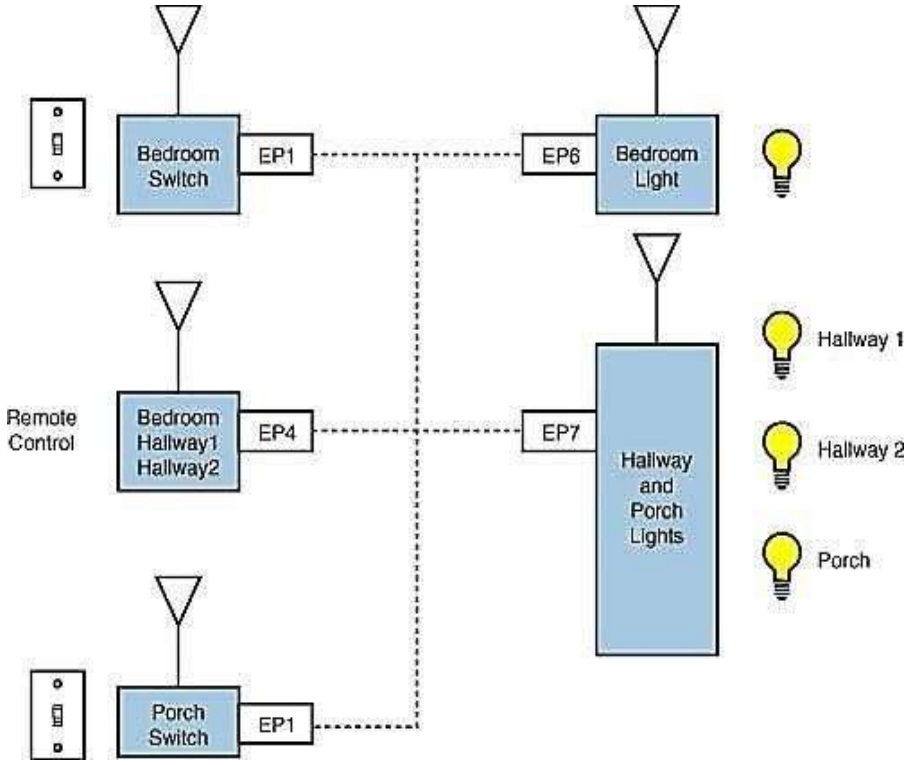
- Located between the MAC layer and application support sublayer
- Provides the following functions:
- Starting a network
- Managing end devices joining or leaving a network
- Route discovery
- Neighbor discovery

APS Layer

- Application Support Sublayer (APS)
- Provides services necessary for application objects (endpoints) and the ZigBee device object (ZDO)
- Some of services provided by the APS to the application objects for data transfer are
- Request
- Confirm
- Response

APS Layer

- Application Object (endpoint)
  - Defines input and output to the APS
  - For example, a switch that controls a light is the input from the application object, and the output is the light bulb condition



  - Each node can have 240 separate application objects

APS Layer

- ZigBee Device Object (ZDO)
- Control and management of application objects • Performs overall device management tasks:
- Determines the type of device in a network (for example, end device, router, or coordinator)
- Initializes the APS, network layer, and security service provider
- Performs device and service discovery
- Initializes coordinator for establishing a network
- Security management
- Network management

APS Layer

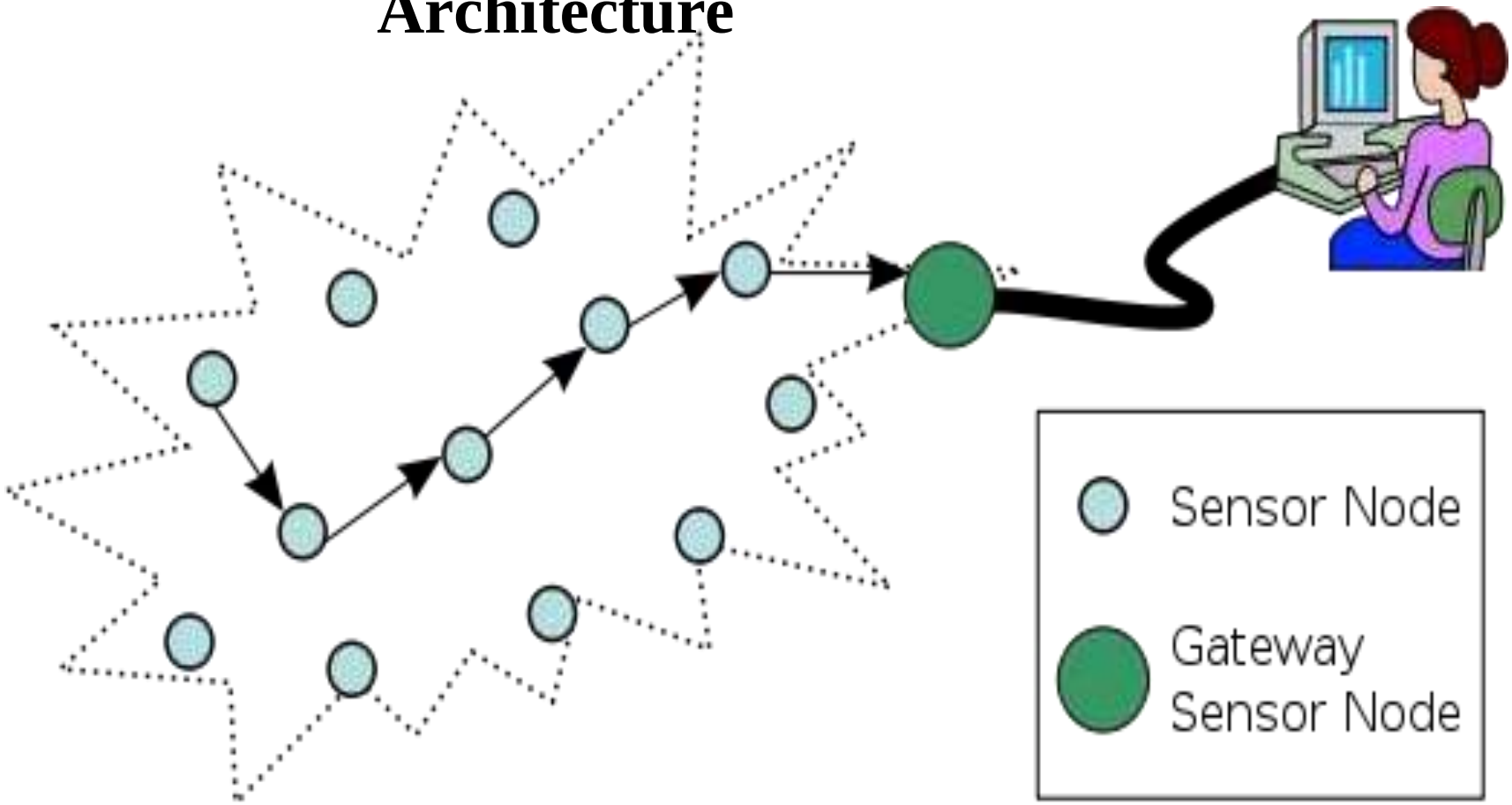
- End Node
- Each end node or end device can have multiple EPs
- Each EP contains an application profile, such as home automation
- can be used to control multiple devices or single device
- ZigBee Addressing Mode
- ZigBee uses direct, group, and broadcast addressing for transmission of information

Wireless Sensor Networks(WSN)

Wireless Sensor Networks(WSN)

- Even though wireless sensors has limited resources in memory, computation power, bandwidth, and energy.
- With small physical size. It Can be embedded in the physical environment.
- Self-organizing multi-hop ad-doc networks

