Internet of Things

18 MCA 5 4 E

FACULTY

Dr. R. A. ROSELINE M.Sc., M.Phil., Ph.D.,
Associate Professor and Head,
Post Graduate Department of Computer Applications,
Government Arts College (Autonomous),
Coimbatore – 641 018.

UNIT – II

IoT Protocols and Security

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

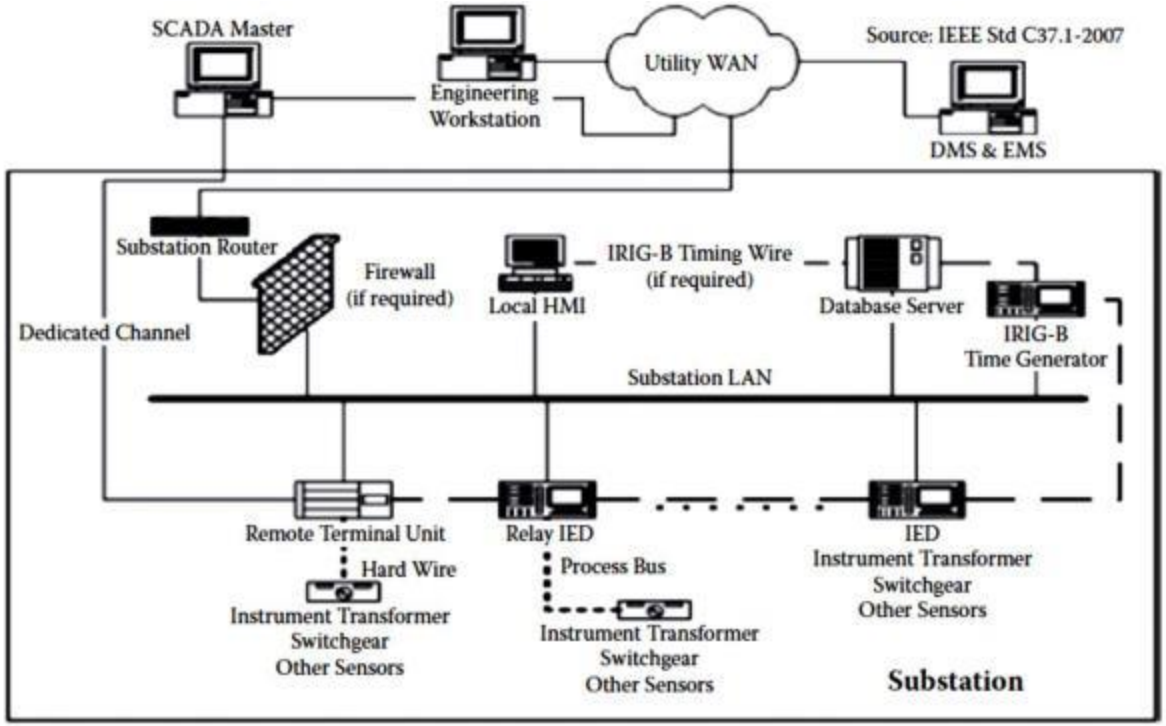
M2M and WSN Protocols

- 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
- They could be contradictory to each other in some cases, even though this observation is debatable

Issues with IoT Standardization

- 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
- 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

Issues with IoT Standardization

- Some people believe that the IoT concept is well established
- 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:

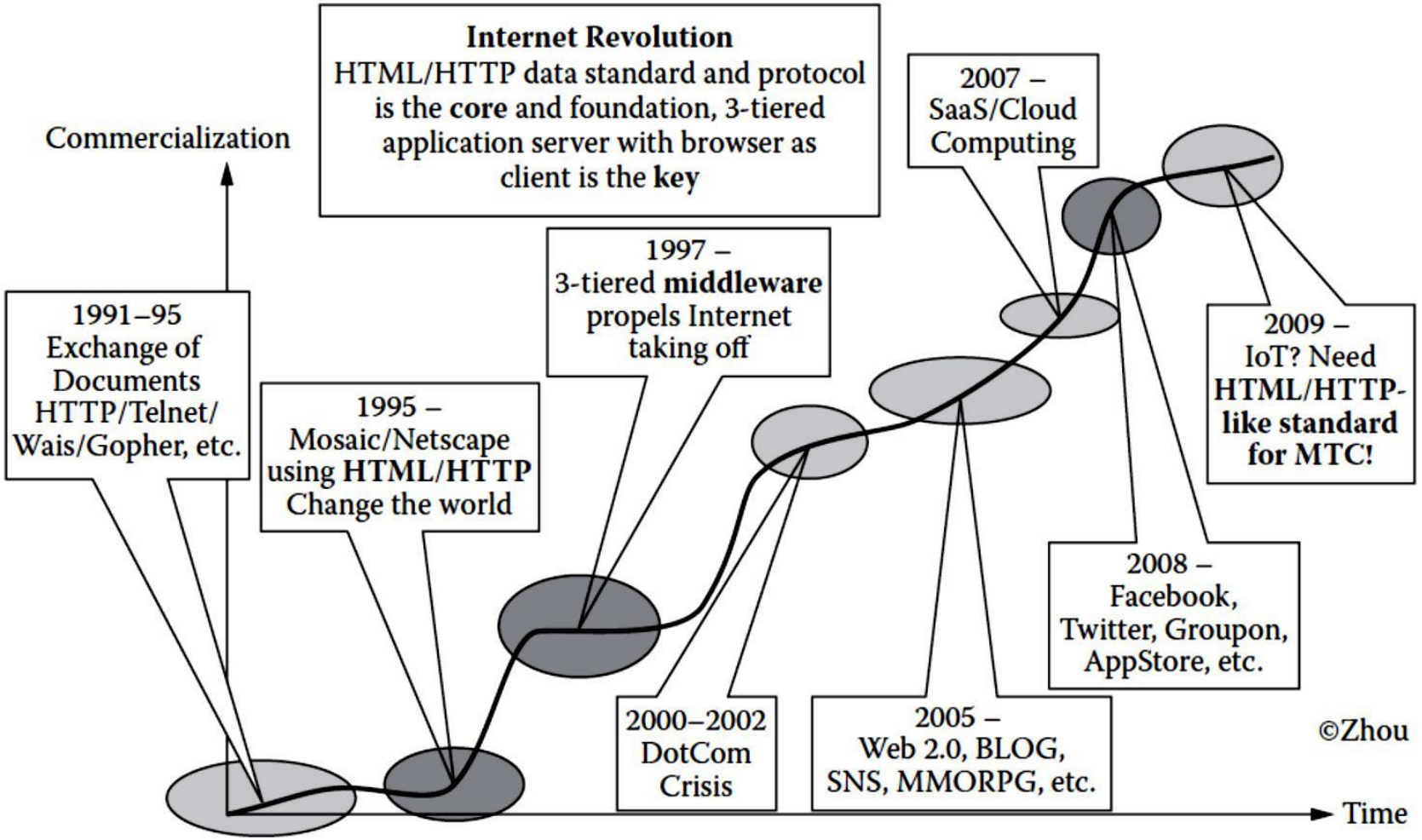
Issues with IoT Standardization

1. ICT standardization is a highly decentralized activity. How can the individual activities of the network of extremely heterogeneous standards-setting 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?

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



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?

Unified Data Standards

- *Do we need a new HTML/HTTP-like standard for MTC and WoT? If there is no need to reinvent the 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*

