IoT Protocols, Standards & Security

By,

Dr. Vidya Rao
Assistant Professor,
Dept of DSCA, MIT, MAHE

Outline

- M2M and WSN Protocols
- SCADA
- RFID
- BACNet
- ModBus
- Zigbee Architecture
- MQTT
- IoT Security

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 - M2M-XML, JavaScript Object Notation (JSON), 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

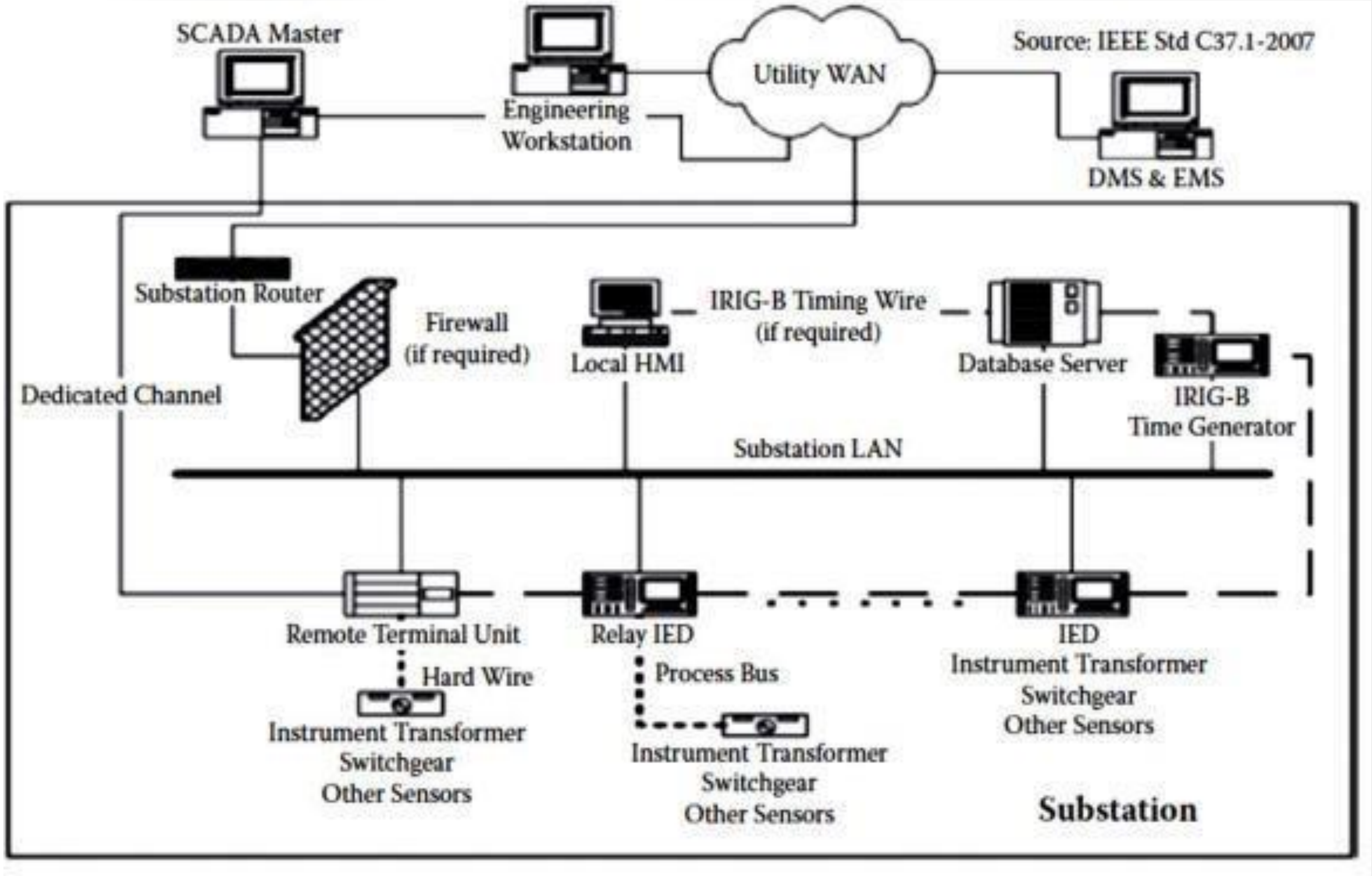
SCADA and RFID Protocols

- Supervisory Control and Data Acquisition (SCADA)
- One of the IoT pillars to represent the whole industrial automation arena
- IEEE created a 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 is a combination of software and hardware components.
- Controlled locally and remotely
- Examines, collects and processes data in real-time.
- HMI(Human-to-machine) interacts with sensors, pumps, hardware etc.
- SCADA logs data for future historical purposes.
- All components are controlled using a Remote Terminal Unit (RTU) and processed using Programmable Control Unit (PCL)

SCADA and RFID Protocols



SCADA and RFID Protocols

- The processing is now distributed
- Functions that used to be done at the control center can now be done by IED i.e. M2M between devices
- Due to the restructuring of the 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 not always 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
- Different consortia, forums and alliances have been doing standardization in their own limited scope

Issues with IoT Standardization (contd..)

- 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.
- Some people believe that the IoT concept is well established
- However, some gray zones remain in the definition, especially which technology should be included

Issues with IoT Standardization (contd..)

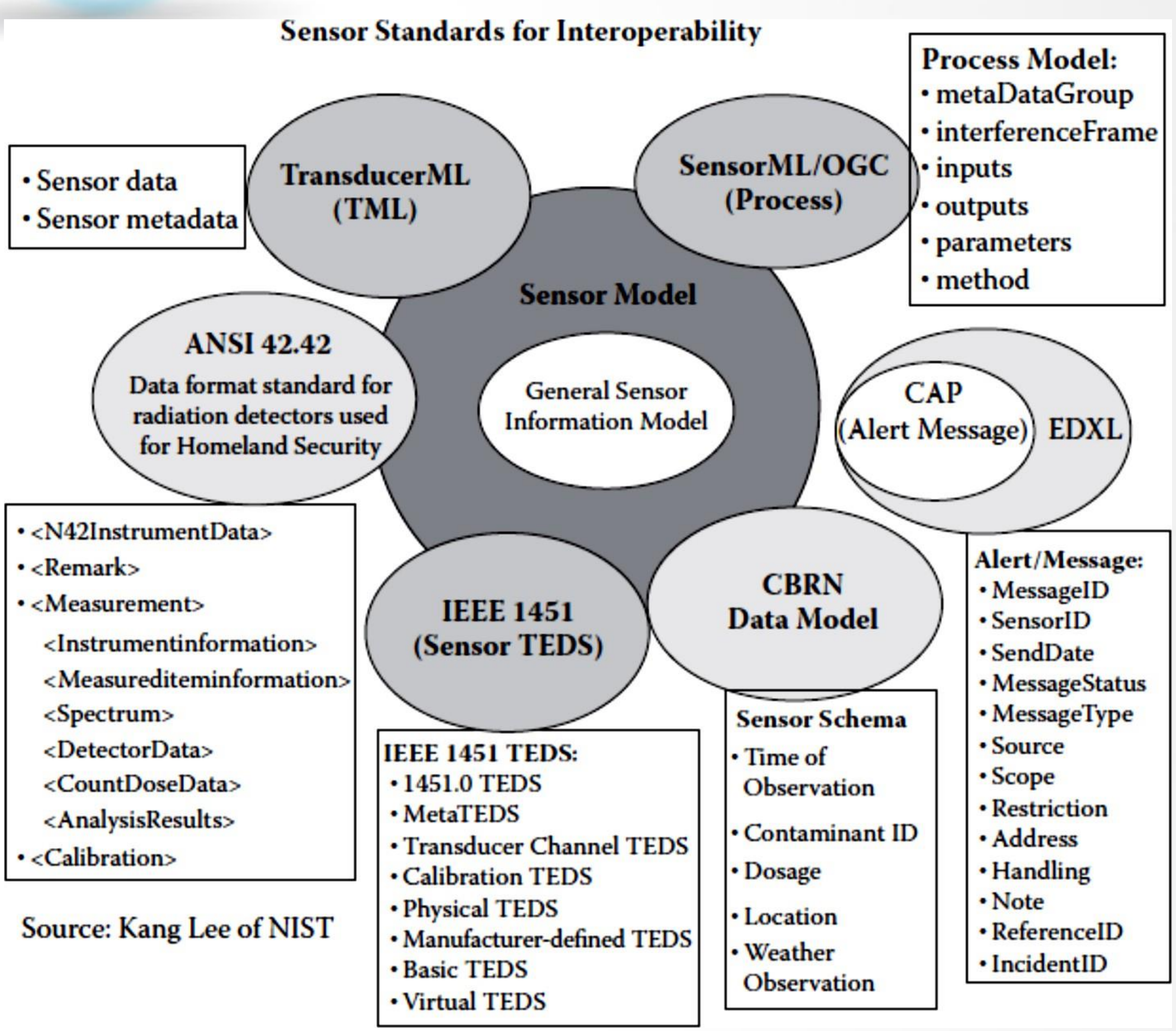
- Following two issues for IoT standardization in particular and ICT standardization, in general, may never have answers:

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

- 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 a 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



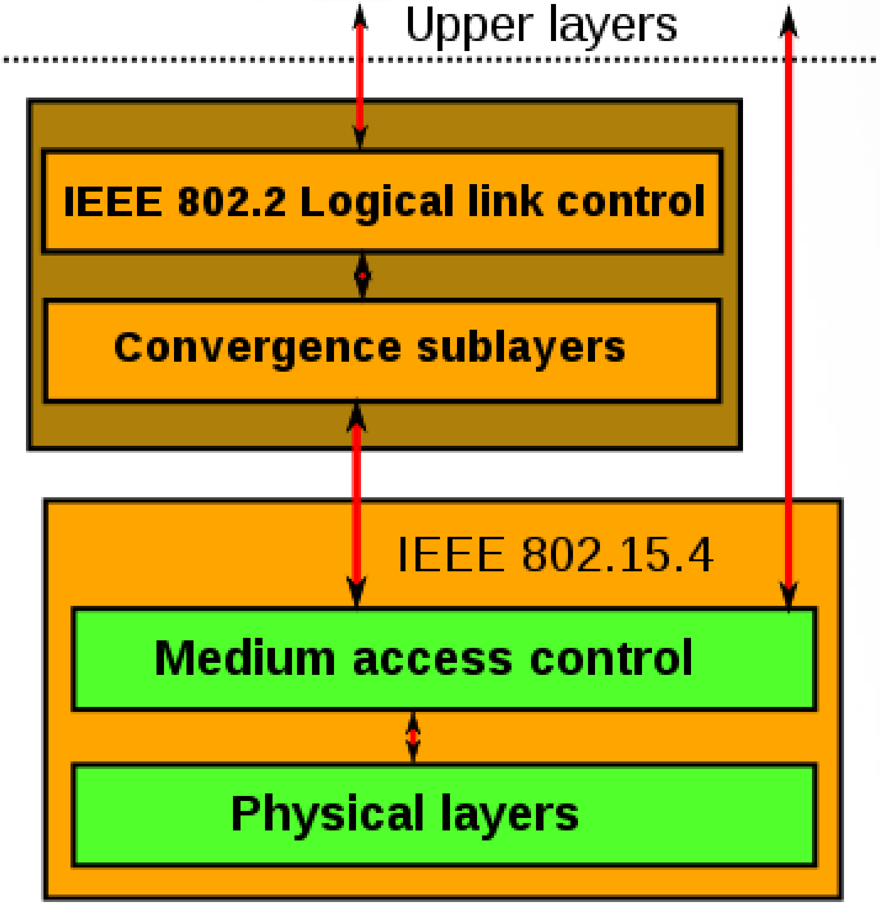
Sensor Standards for Interoperability

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 an industrial environment:
  - Developed with industrial applications
  - Openly publish and royalty-free services
  - Easy to deploy and maintain
- Enables communication among many devices connected to the same network

Modbus (contd..)