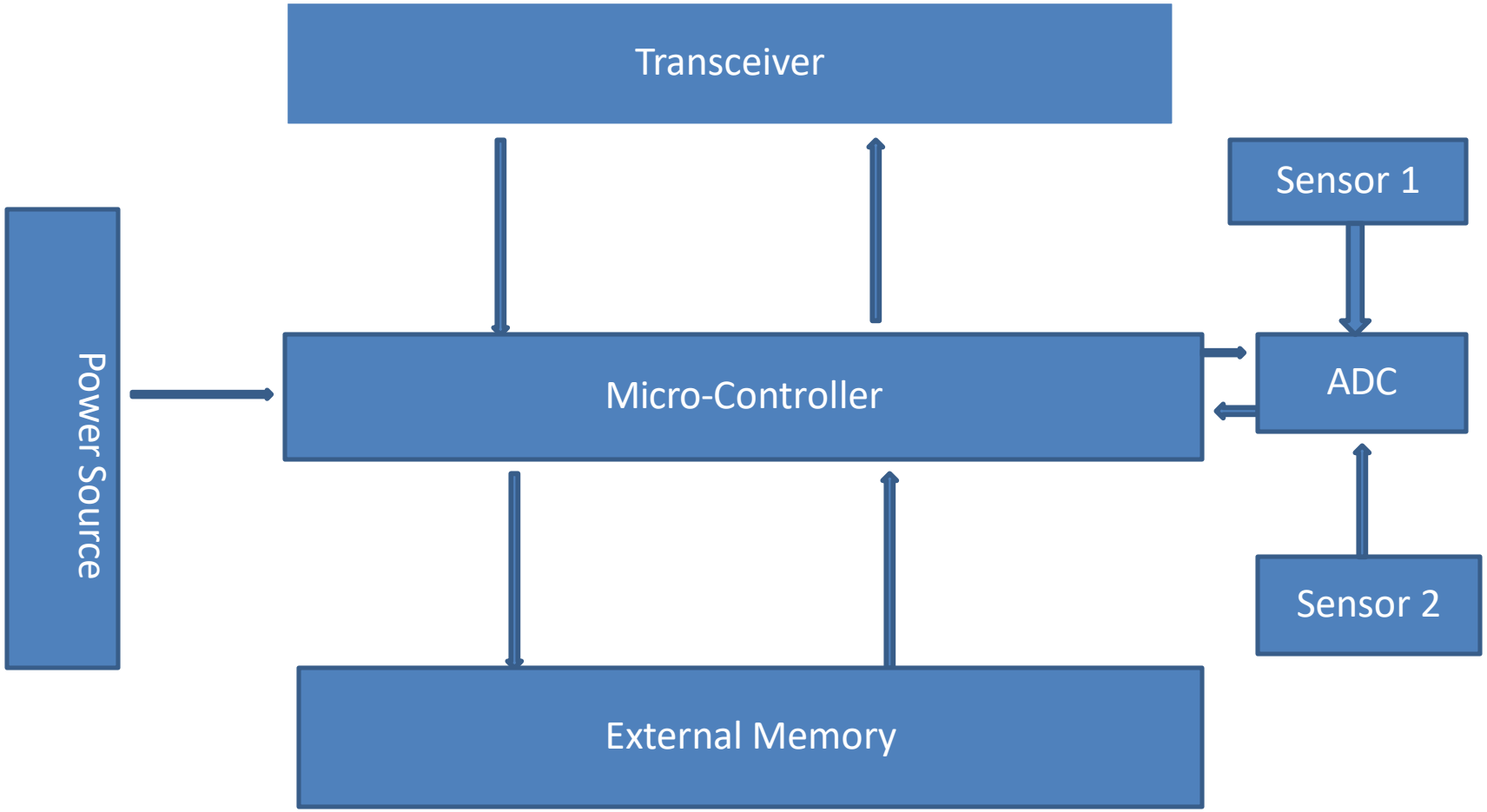
Wireless Sensor Network Architecture



Wireless Sensor Node

- sensor
  - A transducer
  - converts physical phenomenon e.g. heat, light, motion, vibration, and sound into electrical signals
- sensor node
  - basic unit in sensor network
  - contains on-board sensors, processor, memory, transceiver, and power supply
- sensor network
  - consists of a large number of sensor nodes
  - nodes deployed either inside or very close to the sensed phenomenon

Architecture of Sensor Node



Characteristics

- Power consumption constraints for nodes using batteries or energy harvesting
- Ability to cope with node failures (resilience)
- Mobility of nodes
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use
- Cross-layer design

Factors Influencing WSN Design

- Fault tolerance
- Scalability
- Production costs
- Hardware constraints
- Sensor network topology
- Environment
- Transmission media
- Power Consumption
  - Sensing
  - Communication
  - Data processing

Applications

- Military Applications
- Environmental Applications
- Health Applications
- Home and Office Applications
- Automotive Applications
- Other Commercial Applications

Advantages

- It avoids a lot of wiring .
- It can accommodate new devices at any time .
- It's flexible to go through physical partitions .
- It can be accessed through a centralized monitor

Disadvantages

- Lower speed compared to wired network.
- Less secure because hacker's laptop can act as Access Point. If you connected to their laptop, they'll read all your information (username, password.. etc).
- More complex to configure than wired network.
- Gets distracted by various elements like Blue-tooth .
- Still Costly at large.
- It does not make sensing quantities in buildings easier.
- It does not reduce costs for installation of sensors.
- It does not allow us to do more than can be done with a wired system

Design Challenges

- **Heterogeneity**
  - The devices deployed may be of various types and need to collaborate with each other.
- **Distributed Processing**
  - The algorithms need to be centralized as the processing is carried out on different nodes.
- **Low Bandwidth Communication**
  - The data should be transferred efficiently between sensors

Continued.

- **Large Scale Coordination**
  - The sensors need to coordinate with each other to produce required results.
- **Utilization of Sensors**
  - The sensors should be utilized in a ways that produce the maximum performance and use less energy.
- **Real Time Computation**
  - The computation should be done quickly as new data is always being generated.

Operational Challenges of Wireless Sensor Networks

- Energy Efficiency
- Limited storage and computation
- Low bandwidth and high error rates
- Errors are common
  - Wireless communication
  - Noisy measurements
  - Node failure are expected
- Scalability to a large number of sensor nodes
- Survivability in harsh environments
- Experiments are time- and space-intensive

Future of WSN

Smart Home / Smart Office

- Sensors controlling appliances and electrical devices in the house.
- Better lighting and heating in office buildings.
- The Pentagon building has used sensors extensively.

Conclusion

- WSNs possible today due to technological advancement in various domains
- Envisioned to become an essential part of our lives
- Design Constraints need to be satisfied for realization of sensor networks
- Tremendous research efforts being made in different layers of WSNs protocol stack

SCADA

Introduction

- What is SCADA?
- What is data acquisition?
- Where and why, use of SCADA?

Application area :

- **Industrial processes : chemical, power generation and distribution, metallurgy, …**
- **Nuclear processes : reactors, nuclear waste, …**
- **Experimental physics : HEP laboratories**

Application size:

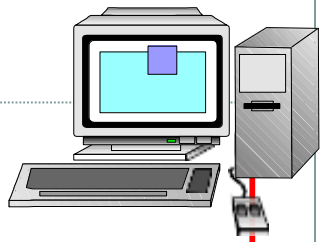
- **20 k I/O to 450 K I/O,**
- **1 M I/O under development**

SCADA ?

Supervisory Control

And

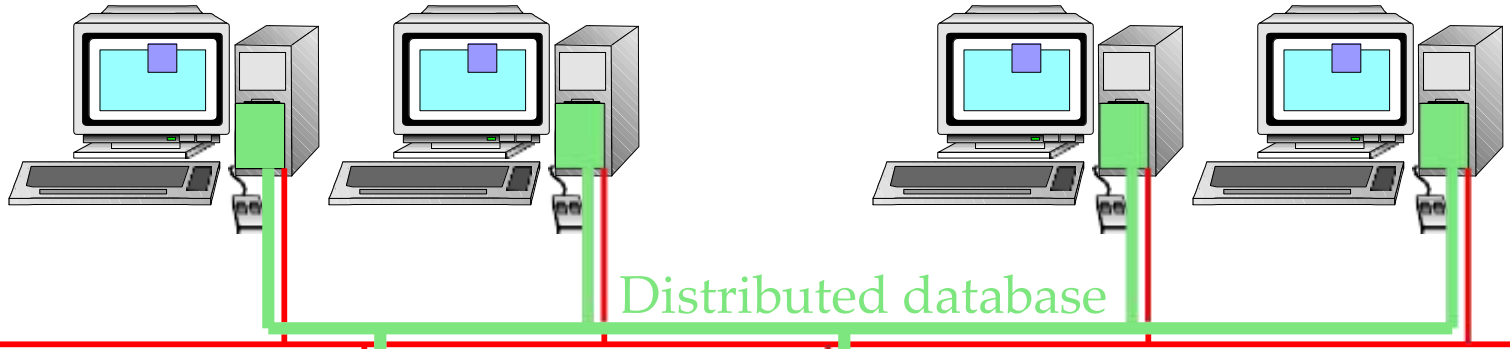
Data Acquisition



ERP Systems
Expert Systems

Graphics and Batch processing

Archiving, Logging,
Access Control, Alarms

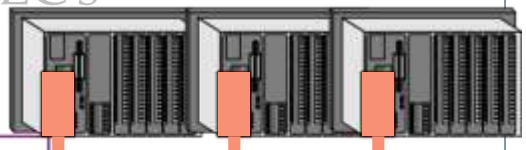


Distributed database

Data Server

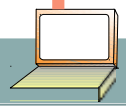
Data Server

PLC's



Field Bus

Control Programs



SCADA generations

- 1st generation (1970s). Co-located control
  - Controlled units were on the same site as the controlling computer with hard-wired connections between them
  - No network so no potential for external attack. Very limited chance of insider attack because operation by teams rather than individuals

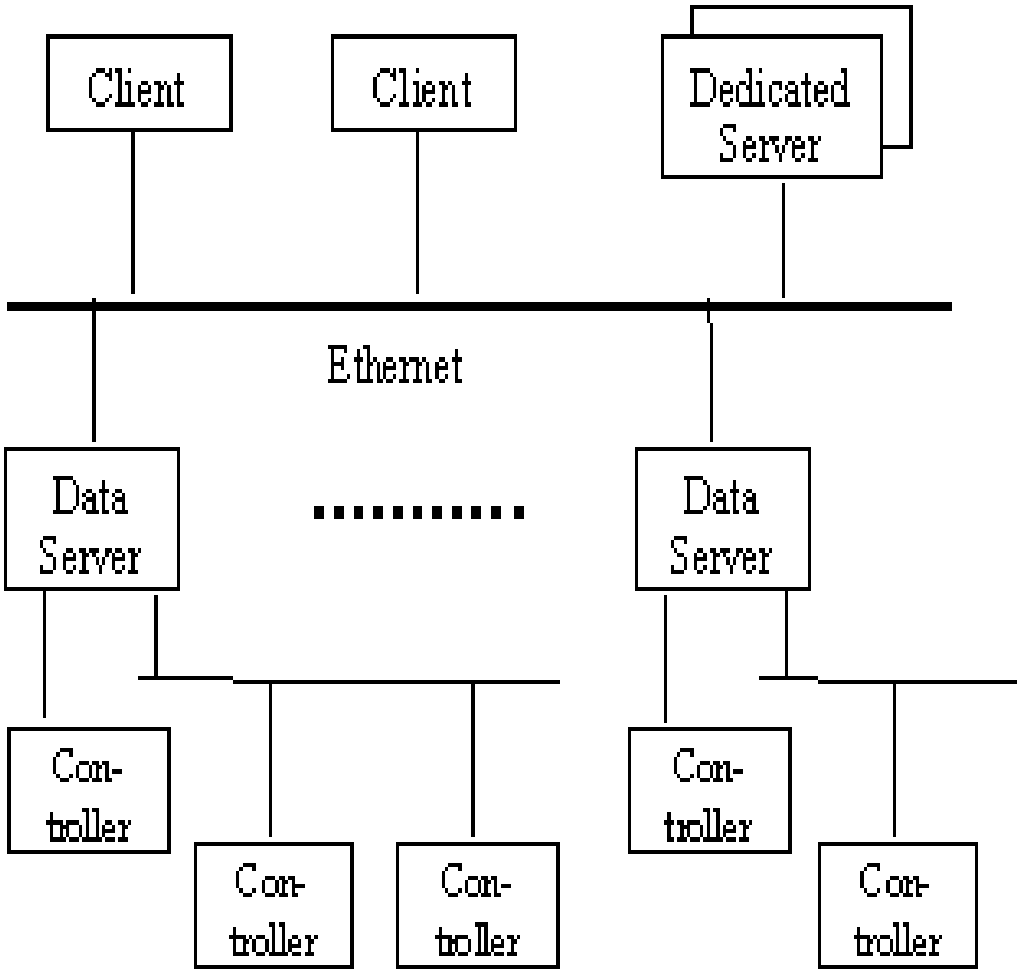
SCADA generations

- 2nd generation (1980s/90s) Distributed control
  - SCADA systems networked with devices using special-purpose protocols
  - No external network connection
  - Vulnerable to insider attacks because of distributed sites