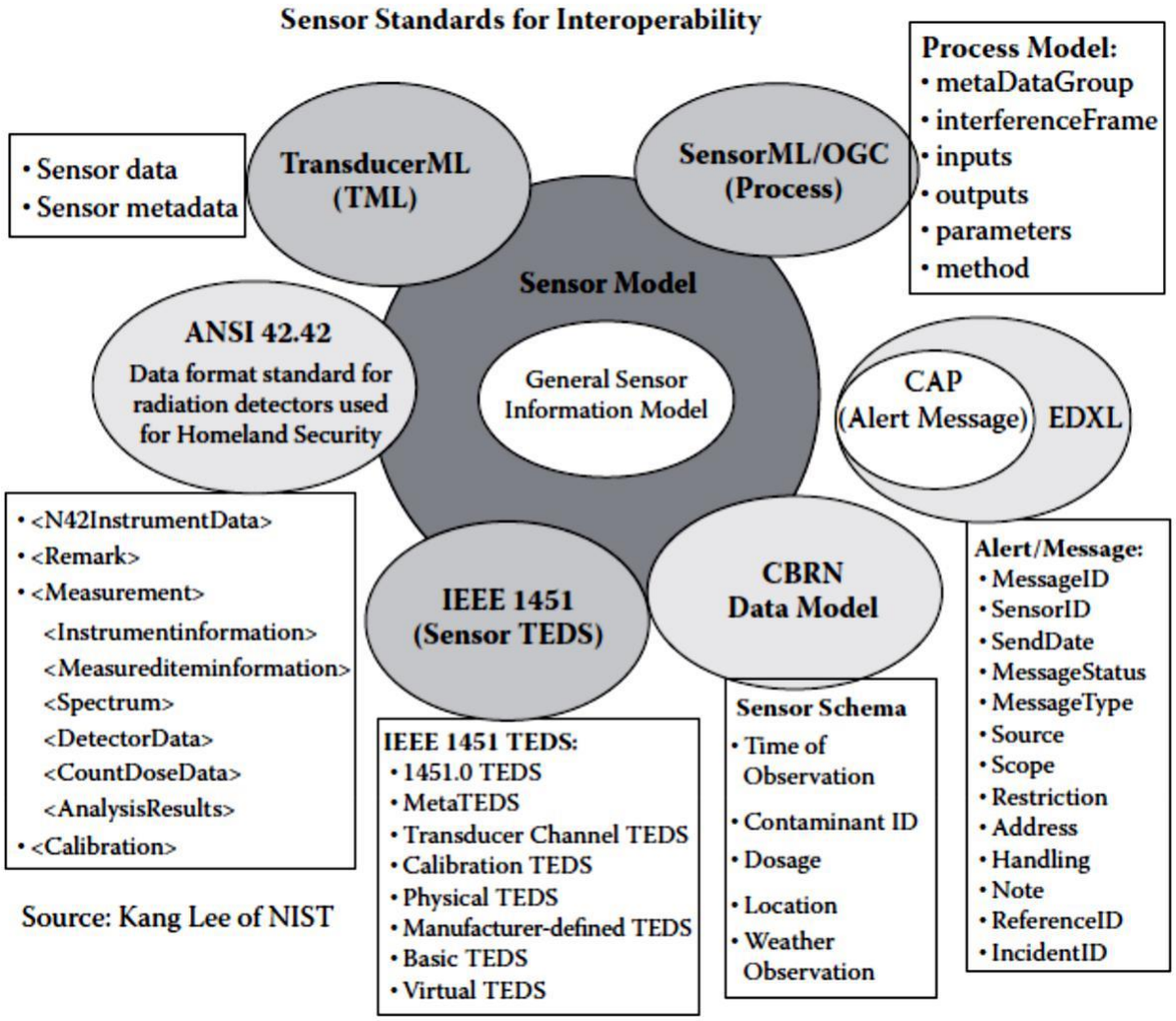
Unified Data Standards

- *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

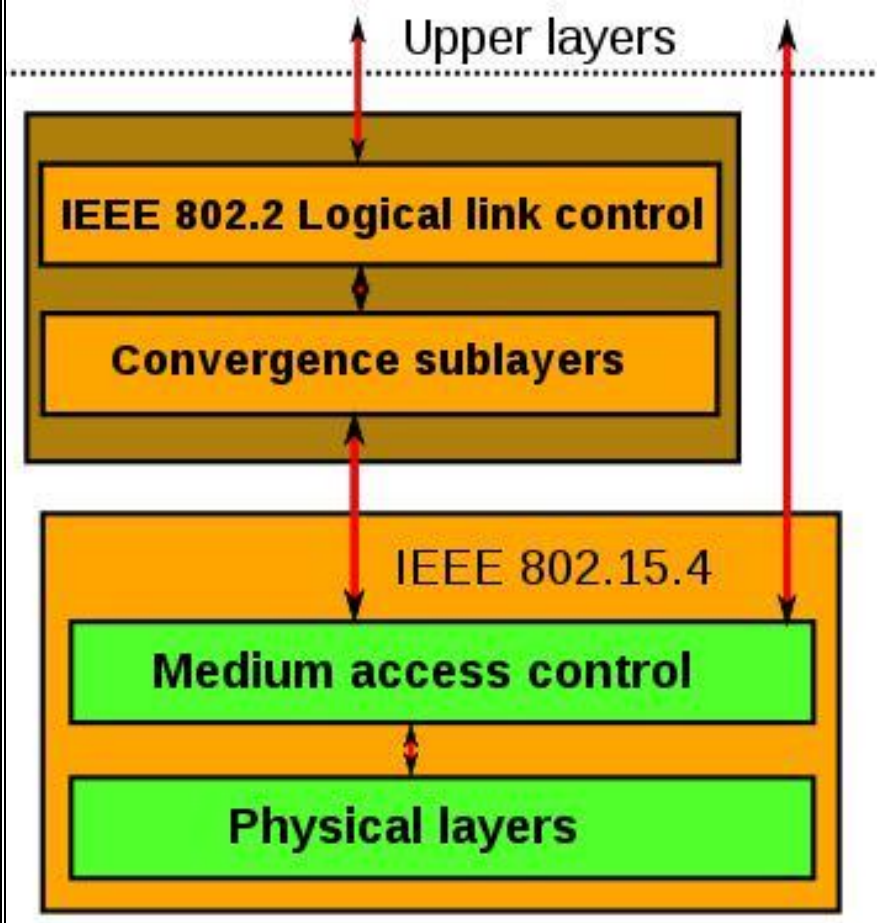


Source: Kang Lee of NIST

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, I-Have 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

BACNet Protocol

- 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)