Objects

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

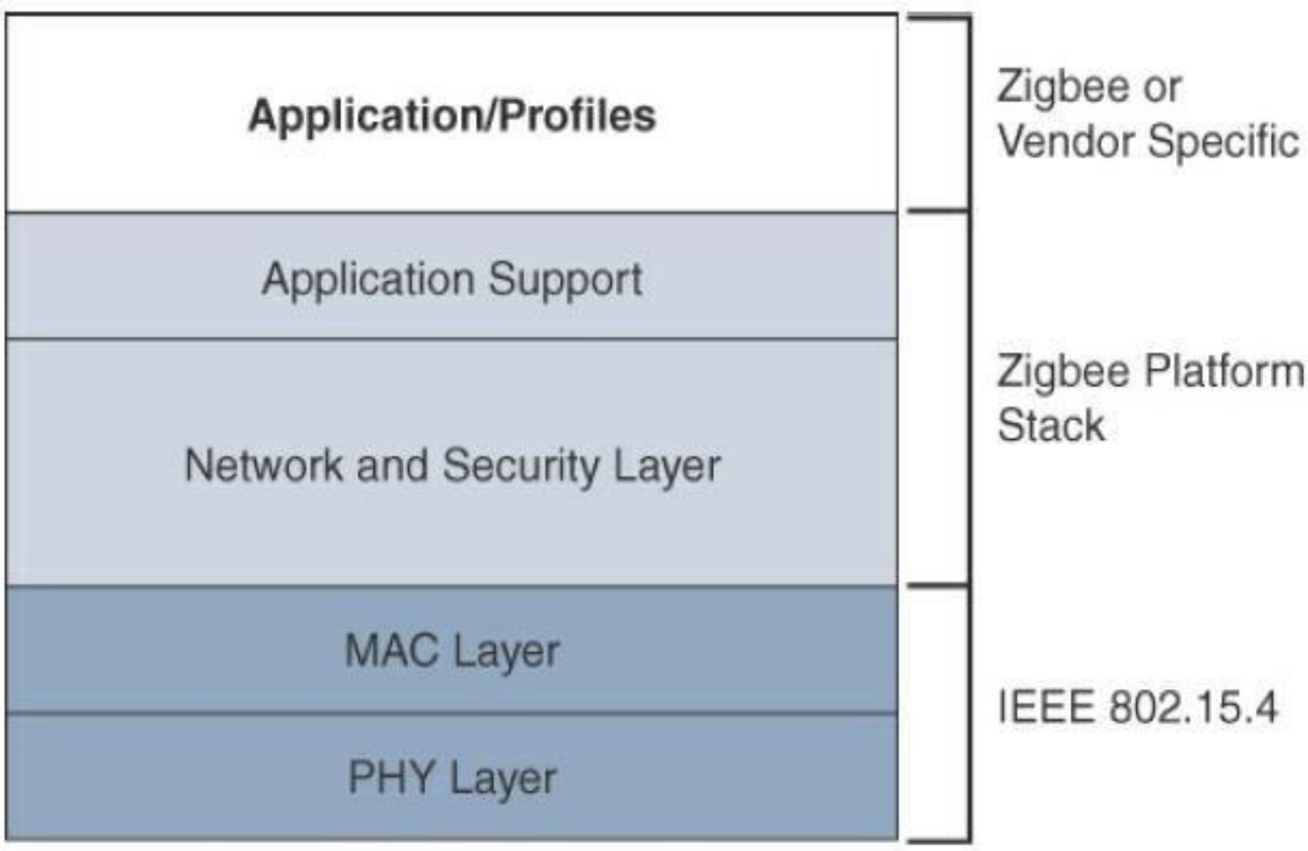
Protocol versions

- 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

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 protocol stack

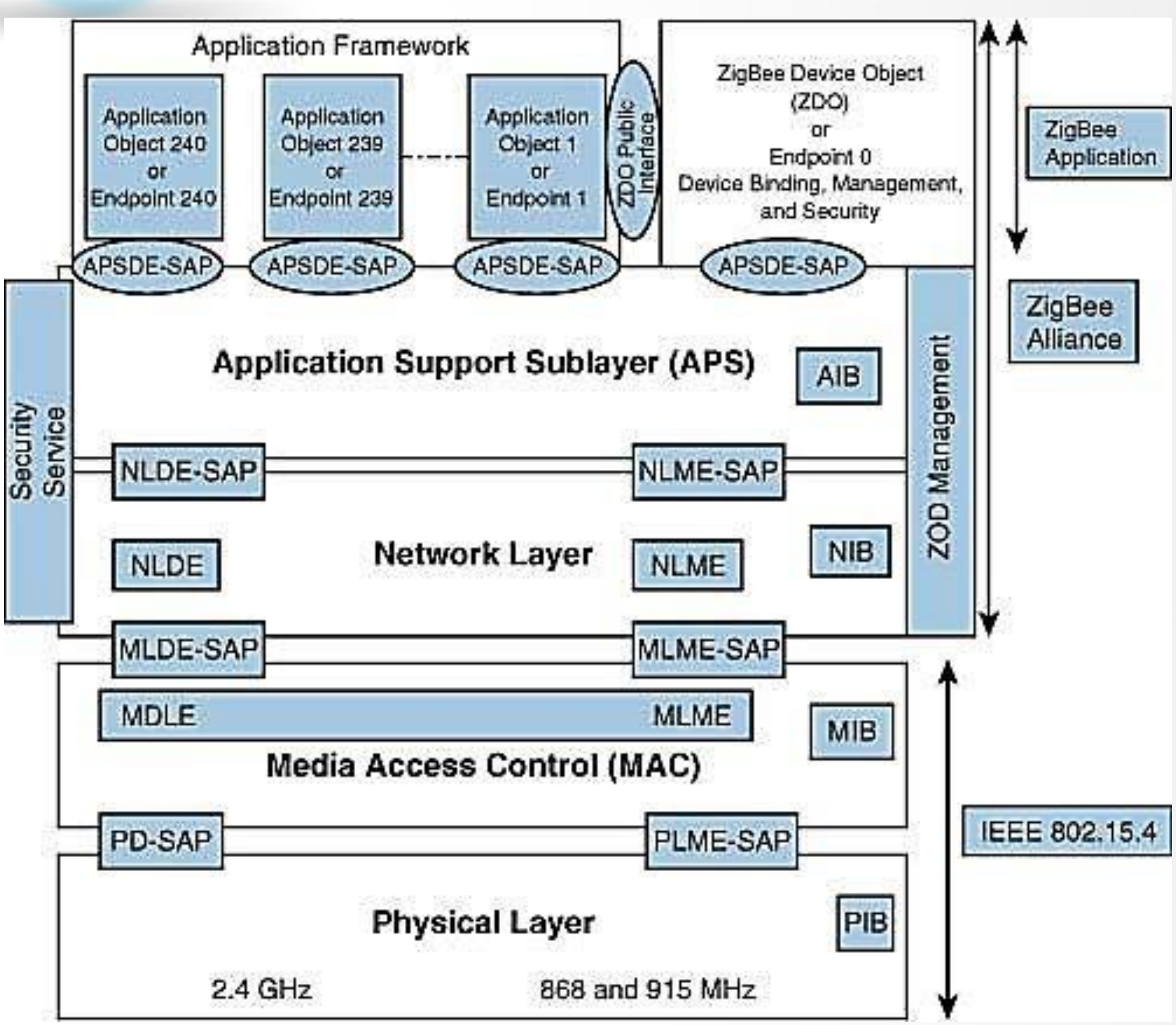


High-Level ZigBee Protocol Stack

ZigBee protocol stack

- The **network layer** is also responsible for forming the appropriate topology, which is often a **mesh** but could be a star or tree as well.
- From a **security perspective,** ZigBee utilizes 802.15.4 for security at the MAC layer, using the **Advanced Encryption Standard (AES) with a 128-bit** key and also provides security at the network and application layers.
- The **application support layer** interfaces the lower portion of the stack dealing with the networking of ZigBee devices with the higher-layer applications.

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

ZigBee Architecture

- **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

ZigBee Architecture

APS Layer

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

ZigBee Architecture

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

ZigBee Architecture

- **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 a single device
- **ZigBee Addressing Mode**
  - ZigBee uses direct, group, and broadcast address for the transmission of information

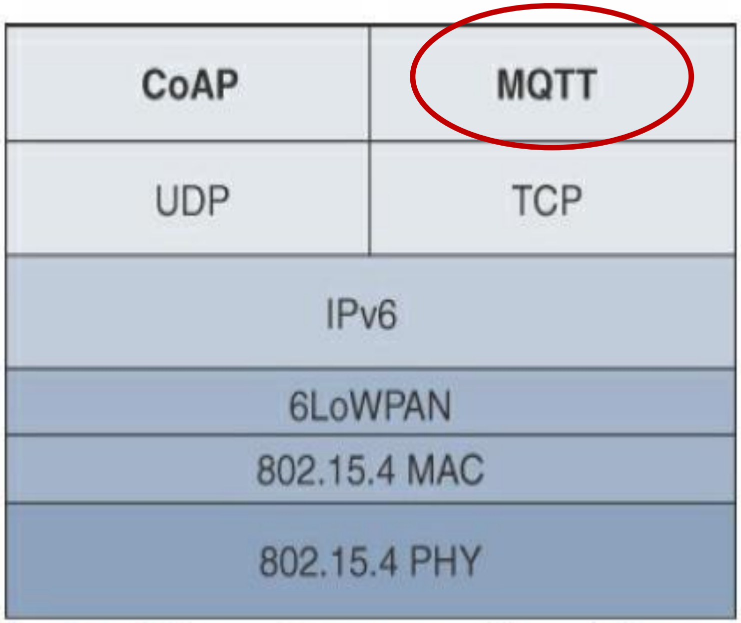
Message Queuing Telemetry Transport

IoT Application Layer Protocols:

- ➢IoT industry is working on new lightweight protocols that are better suited to large numbers of constrained nodes and networks.