SCADA generations

- 3rd generation (2000s). Networked systems
  - SCADA systems no longer isolated but connected to external networks
  - External connection through computers (particularly PCs) that are directly connected to the Internet
  - May also interface with other Internet-connected systems such as manufacturing control systems
  - More use of standard protocols such as TCP/IP for communications
  - Remote system monitoring and upgrades from providers requires network connection

Hardware Architecture



Typical Hardware Architecture

Functionality

- Generic SCADA functionality
  - Access Control,
  - Alarm Handling,
  - Logging, Archiving,
  - Report Generation,
  - Automation.

Functionality Contd..

- Access Control

  Users - allocated to groups

  group - defined read/write access

- MMI

  multiple screens

  library of standard graphical symbols

  dragged and dropped

  zooming, re-sizing, scrolling…

  Links - pages to navigate

Functionality Contd..

- Trending

  based on parameters on specific chart

  can be predefined or defined on-line

  more than 8 trended parameters per chart

  both real-time and historical trending

  zooming and scrolling

- Alarm Handling

  based on limit and status checking

  handled centrally

  E-mails can be generated

Functionality Contd..

- Logging, Archiving

  Data stored in compressed and proprietary format

  Logging / Archiving either for a set number of parameters or for a set period of time

  Logging / Archiving can be frequency or event driven * Logging of user actions together with a user ID

  VCR facility for playback of stored data Writing logs into RTDB

- Report Generation

  Reports created using SQL type queries to the RTDB or logs

  Automatic generation, printing and archiving of reports

  Use of 'components' for report generation

Functionality Contd..

- Automation

  triggered by events

  defined in scripting languages

  send e-mail ,write into RTDB

  recipes

  Sequencing

RFID

Radio Frequency Identification

What is RFID?

- Radio Frequency Identification is an identification system used for retail and wholesale, security, veterinary, and military purposes. The RFID technology sector is growing rapidly as new uses for it are found.

- Technology used to track and identify a person or object by means of radio transmission

- RFID systems can be either active or passive.

- You may be surprised to find that you have been using RFID technology for years without knowing it.

How does RFID work?

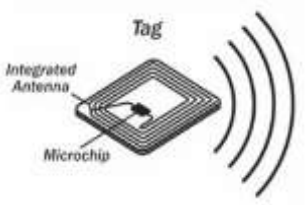
Three main components to a basic RFID system:

- RFID Tag (transponder)
- Antenna
- RFID Reader (Interrogator)

How does RFID work?

RFID Tag (Transponder)

- Consists of a microchip and an antenna
- Attached to an object to be tracked (vary in size)
- Stores information about the object (ID number, kilobytes, dynamic info maintained)
- Read only or read/write
- Contact-less, Non-line of sight
- Read Range: few inches to hundreds of ft.



How does RFID work?

Two classes of RFID Tags, Passive and Active, based on the means in which they receive power:

- Passive
  - ✓ Power source is provided by the RFID Reader's generated field
  - ✓ Smaller size tags, must be within close range of reader (~ 2m)
- Active
  - ✓ Have an internal power source
  - ✓ Larger, more expensive, shorter life
  - ✓ Longer reading ranges, more memory

How does RFID work?

Antenna

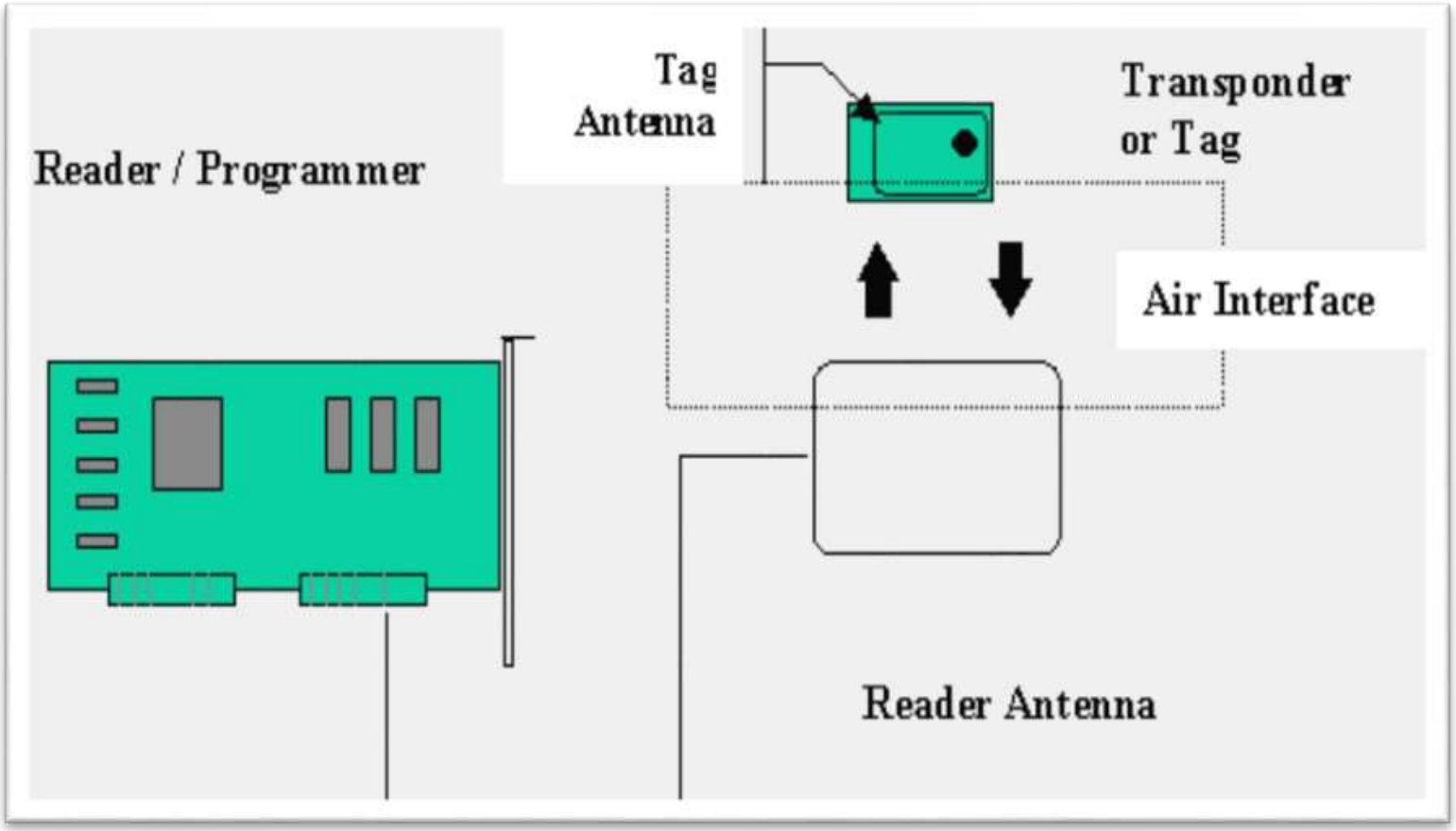
- An antenna (or aerial) is an electrical device which converts electric power into radio waves, and vice versa. It is used for communication between reader and tags.

How does RFID work?

RFID Reader (Interrogator)

- Retrieves information from the RFID Tag
- Detects/Activates tag, reads and writes data to tag
- May consist of a signal processor, operating system, antenna, virtual memory, and transmitter/receiver unit
- Active or Passive

How does RFID work?



Active RFID

- Active RFID devices are RF tags with an attached power supply. These tags emit a signal whether or not there is an antenna in the vicinity to receive the data.