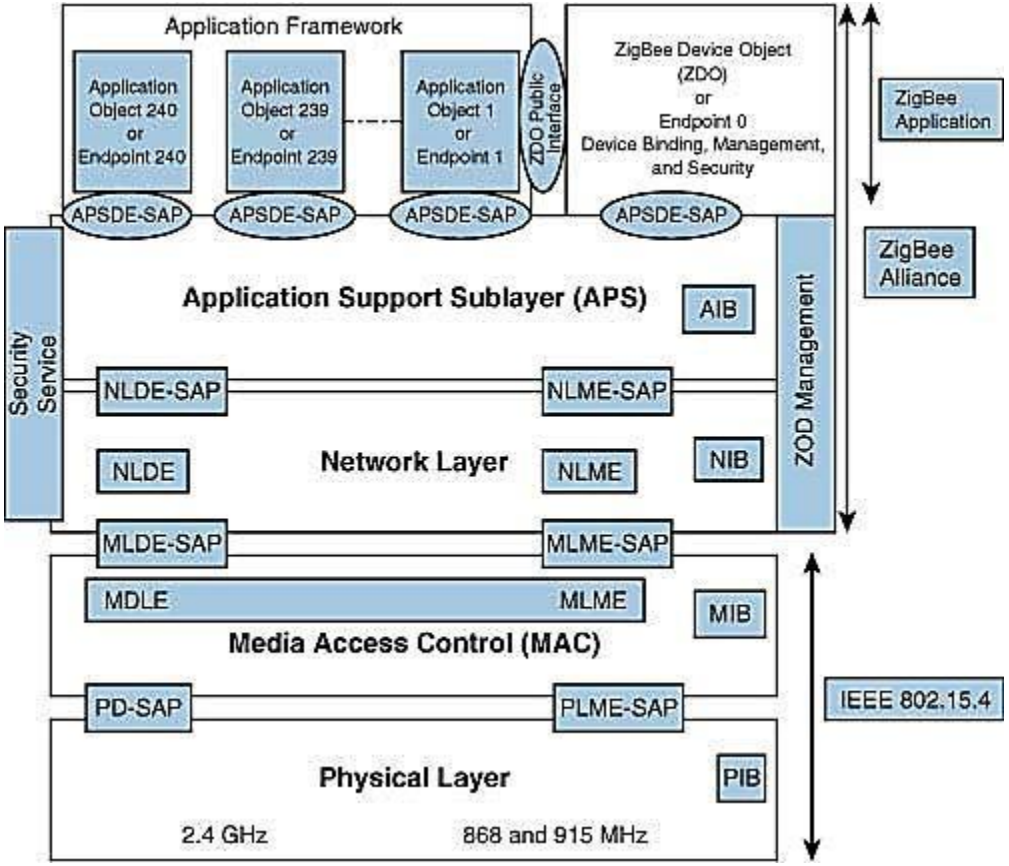
KNX System Components

- 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-based specification for a suite of high-level communication protocols
- Used to create personal area networks with small, low-power digital radios
- ZigBee based applications
  - Home Automation
  - Medical Device Data Collection
  - other low-power low-bandwidth

ZigBee Architecture



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

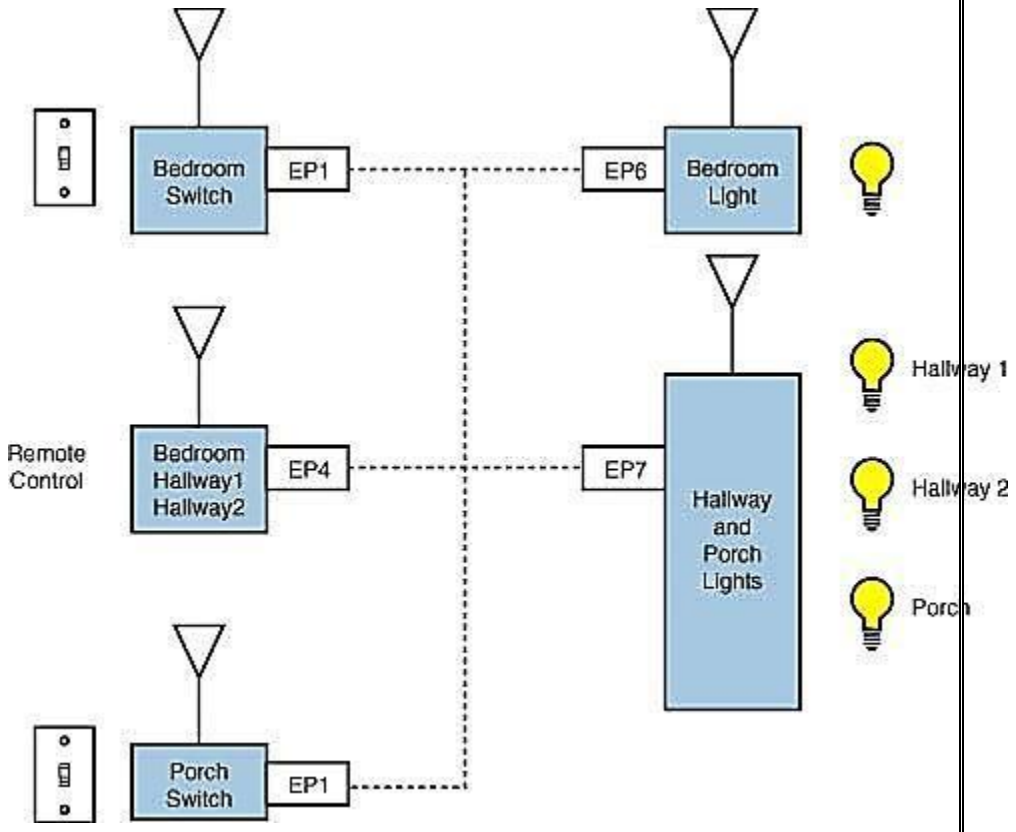
- Located between the MAC layer and application support sublayer
- Provides the following functions:
  - Starting a network
  - Managing end devices joining or leaving a network
  - Route discovery
  - Neighbor discovery