- ➢Two of the most popular protocols are CoAP and MQTT.

- ➢Figure highlights their position in a common IoT protocol stack.



CoAP	MQTT
UDP	TCP
IPv6	
6LoWPAN	
802.15.4 MAC	
802.15.4 PHY	

Example of a High-Level IoT Protocol Stack for CoAP and MQTT

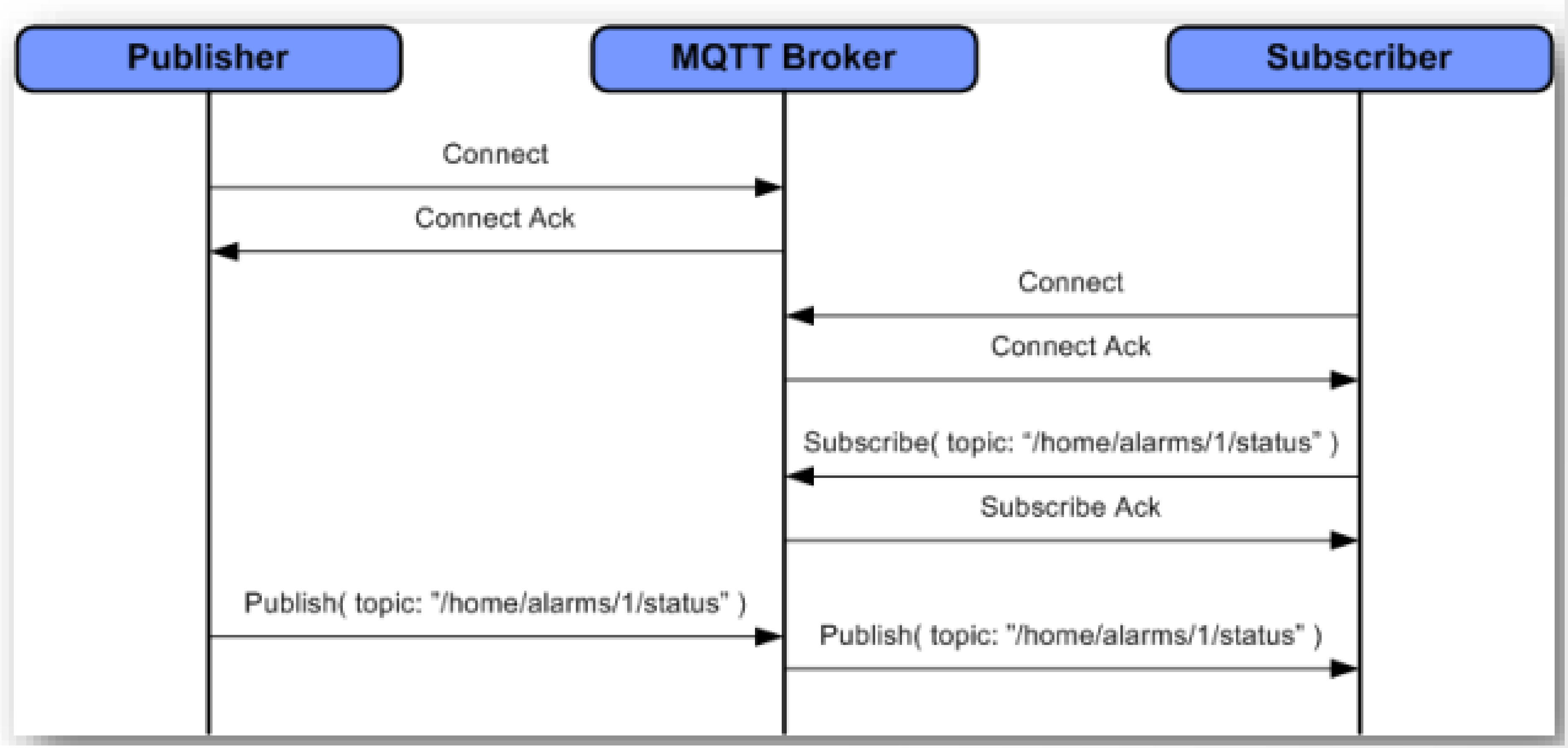
MQTT

- MQTT is described on the https://mqtt.org site as a machine to-machine (M2M) / IoT connectivity protocol.
- MQTT is an Event based IoT protocol :
  - Publish/subscribe messaging transport protocol
  - Over TCP/IP (or MQTT-S over UDP for LAN)
- Properties:
  - Its a lightweight protocol.
  - Supports smallest measuring and monitoring devices
  - Transmit data over far reaching networks .
  - Provide a low latency two-way communication channel.
  - Minimizes the number of bytes flowing over the wire
  - Consumes less power.