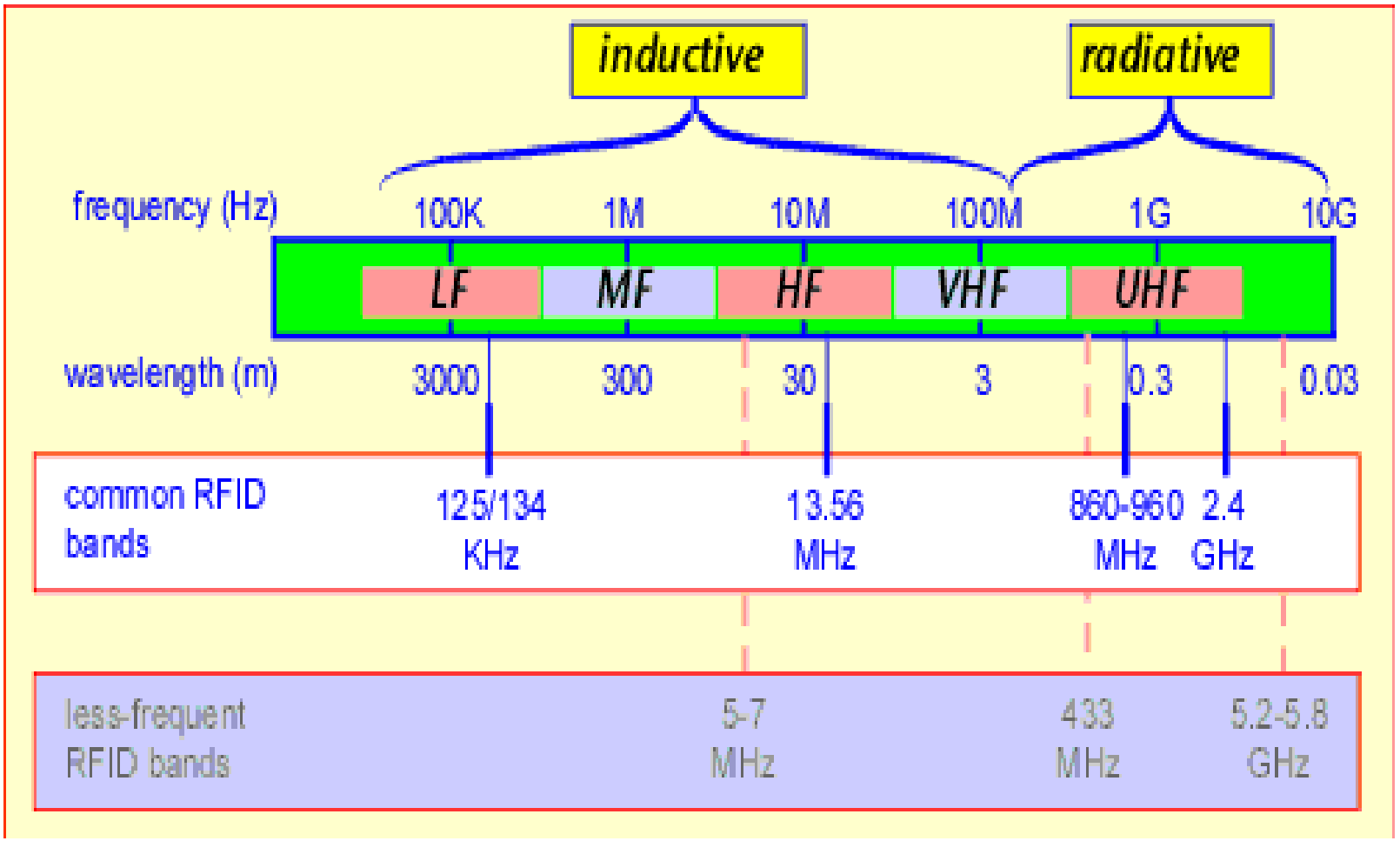
Passive RFID

- Passive RFID devices are RF tags that do not have an attached power supply. The passive RF tags receive their power when it is emitted from active antennas in close proximity.

Passive RFID tags generally operate at distinct frequencies:

- Low Frequency (LF) 125 -134 kHz
- High Frequency (HF) 13.56 MHz
- Ultra High Frequency (UHF) 856 MHz to 960 MHz

Frequency


inductive
radiative
frequency (Hz)
100K
1M
10M
100M
1G
10G
LF
MF
HF
VHF
UHF
wavelength (m)
3000
300
30
3
0.3
0.03
common RFID bands
125/134 KHz
13.56 MHz
860-960 MHz
2.4 GHz
less-frequent RFID bands
5-7 MHz
433 MHz
5.2-5.8 GHz

Advantages

- An RFID system is the noncontact, non-line-of- sight nature of the technology.
- It enhance Efficiency ,traceability of production.
- Hundred of tags can be read in seconds.
- They can be combined with sensors.
- It not only saves time but also provides real time information & data access to anybody.
- RFID tags can store a lot of information, and follow instructions
- Has the ability to pinpoint location
- Reliability.

Disadvantages

- Active RFID can be expensive because of batteries.
- There still needs to be regulations about RFID guidelines.
- There is a privacy concern towards RFID devices, for example some claim that Wal-Mart is infringing on natural rights by overseeing what customers buy.
- RFID may be easily intercepted, even if it is Encrypted.
- It takes a lengthy time to program RFID devices
- Any body can access information about anything.
- It is possible to compromise an RFID system by wrapping the protected material in two to three layers of ordinary household foil to block the radio signal.

Applications

RFID tags come in a wide variety of shapes and sizes; they may be encased in a variety of materials:

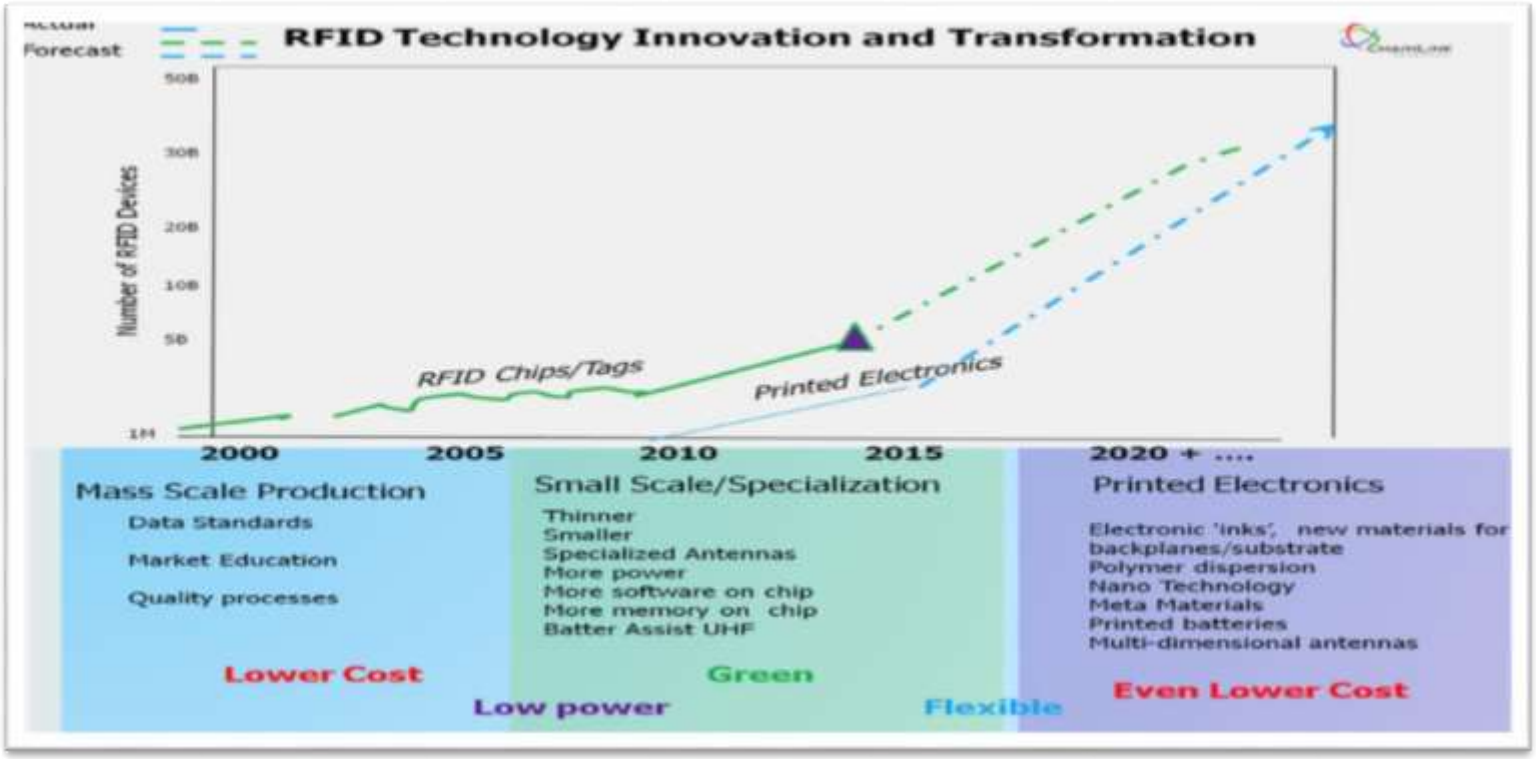
- Animal tracking tags, inserted beneath the skin, can be rice-sized.
- Tags can be screw-shaped to identify trees or wooden items.
- Credit-card shaped for use in access applications.
- The anti-theft hard plastic tags attached to merchandise in stores are also RFID tags.
- Heavy-duty 120 by 100 by 50 millimeter rectangular transponders are used to track shipping containers, or heavy machinery, trucks, and railroad cars.

Applications

- Use RFID if you want to wirelessly identify something without line of sight.
- Use RFID if you want a computing device but not humans to see the ID.
- Use in tracking assets, people, documents, car or any important thing which wanted to be tracked.
- Airport Security/Baggage: Track and identify passengers and airline luggage
- Medical: Restricting access; tracking patients and guests with authorized wristbands; tracking babies (to reduce risk of abduction); tracking of medicine and equipment;
- Postal Services: Tracking of mail/packages

Future of RFID

- The future of electronics, RFID and antennas is quite interesting.1 Material innovations in organic polymers, Nano technology, meta materials; and innovations in processing such as advances in photolithography, electron-beam lithography, direct laser/optical lithography, electrophoretic; new battery/power technologies—the whole area of printed electronics on organic new material, cloth and paper, all are in motion to step by step transform the semiconductor world. More flexible and cheaper production will enable a new generation of RFID growth.