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

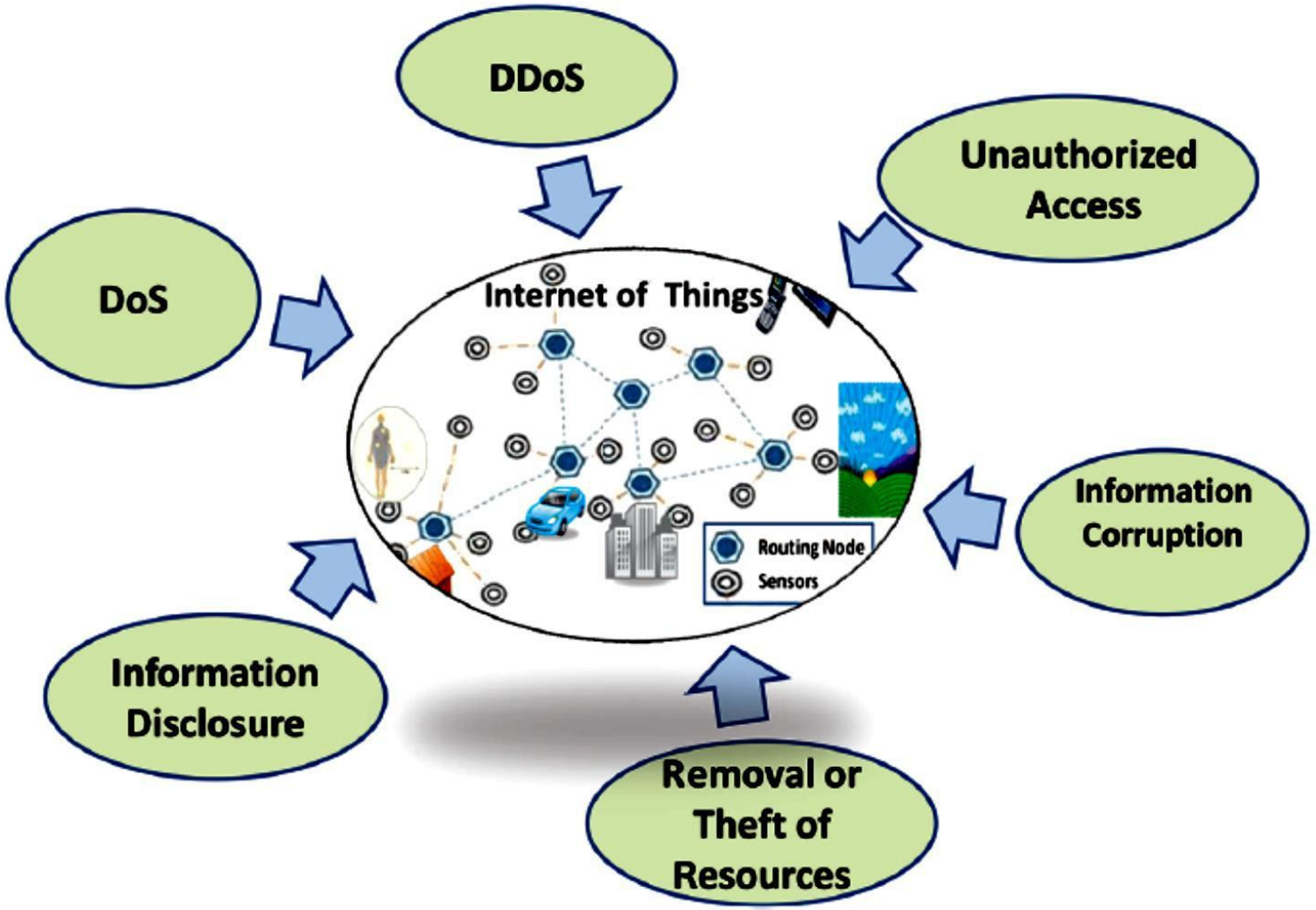
IOT Security

- 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

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
- Privacy of things and security of data is one of the key challenges in the IoT

Vulnerabilities of IoT



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

Vulnerabilities of IoT

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

Vulnerabilities of IoT

- 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
  - That flood the network and deny other authentic users from access to the network

Vulnerabilities of IoT

- DDoS Attack
  - Distributed Denial of Service
  - Type of DoS attack where multiple compromised systems are used to target single system causing DoS
  - Compromised systems – usually infected with Trojan
  - Victims of a DDoS attack consist of both
    - End targeted systems
    - All systems maliciously used and controlled by the hacker in the distributed attack