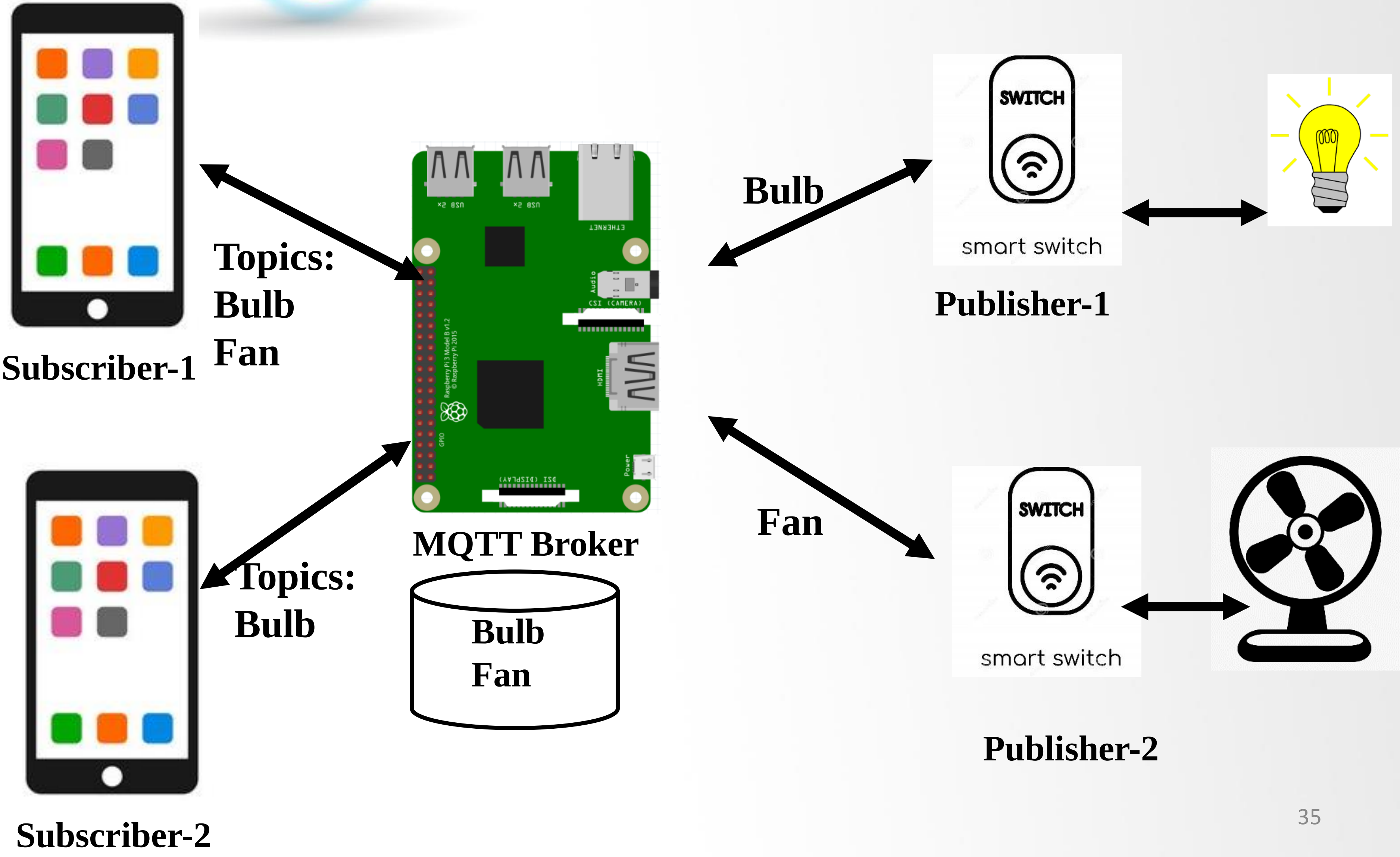
MQTT Concepts

- Major Concepts of MQTT:
  - Publisher/Subscriber
  - Messages → Command or data
  - Topics & Wildcards → string separated by “/”
    - Ex. Home/office/lamp for lamp topic can be “turn on the lamp”
  - Broker :
    - Receives all messages
    - Filters the messages
    - Publishes the message to all subscribed clients

Pub/Sub Architecture


Publisher
MQTT Broker
Subscriber
Connect
Connect Ack
Connect
Connect Ack
Subscribe(topic: "/home/alarms/1/status")
Subscribe Ack
Publish(topic: "/home/alarms/1/status")
Publish(topic: "/home/alarms/1/status")