Conclusion

- It is an another TECH REVOLUTION which will change our lives completely And it will be used 24/7days.
- The billion dollar industry that RFID has evolved into has done great good for a lot of different fields. RFID has given doctors the ability for quick access to patients records, the assurance of accounted merchandise for small business and large alike, and the government the ability to conduct taxes for tolls in this technological day and age. But with as many benefits as it has, Radio Frequency Identification's overwhelming credibility is balanced out by the criticism against it. Though RFID allows for the allocation and distribution of sensitive information, if that information is compromised, the effects could be devastating. For there to be order in the realm of RFID, legislation and guidelines need to be set up and enforced to ensure the integrity and confidence of the data being communicated, which will in turn help Radio Frequency Identifications emerge as more secure and advanced.

M2M Technology

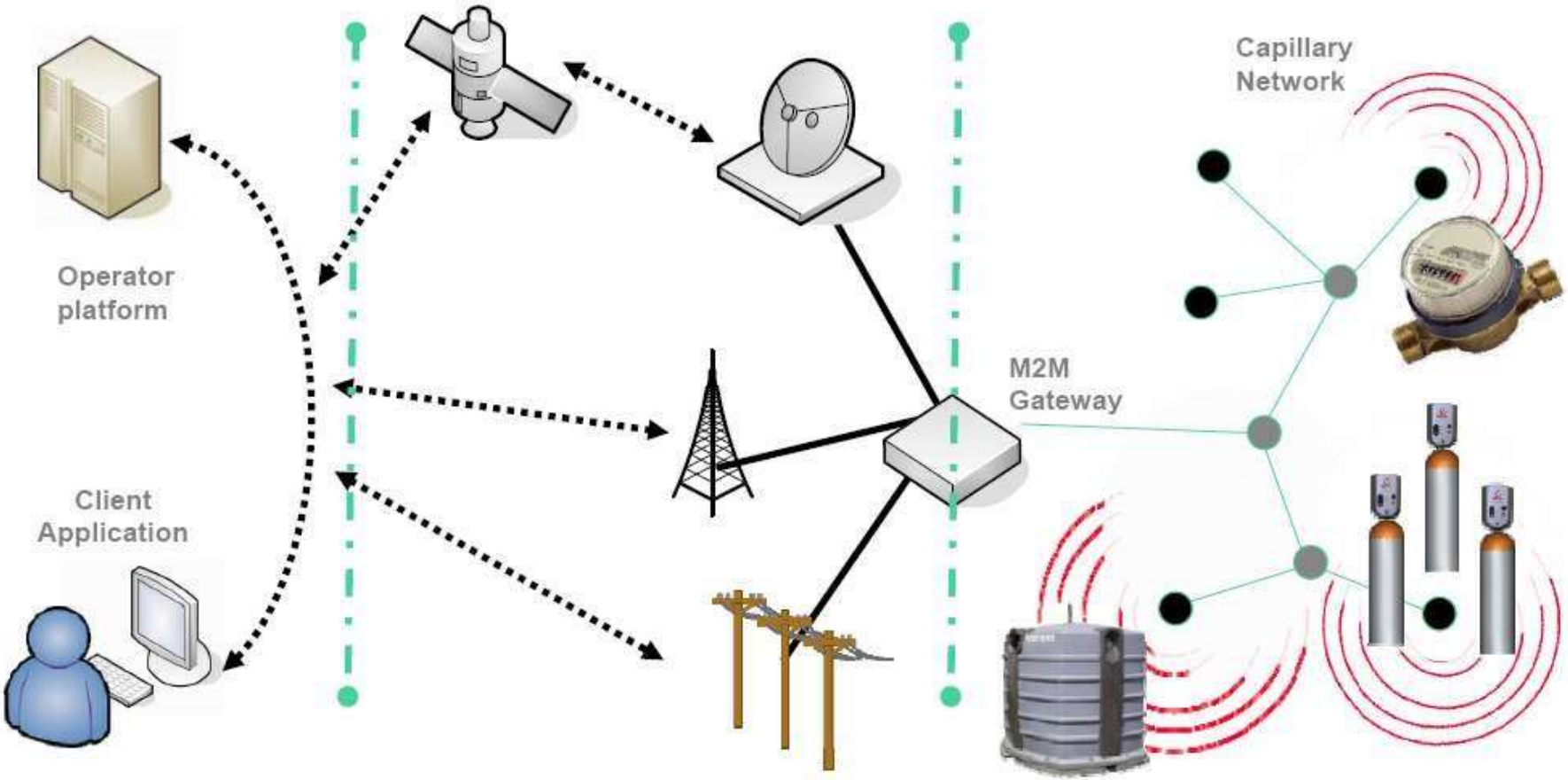
What is M2M ?

thout, or with only human intervention.

2M is a new business concept originating from the telemetry technology.

2M is based on very common used technologies – wireless sensors,
bile networks and the Internet.

Architecture



Contd…

Explanation

4 basic stages that are common to most M2M based applications:

- Collection of data;
- Transmission of data through a communication network;
- Assessment of data;
- Response to the available information;

Architecture

- M2M devices reply to requests for data contained within them or transmit the data automatically.

- M2M devices may constitute an M2M area network, which can be realised as, e.g. a Bluetooth based personal area network of body sensors. M2M gateway provides interconnection of M2M devices and forwards data collected from them to communications network.

- The communication network serves as infrastructure for realising communication between M2M gateway and M2M end-user application or server.

Contd...

For this purpose cellular network, telephone lines and
communication satellites can be used.
There are several means of sending data over the cellular network, such as CDMA and GPRS.
(Advantage of cellular data services is the ability to send large amounts of data frequently).

Finally, when data reach an M2M application, they can be analysed.

M2M Access Networks

Wired Solution – dedicated cabling between sensor gateway

PROS: very, very reliable; very high rates, little delay, secure

CONS: very expensive to roll out.

Wireless Capillary Solution – shared short-range link/network.

PROS: cheap to roll out, generally scalable, low power

CONS: short range, multi-hop not a solution, low rates, weaker security, lack of universal coverage

Wireless Cellular Solution – dedicated cellular link

PROS: excellent coverage, mobility, roaming, generally secure

Cons: expensive operate, not cheap to maintain, not power efficient

How does it Work ?

When machines “talk” they do so in a language known as “Telemetry”. The concept of telemetry – remote machines and sensors collecting and sending data to a central point for analysis, either by humans or computers.

Making a machine-to-machine communications system work is a step-by-step process. The main elements involved are **sensors** (usually the kind that can send telemetry wirelessly), **a wireless network** and a computer connected to the **Internet**.

Contd...

Lets take the case of Water Treatment Faciltiy

City engineers are charged with supplying the community with fresh drinking water. They need to monitor the raw water supply, the treatment process and the end product, which is drinkable water.

Water Treatment Facility

Firstly

- the engineers would place sensors in strategic locations. This includes placing sensors that can detect contaminants near or around the raw water supply, such as a lake or river

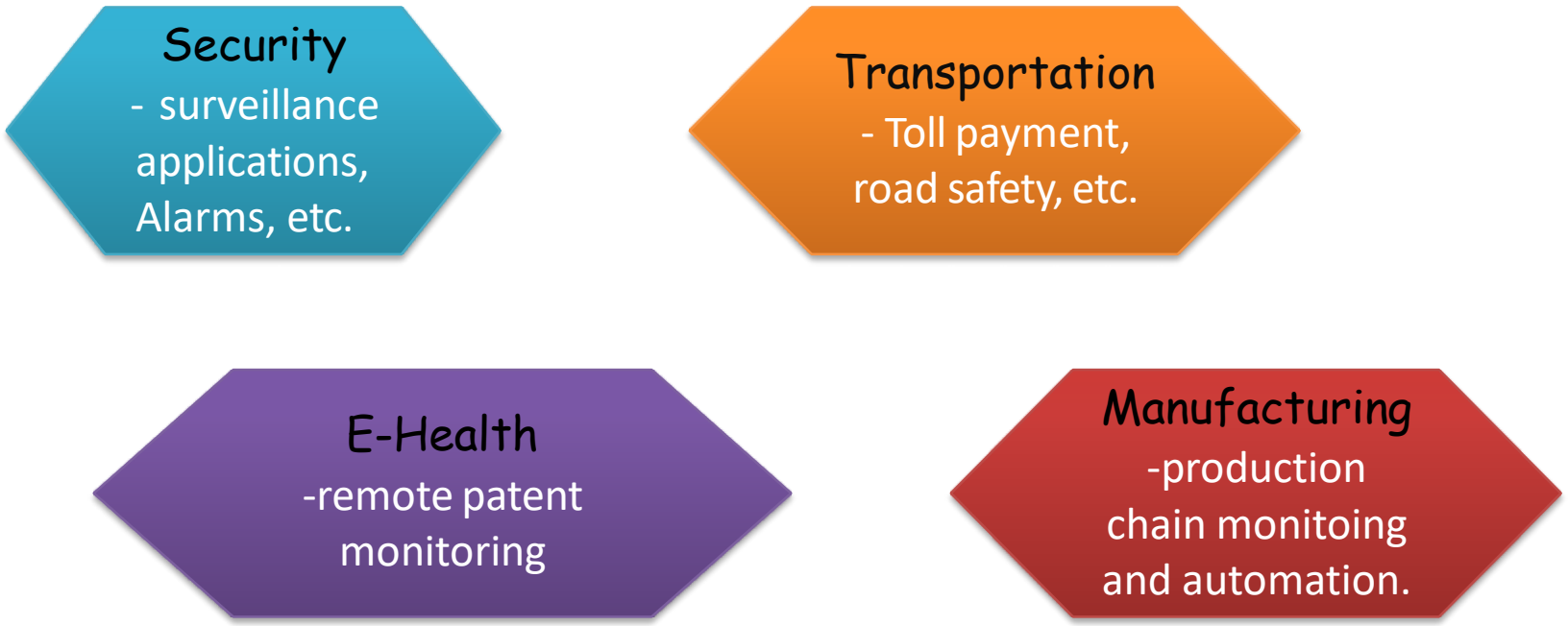
Secondly

- These sensors will send real-time data to a wireless network, which connects to the Internet. Engineers then monitor this incoming streaming data using computers loaded with specialized software.