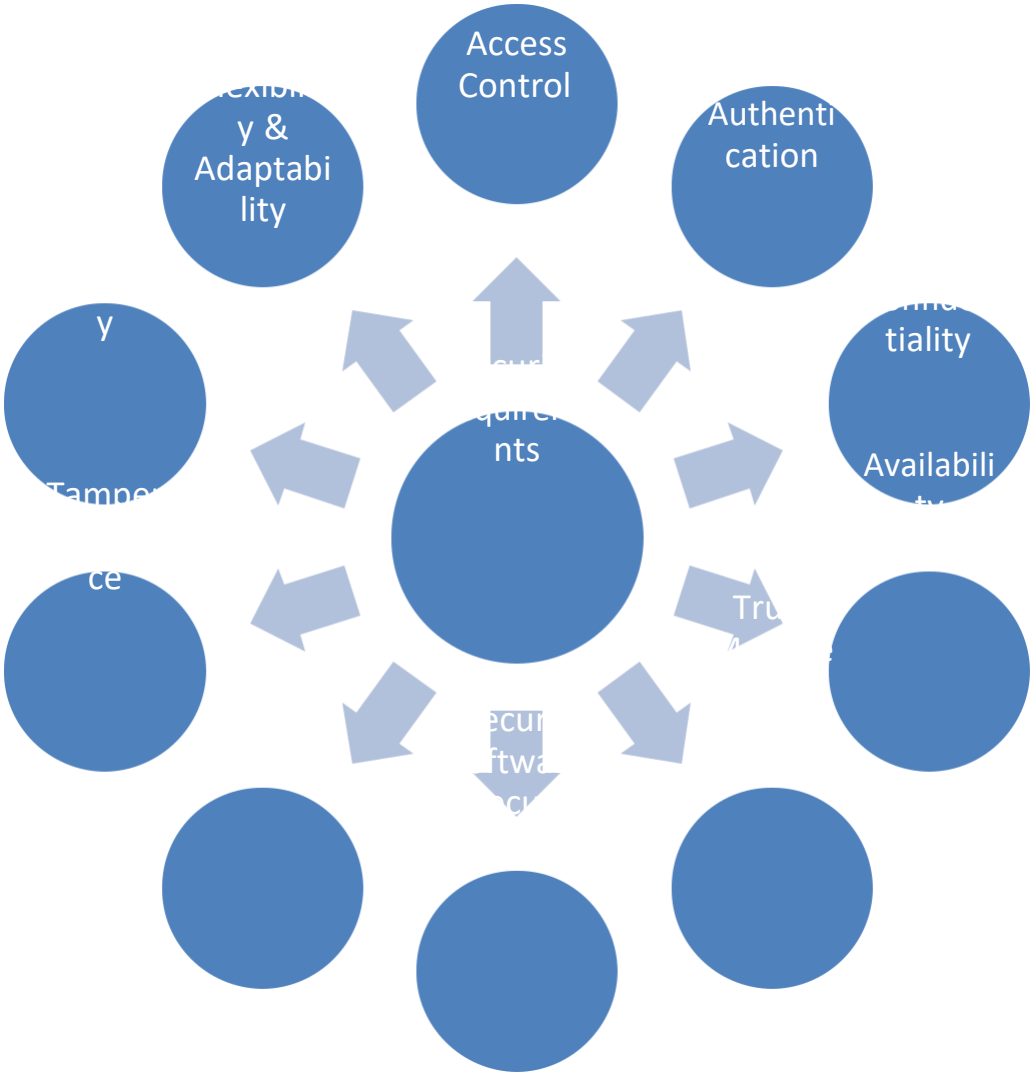
Vulnerabilities of IoT

- CyberBunker Launches “World’s Largest” DDoS Attack
- Slows down the Entire Internet
- CyberBunker - Dutch web hosting company
- Caused global disruption of the web
- Slowing down internet speeds for millions of users across the world, according to BBC report

Vulnerabilities of IoT

- Few real examples of attacks that hit the IoT:
  - Carna Botnet – 4,20,000 ‘things,’ such as routers, modems, printers were compromised
  - TRENDnet’s connected cameras were hacked, with feeds from those cameras published online
  - Linux.Darlloz - PoC IoT worm found in the wild by Symantec, 1,00,000 compromised systems including connected things such as TVs, routers and even a fridge

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

Security Requirements

- Data Confidentiality
  - Protecting data from unauthorized disclosure
  - Secure, lightweight, and efficient key exchange mechanism is required
- Availability
  - Ensuring no denial of authorized access to network resources