Pub/Sub Architecture



Subscriber-1

Topics:
Bulb
Fan

Subscriber-2

Topics:
Bulb

MQTT Broker

Bulb
Fan

Bulb

Fan

Publisher-1

Publisher-2

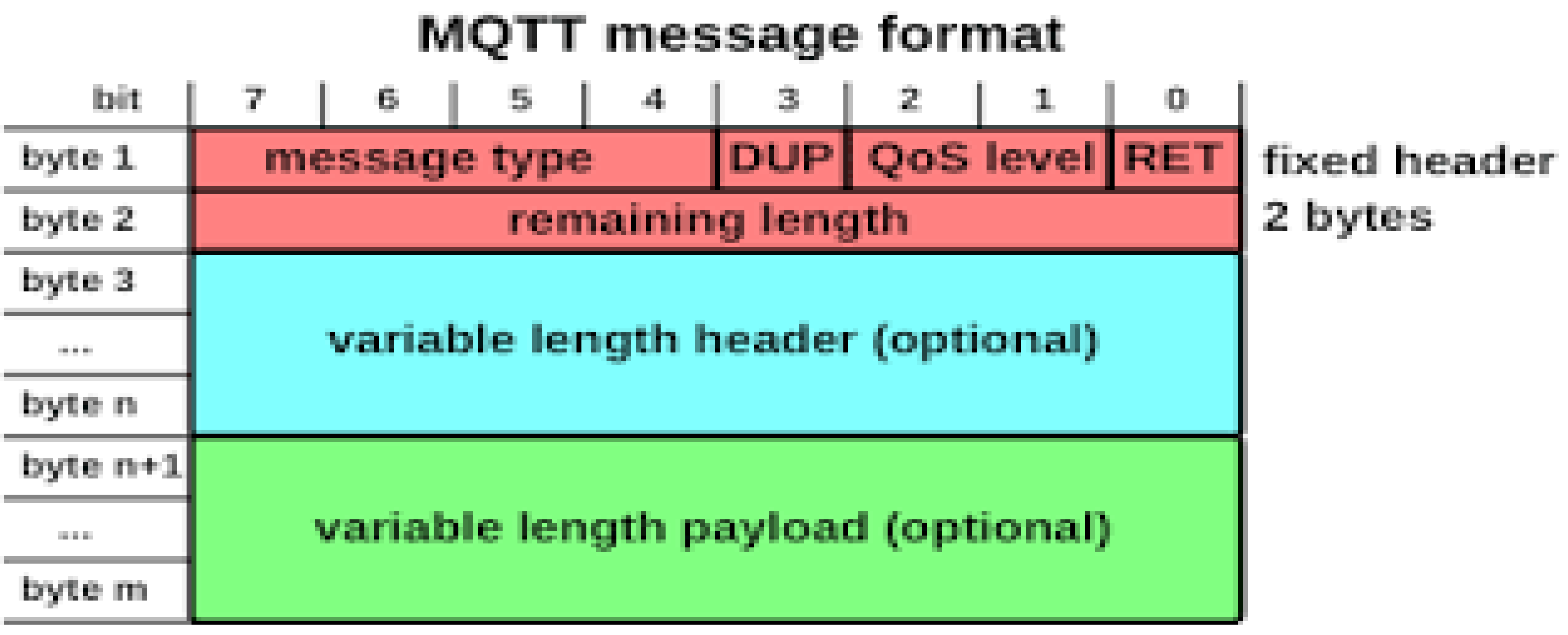
MQTT Message Format

– MQTT Header

- 2-bytes fixed header
- Payload of 256 MB

– MQTT Ports

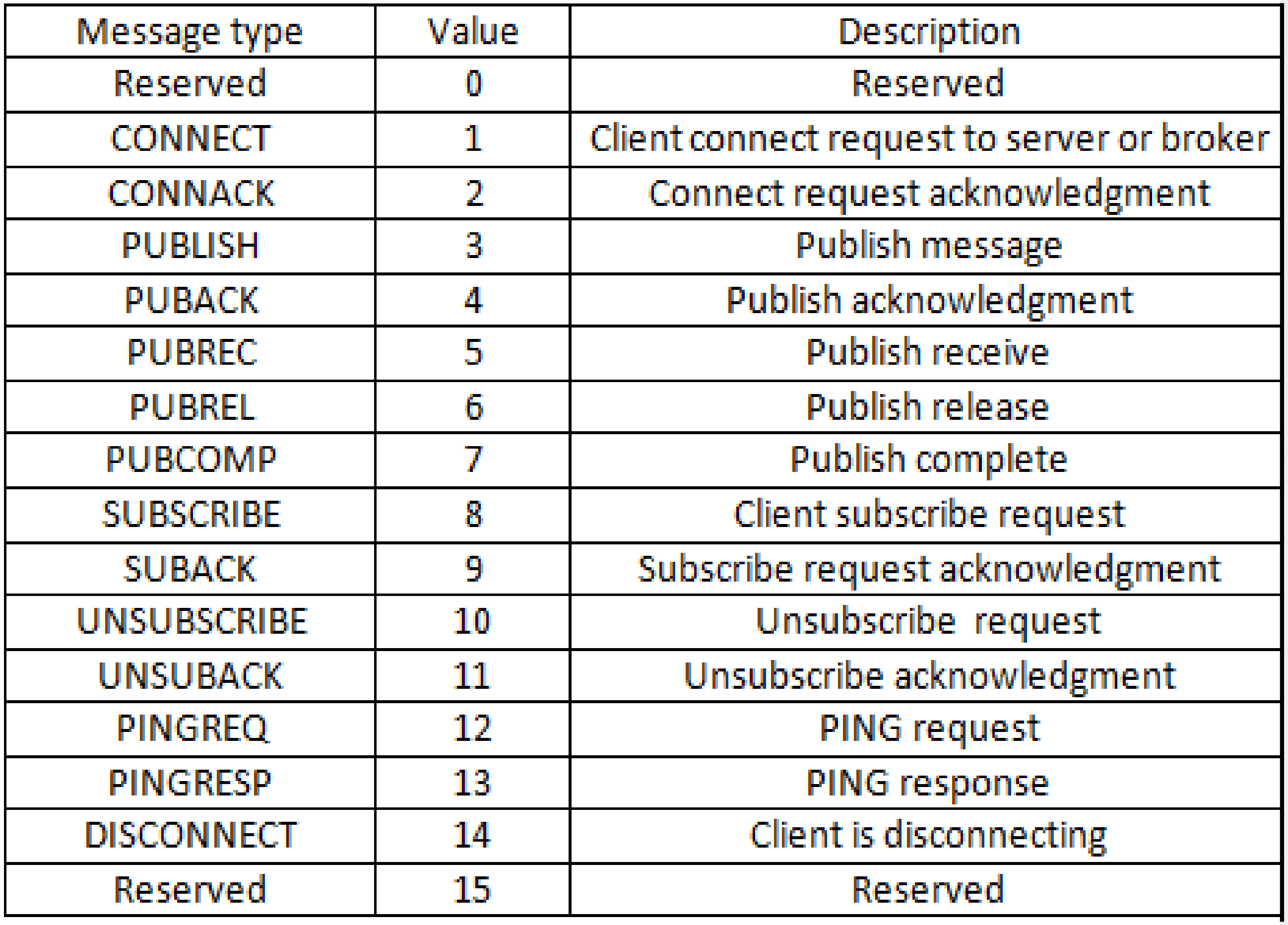
- Control packets run over TCP transport using port 1883
- Secured using TLS on port 8883
- Web Socket (defined in RFC 6455)



MQTT message format

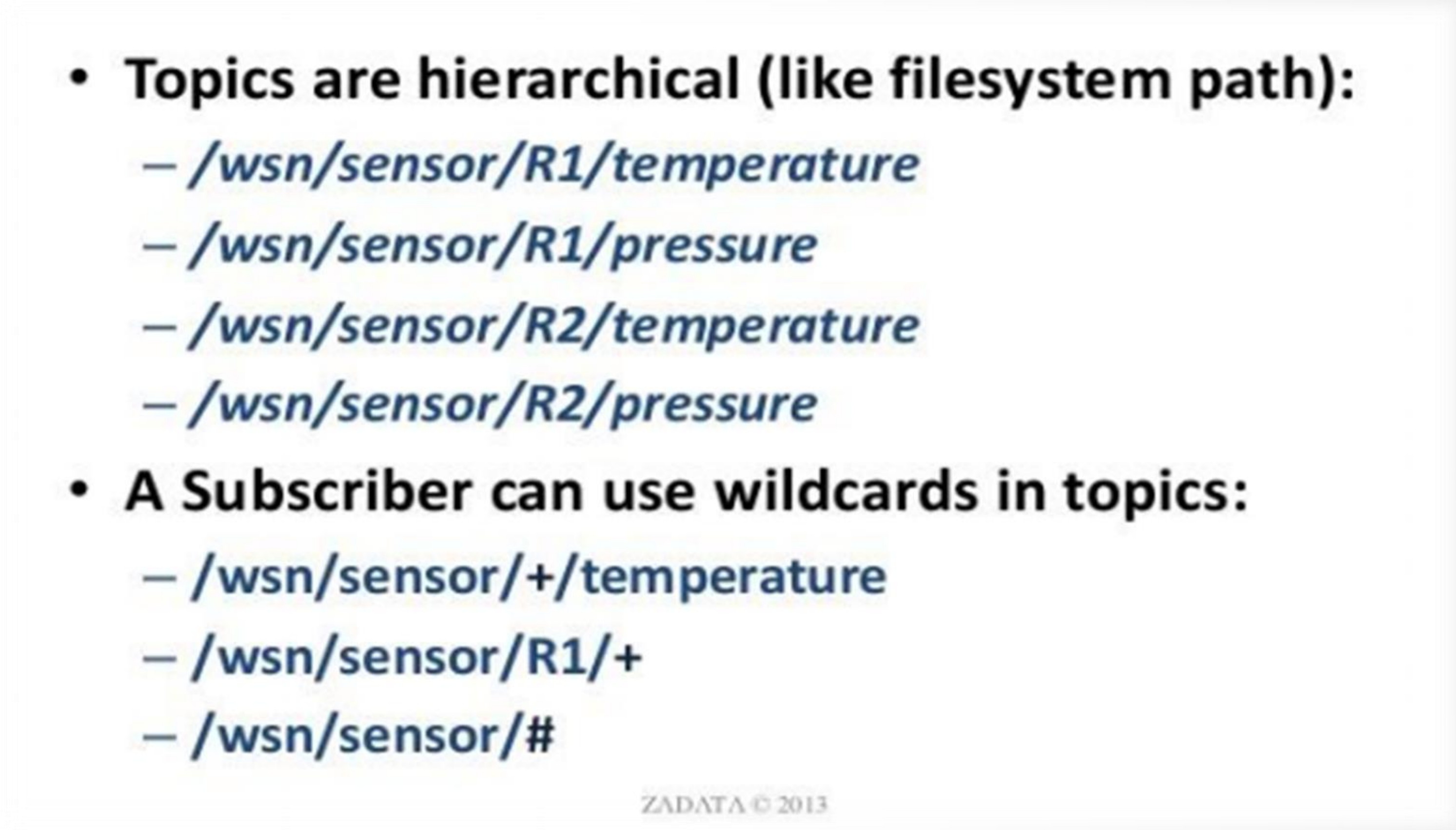
bit	7	6	5	4	3	2	1	0	
byte 1	message type				DUP	QoS level		RET	fixed header
byte 2	remaining length								2 bytes
byte 3	variable length header (optional)								
...									
byte n									
byte n+1	variable length payload (optional)								
...									
byte m									

MQTT Message Types



Message type	Value	Description
Reserved	0	Reserved
CONNECT	1	Client connect request to server or broker
CONNACK	2	Connect request acknowledgment
PUBLISH	3	Publish message
PUBACK	4	Publish acknowledgment
PUBREC	5	Publish receive
PUBREL	6	Publish release
PUBCOMP	7	Publish complete
SUBSCRIBE	8	Client subscribe request
SUBACK	9	Subscribe request acknowledgment
UNSUBSCRIBE	10	Unsubscribe request
UNSUBACK	11	Unsubscribe acknowledgment
PINGREQ	12	PING request
PINGRESP	13	PING response
DISCONNECT	14	Client is disconnecting
Reserved	15	Reserved