Finally

- engineers can monitor the outflow water to ensure their treatment process is indeed resulting in high quality drinking water for the community.

Applications



Applications - eHealth

Disease Management

Ageing independently

Personal Fitness

Remote Monitoring

Health Check

On-line health records

Applications - Automotive

Use Cases for Automative applications

Automative applications integration in M2M platform

Applications - Avoid Road Accidents

The possibilities for M2M communications seem virtually limitless. But one of the areas where M2M holds potential for the most transformative change is the automotive industry. The ability to share realtime information with a vehicle opens the door for a broad range of new and exciting applications that will make driving safer, more convenient, and more efficient.

An exciting area within M2M is the work going on within vehicular networks, including new work on vehicle-to-vehicle (V2V) communications.

V2V Communication

Wireless technology allows connected vehicles to communicate with one another, as well as the infrastructure around them and alert motorists of road conditions. Drivers can be alerted to dangerous road conditions, possible collisions, and hazardous curves using vehicle systems based on Dedicated Short Range Communications (DSRC). DSRC is a technology similar to Wi-Fi and connected vehicles could also "talk" or provide the driver with information regarding tolls, work zones, traffic signals, and school zones, giving relief to delays and other surprises that motorists face.

Benefits of V2V

Benefits of V2V communication technologies could be endless. A study by the NHTSA stated that connected vehicle technology could handle roughly 80% of crash scenarios involving non-impaired drivers.

Contd…

Wireless Connectivity allows cars to be continuously aware of each other so when one car brakes suddenly cars several yards behind the vehicle get a safety warning before they get too close

Contd…

Connected vehicles can help to mitigate crashes on busy urban streets.

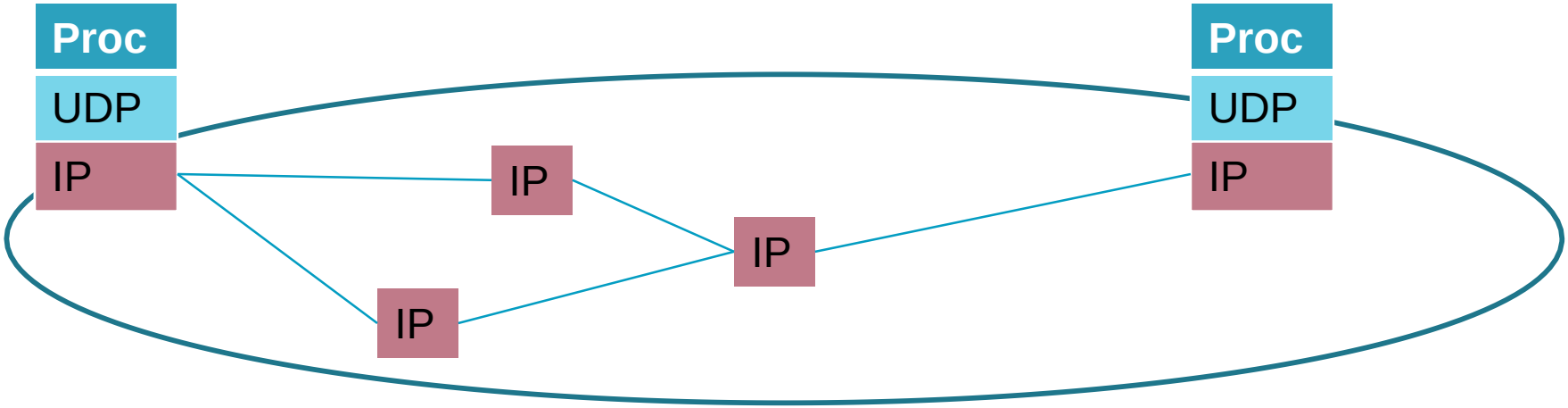
USER DATAGRAM PROTOCOL(UDP)

TCP vs UDP

The main difference between TCP (transmission control protocol) and UDP (user datagram protocol) is that TCP is a connection-based protocol and UDP is connectionless. While TCP is more reliable, it transfers data more slowly. UDP is less reliable but works more quickly. This makes each protocol suited to different types of data transfers.

USER DATAGRAM PROTOCOL(UDP)

- Layer 4 (Transport Layer) protocol
  - Runs over IP
  - Unreliable i.e. Best Effort service
    - UDP segments may be:
      - lost
      - delivered out of order
  - Connectionless
    - no handshaking between UDP sender, receiver
    - each UDP segment handled independently of others



- Provides a *lossy* connection (data may vanish).

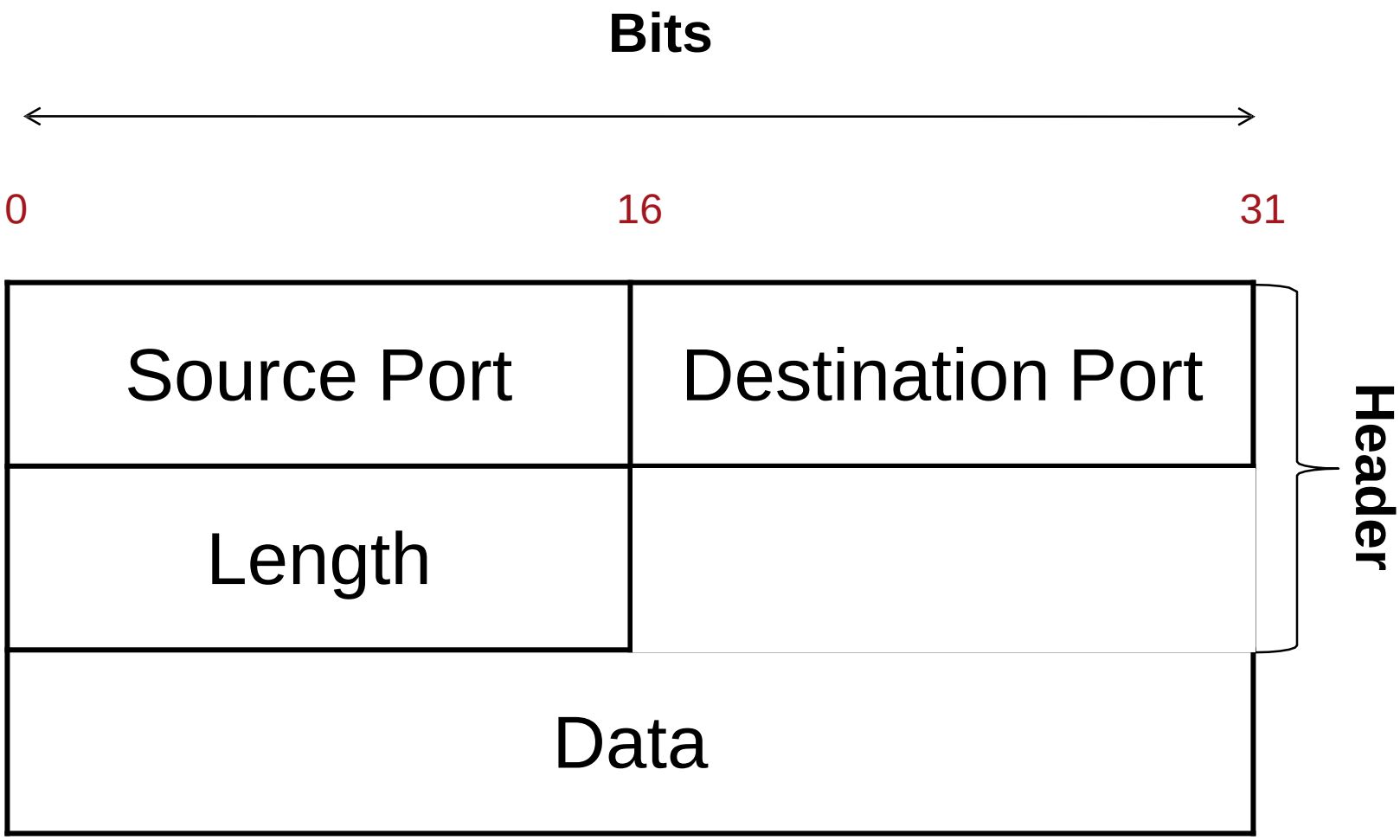
UDP FUNCTION

- Demultiplexing
  - UDP can support multiple applications in the same end systems.
    - Such as:
      - DNS
      - Management (ex. SNMP)
      - Distributed File System Support (ex. NFS)