Security Requirements

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

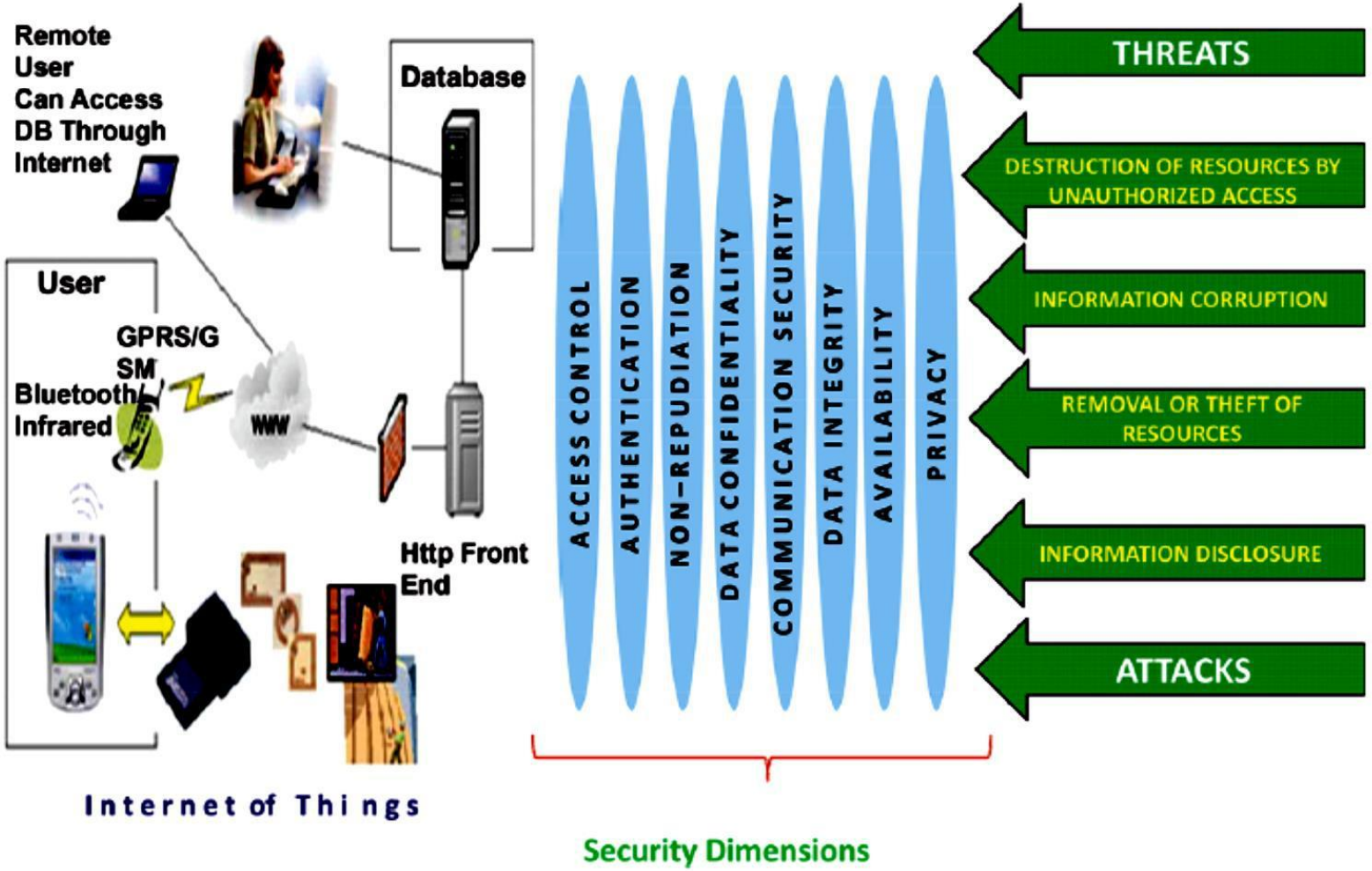
Security Requirements

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

Security Requirements

- 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)