MQTT Topics and Wildcards



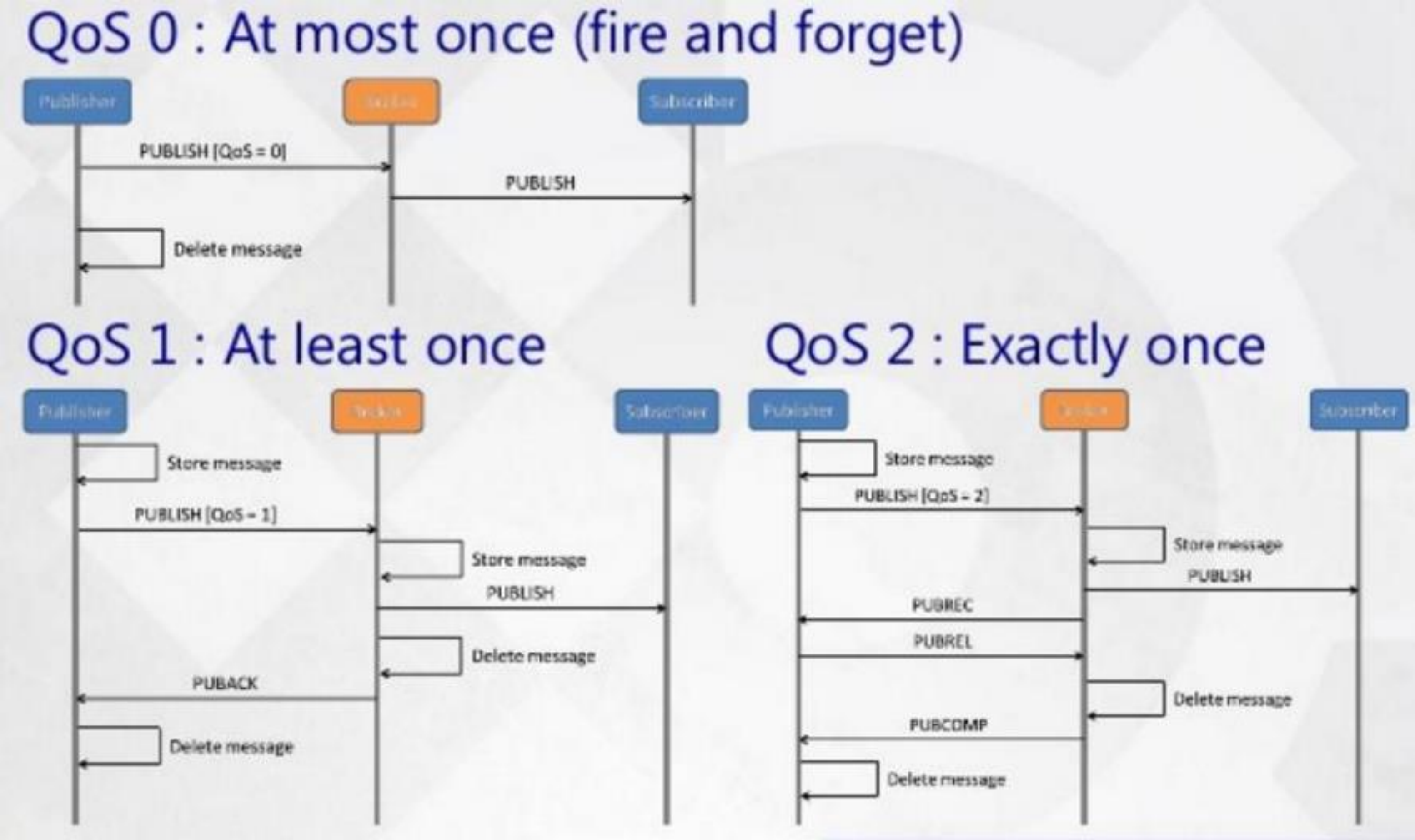
- Topics are hierarchical (like filesystem path):
  - */wsn/sensor/R1/temperature*
  - */wsn/sensor/R1/pressure*
  - */wsn/sensor/R2/temperature*
  - */wsn/sensor/R2/pressure*
- A Subscriber can use wildcards in topics:
  - /wsn/sensor/+/temperature
  - /wsn/sensor/R1/+
  - /wsn/sensor/#

ZADATA © 2013

MQTT QoS

- Quality of service (QoS) levels determine how each MQTT message is delivered.
- Three QoS for message delivery could be achieved using MQTT:
  - QoS 0 (At most once) - where messages are delivered according to the best efforts of the operating environment. Message loss can occur.
  - QoS 1 (At least once) - where messages are assured to arrive but duplicates can occur.
  - QoS 2 (Exactly once) - where message are assured to arrive exactly once.
- There is a simple rule when considering performance impact of QoS : “The higher the QoS, the lower the performance"