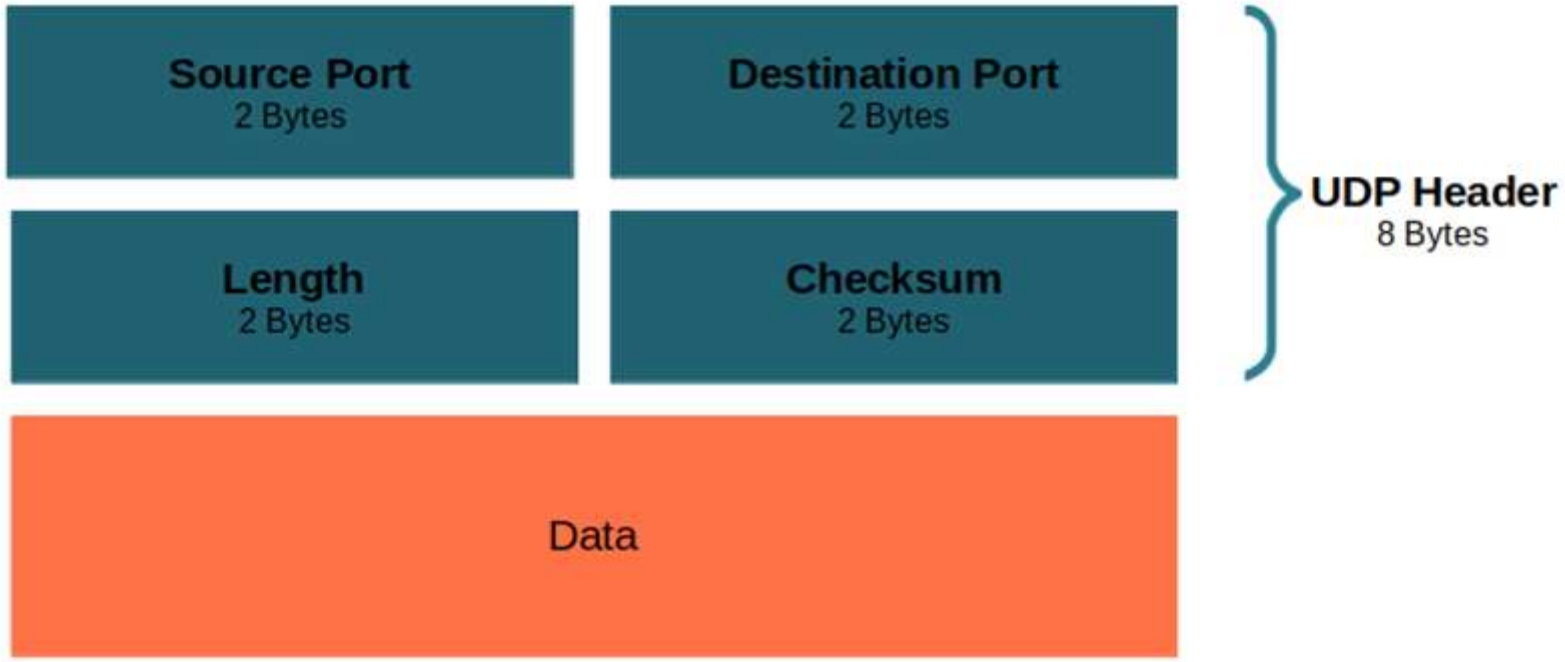
UDP is intended for simple applications

UDP DATAGRAM

8 Bytes Header + Variable Payload



UDP: The Header



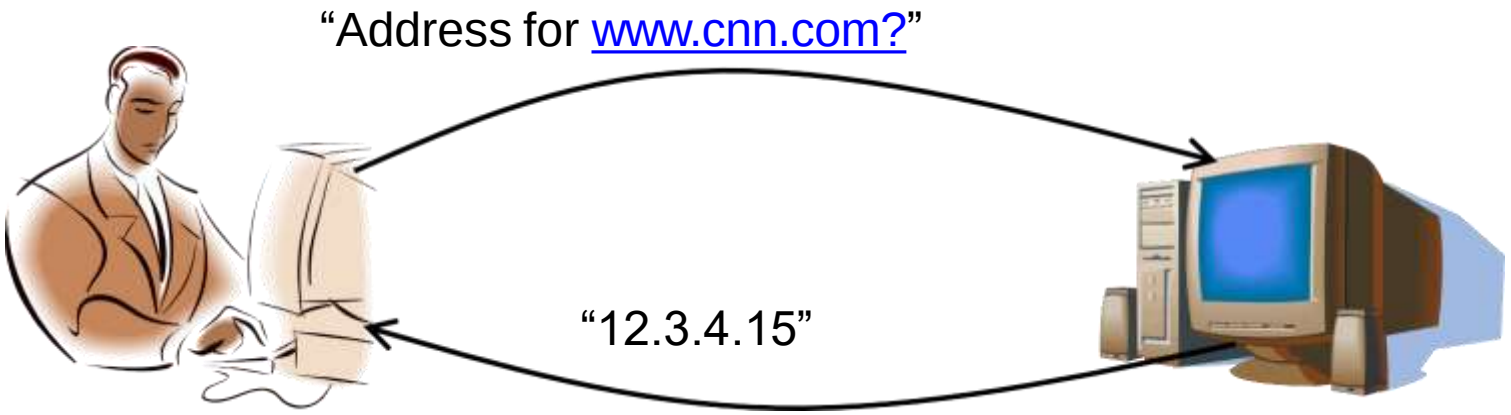
WHY WOULD ANYONE USE UDP?

- UDP is light weight protocol :
  - **No** delay for **connection establishment**
    - UDP just blasts away without any formal preliminaries
    - … which avoids introducing any unnecessary delays
  - **No connection state**
    - No allocation of buffers, parameters, sequence #s, etc.
    - … making it easier to handle many active clients at once
  - **Small packet header overhead**
    - UDP header is only eight-bytes long

POPULAR APPLICATIONS THAT USE UDP

- **Multimedia streaming**
  - Retransmitting lost/corrupted packets is not worthwhile
  - By the time the packet is retransmitted, it's too late
  - E.g., telephone calls, video conferencing, gaming

- **Simple query protocols like Domain Name System**
  - Overhead of connection establishment is overkill
  - Easier to have application retransmit if needed



Security Requirements
IOT Security

- Fundamental idea - IoT will connect all objects around us to provide smooth communication
- Economic of scale in IoT presents new security challenges for global devices in terms of
  - Authentication
  - Addressing
  - Embedded Security

Security Requirements
IOT Security

- Devices like RFID and sensor nodes have no access control functionality
- Can freely obtain or exchange information from each other
- So authentication & authorization scheme must be established between these devices to achieve the security goals for IoT

Security Requirements

- Privacy of things and security of data is one of the key challenges in the IoT
- Unauthorized Access
  - One of the main threats is the tampering of resources by unauthorized access
  - Identity-based verification should be done before granting the access rights
- Information corruption

Security Requirements

- Device credential must be protected from tampering
- Secure design of access rights, credential and exchange is required to avoid corruption

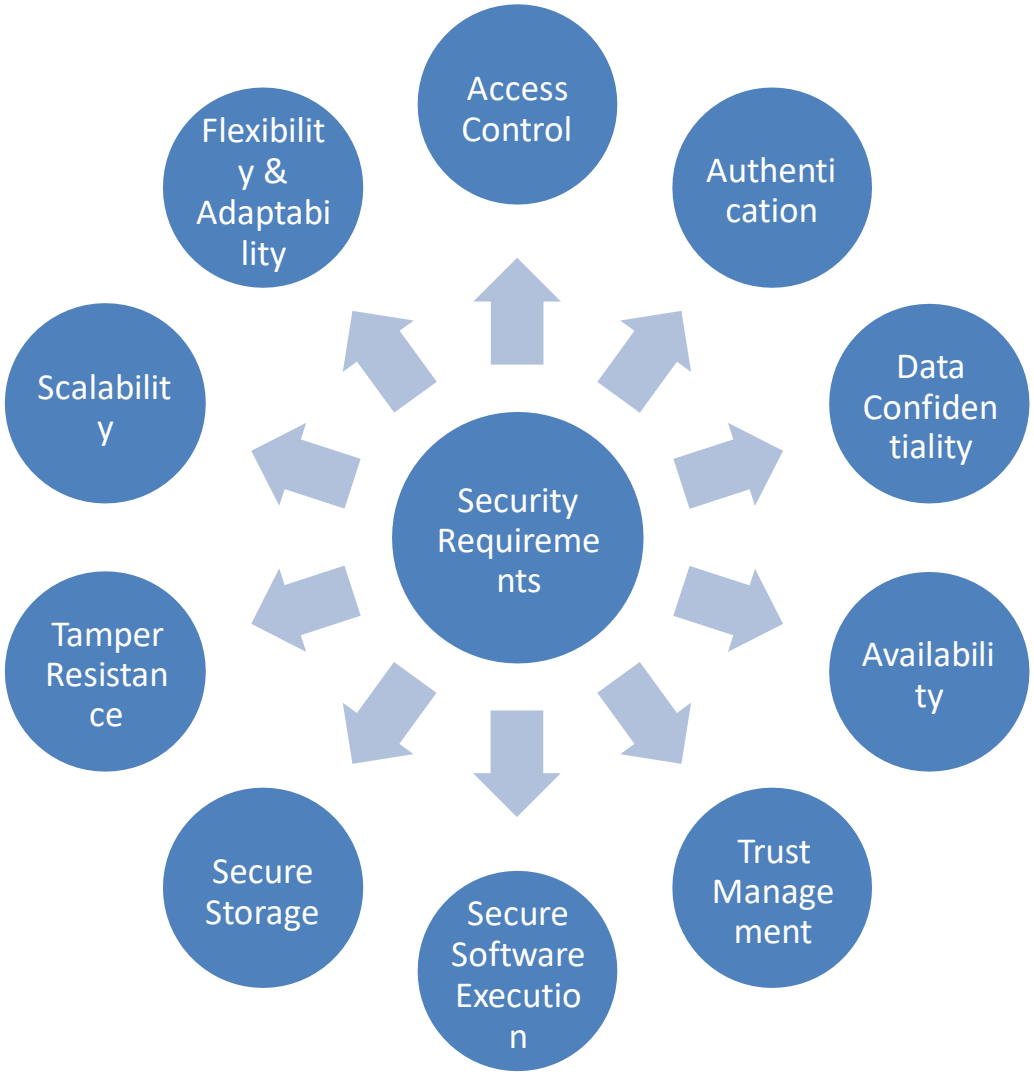
- Theft of Resources
  - Access of shared resources over insecure channel causes theft of resources
  - Results into man-in-the-middle attack
- Information Disclosure
  - Data is stored at different places in different forms

Security Requirements

- Distributed data must be protected from disclosure
- Context-aware access control must be enforced to regulate access to system resources

- DoS Attack
  - Denial of Service (DoS)
  - Makes an attempt to prevent authentic user from accessing services which they are eligible for
  - For example, unauthorized user sends to many requests to server