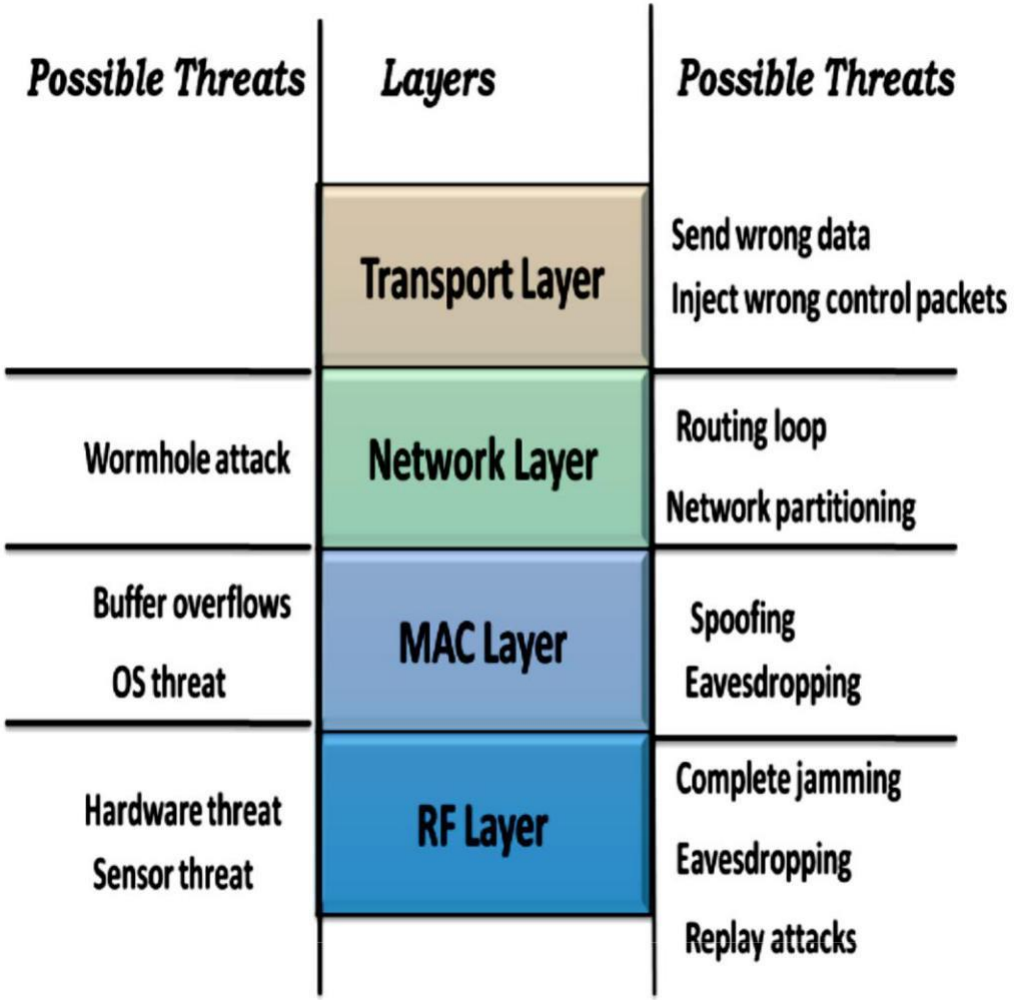
Use Cases and Misuse Cases

- 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

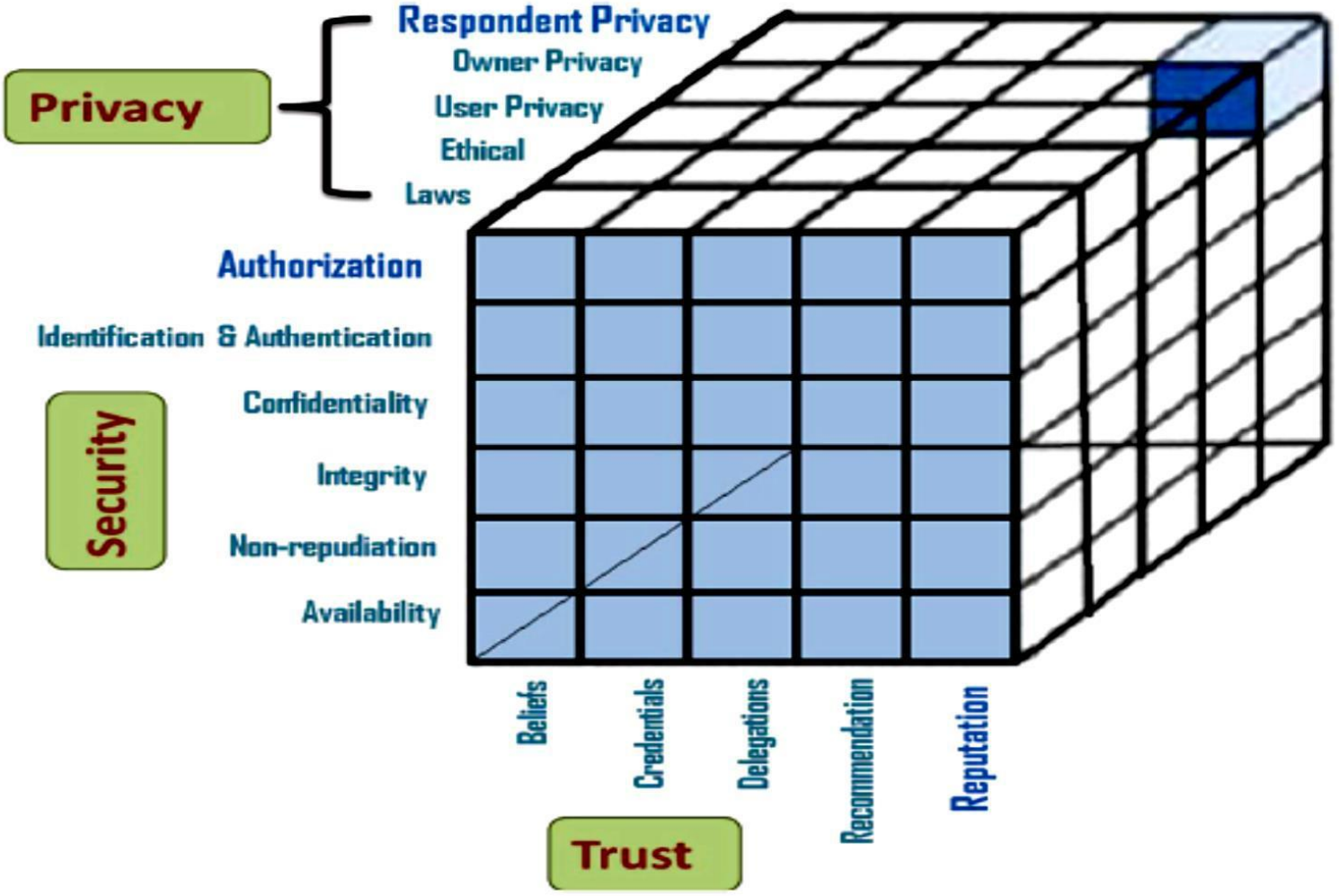
Non-repudiation and Availability

- Non-repudiation is the security services for point-to-point communications
- Process by which an entity is prevented from denying a transmitted message
- So when message is sent, receiver can prove that initiating sender only sent that message
- Sender can prove that receiver got message
- To repudiate means to deny

Non-repudiation and Availability

- Availability is ensured by maintaining all h/w, repairing immediately whenever require
- Also prevents bottleneck occurrence by keeping emergence backup power systems
- And guarding against malicious actions like Denial of Service (DoS) attack

Security Model for IoT



THANK YOU

The material for this course is taken from the Text Books and Reference Books prescribed in the Syllabus.