Security Requirements



Security Requirements

- Access Control
  - Provides authorized access to network resources
  - IoT is ad-hoc, and dynamic in nature
  - Efficient & robust mechanism of secure access to resources must be deployed with distributed nature
- Authentication
  - Identity establishment b/w communicating devices

Security Requirements

- Due to diversity of devices & end users, an attack resistant and lightweight solution for authentication

- Data Confidentiality
  - Protecting data from unauthorized disclosure
  - Secure, lightweight, and efficient key exchange mechanism is required

- Availability

Security Requirements

- Ensuring no denial of authorized access to network resources

- Trust Management
  - Decision rules needs to be evolved for trust management in IoT
- Secure Software Execution
  - Secure, managed-code, runtime environment designed to protect against different applications
- Secure Storage

Security Requirements

- Involves confidentiality and integrity of sensitive information stored in the system

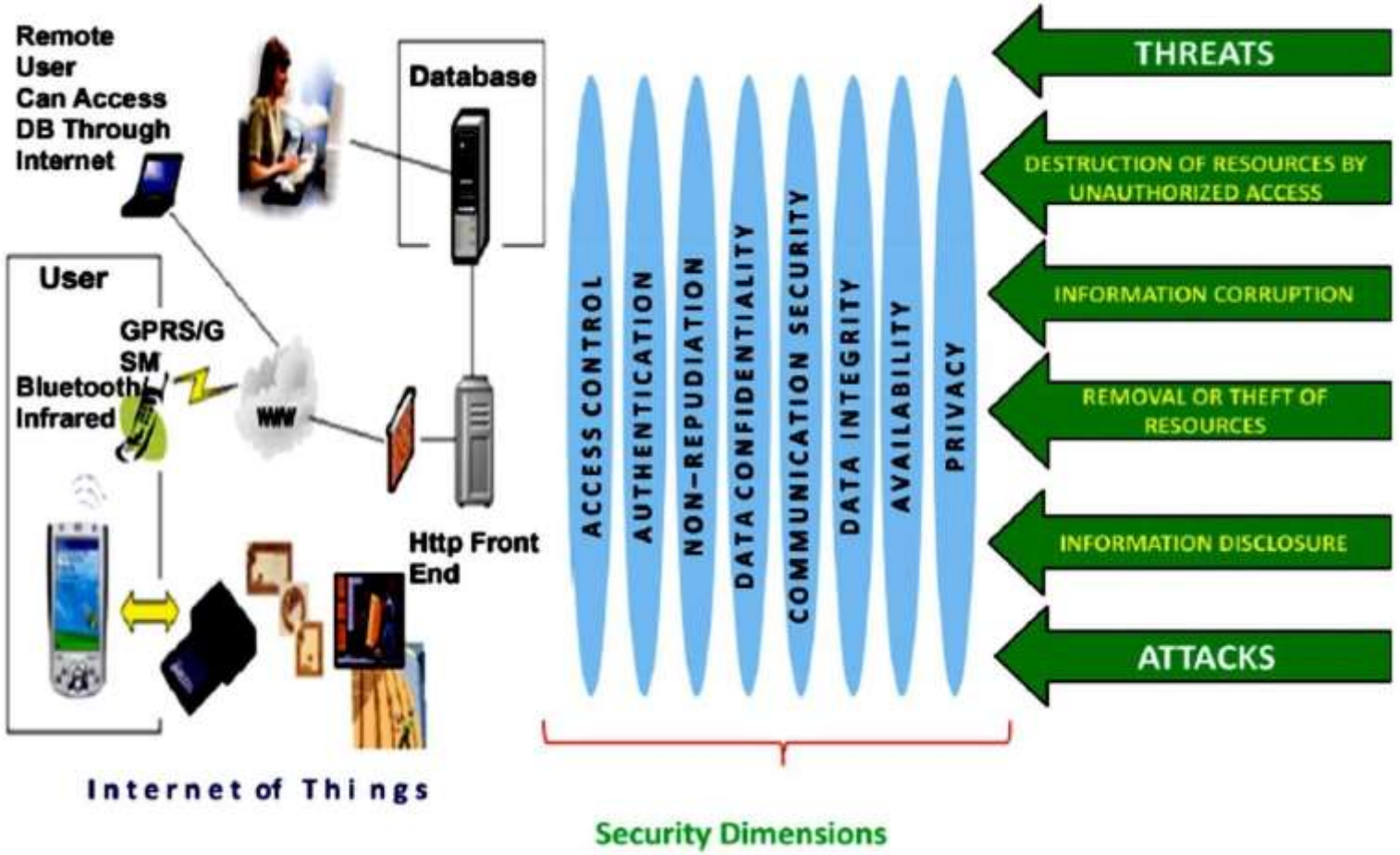
- Tamper Resistance
  - Desire to maintain security requirements even when device falls into hands of malicious parties
  - Can be physically or logically probed
- Scalability
  - IoT consist of various types of devices with different capabilities from intelligent sensors and actuators, to home appliances

Security Requirements

- Communication (wire or wireless) & protocols (Bluetooth, ZigBee, RFID, Wi-Fi, etc.)

- Flexibility and Adaptability
  - IoT will consist of mobile communication devices
  - Can roam around freely from one type of environment to others
  - With different type of risks and security threats
  - So users are likely to have different privacy profile depending on environment

Security Architecture for IoT



Threat Modeling

- Presented by first defining misuse case
- Means negative scenario describing the ways the system should not work
- And then standard use case
- Assets to be protected in IoT will vary with respect to every scenario case

Threat Analysis

- Assets needs to be identified to drive threat analysis process
- Smart home is localized in space, provide services in a household
- Devices in Smart Home are combined with n/w
- Provide means for entertainment, monitoring of appliances, controlling of house components and other services

Use Cases and Misuse Cases

- Actor in use case and misuse case in the scenario of smart home includes:
  - Infrastructure owner (smart home)
  - IoT entity (smartphone device or software agent)
  - Attacker (misuser)
  - Intruder (exploiter)

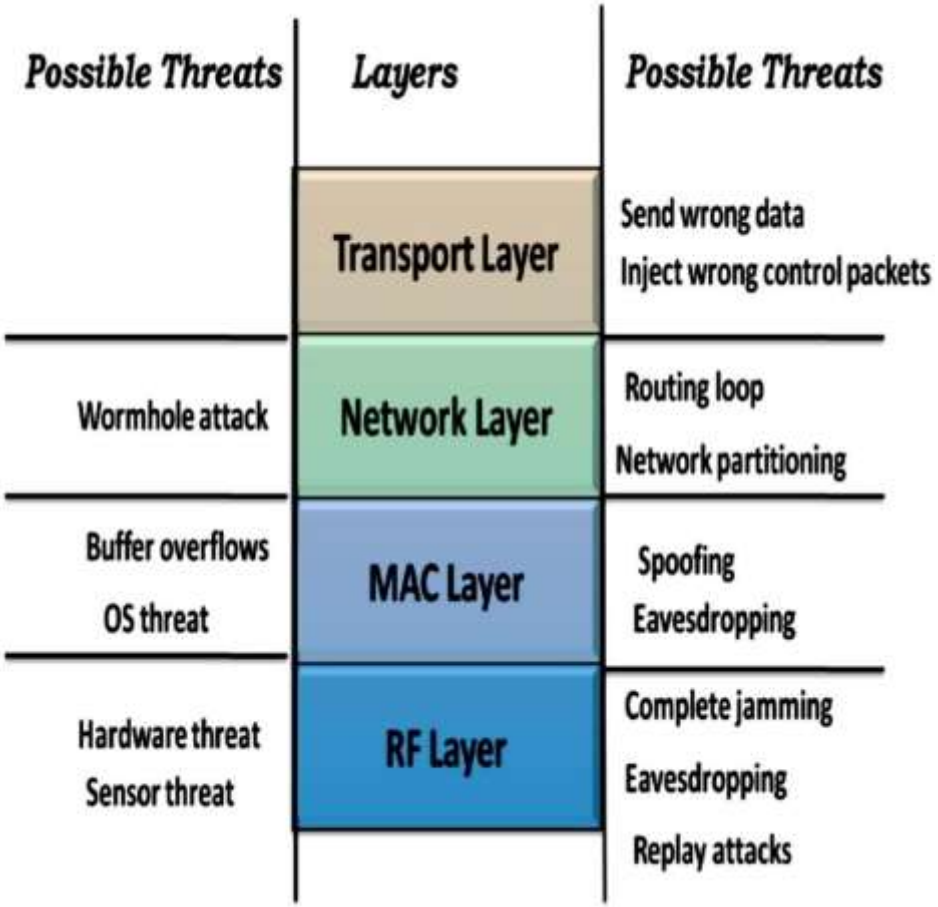
Use Cases and Misuse Cases

- Access rights granted to unauthorized entity
- Corruption of access credentials
- Unauthorized data transmission
- Denial of service (DoS) attack
- Man-in-the-middle attack

IoT Security Tomography

- Classified according to attacks addressing to different layers
  - Transport Layer
  - Network Layer
  - MAC layer
  - RF layer

IoT Security Tomography



Key Elements of Security

- Authentication
- Access Control
- Data and Message Security
- Prevention from denial of taking part in a transaction

Identity Establishment

- Secure Entity Identification or Authentication
- Authentication is identity establishment between communicating devices or entities
- Entity can be a single user, a set of users, an entire organization or some networking device
- Identity establishment is ensuring that origin of electronic document & message is correctly identified.

Access Control

- Also known as access authorization
- Principles is to determine who should be able to access what
- Prevents unauthorized use of resources
- To achieve access control, entity which trying to gain access must be authenticated first
- According to authentication, access rights can be modified to the individual

Data and Message Security

- Related with source authenticity, modification detection and confidentiality of data
- Combination of modification & confidentiality of message is not enough for data integrity
- But origin of authenticity is also important
- Location privacy is equally important risk in IoT
- Should not be any way for attacker to reveal identity or location information of device

Security Model for IoT