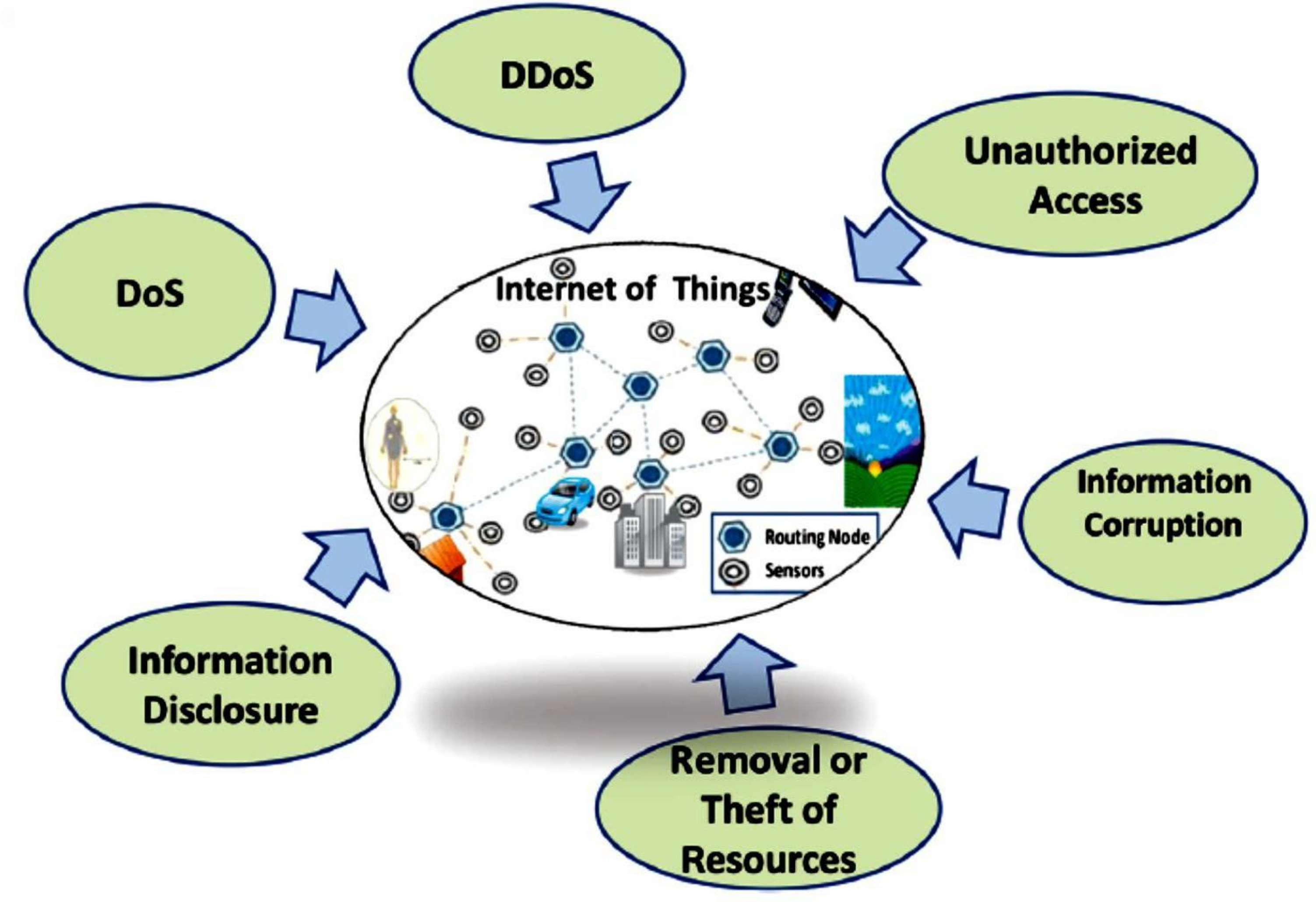
MQTT QoS


QoS 0 : At most once (fire and forget)
Publisher
Broker
Subscriber
PUBLISH [QoS = 0]
PUBLISH
Delete message
QoS 1 : At least once
Publisher
Broker
Subscriber
Store message
PUBLISH [QoS = 1]
Store message
PUBLISH
Delete message
PUBACK
Delete message
QoS 2 : Exactly once
Publisher
Broker
Subscriber
Store message
PUBLISH [QoS = 2]
Store message
PUBLISH
PUBREC
PUBREL
Delete message
PUBCOMP
Delete message

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
- 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
- **Theft of Resources**
  - Access of shared resources over insecure channel causes theft of resources
  - Results into man-in-the-middle attack

Vulnerabilities of IoT

- **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
- **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

Security Breaches

- **The Mirai Botnet(aka Dyn attack)**
  - Largest DDoS attack - Mirai hacked user name and password of IoT devices and infected malware into the user’s network.
  - Laydown of Twitter, the Guardian, Netflix, Reddit and CNN

- **Hackable, cardiac devices from St. Jude medical center**
  - CNN confirmed cardiac device vulnerabilities.
  - Hacker could deplete battery, administrate incorrect pacing or shock data
  - Vulnerability occurred in transmitter that reads the device’s data and shares to remote physicians

- **The Owlet baby hacker, from St. Jude medical center**
  - Baby heart monitoring device hacked and false data sent to parents

- **TRENDnet webcam hack**
  - Camera IP was hacked and people were stalked.

Security Breaches (contd..)

- **The Jeep Hack**
  - IBM security intelligence reported Jeep SUV hacked.
  - Vehicle’s CAN network was taken control by the researchers

- **Xiaomi’s Smart Security camera**
  - The owner of the camera was able to view other Xiaomi’s camera images

- **Faxploit**
  - Fax machine were hacked using landline network

- **Smart TV**
  - Stalking user activities, enable micro camera and capturing the videos.

- **Smart Bulb**
  - Injecting IR waves to other IoT devices and breaking through the network

Security Breaches (contd..)

- **Smart home**
  - Couple from Milwankee reported their smart home being hacked
  - Their music player volume was controlled, videos were captured by the security cameras, room temperature were controlled by thermostat exploit.

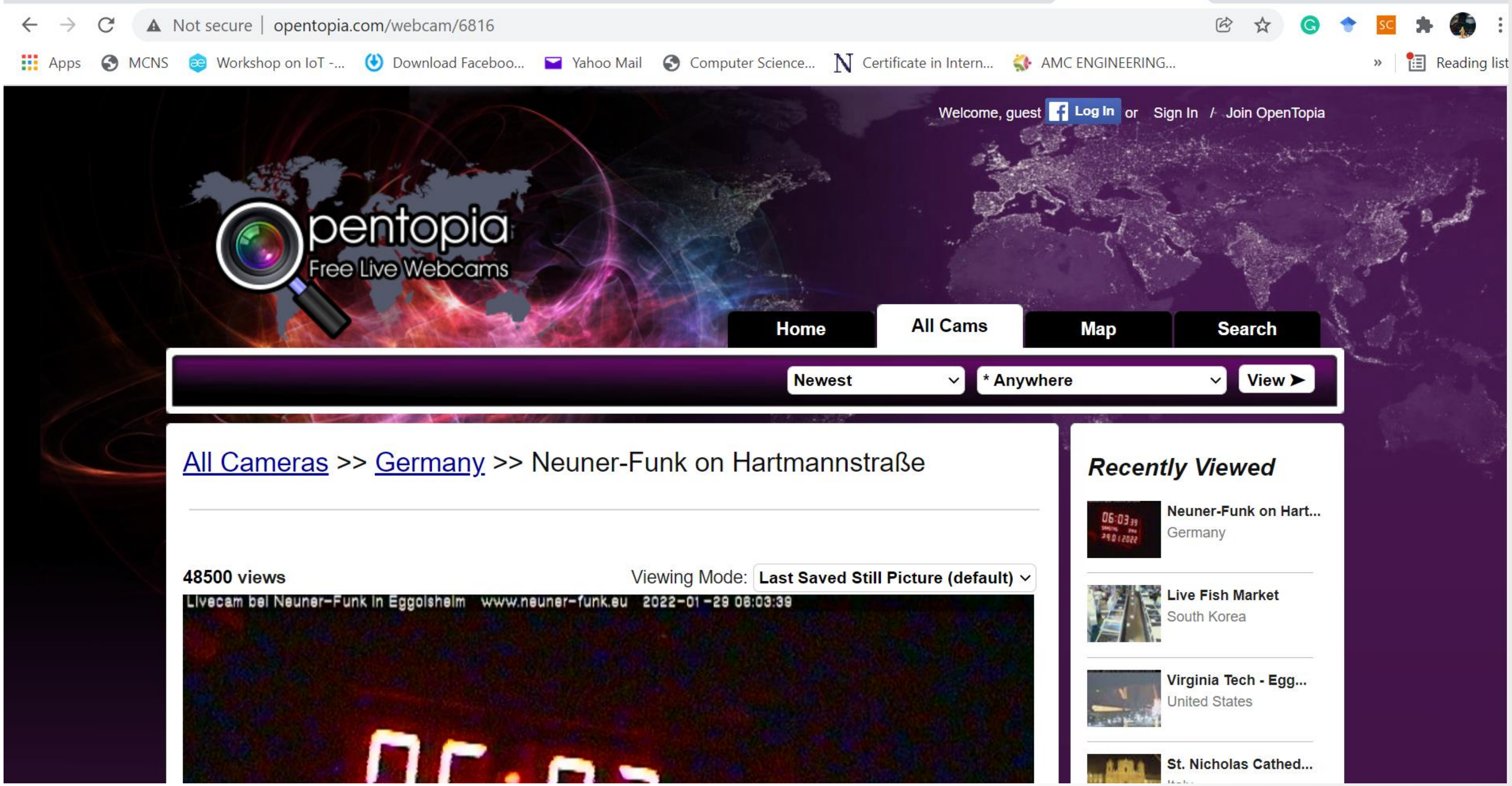
- **Smartphone microphone**
  - Side channel attack

- **Coffee machine hacking, connected printers, smart speakers etc**.
  - Collecting user credit card details and personal information

According to Gartner

40% of smart home appliance globally are being used for botnet attacks

Security Breaches (contd..)



All Cameras >> Germany >> Neuner-Funk on Hartmannstraße

48500 views

Viewing Mode: Last Saved Still Picture (default)

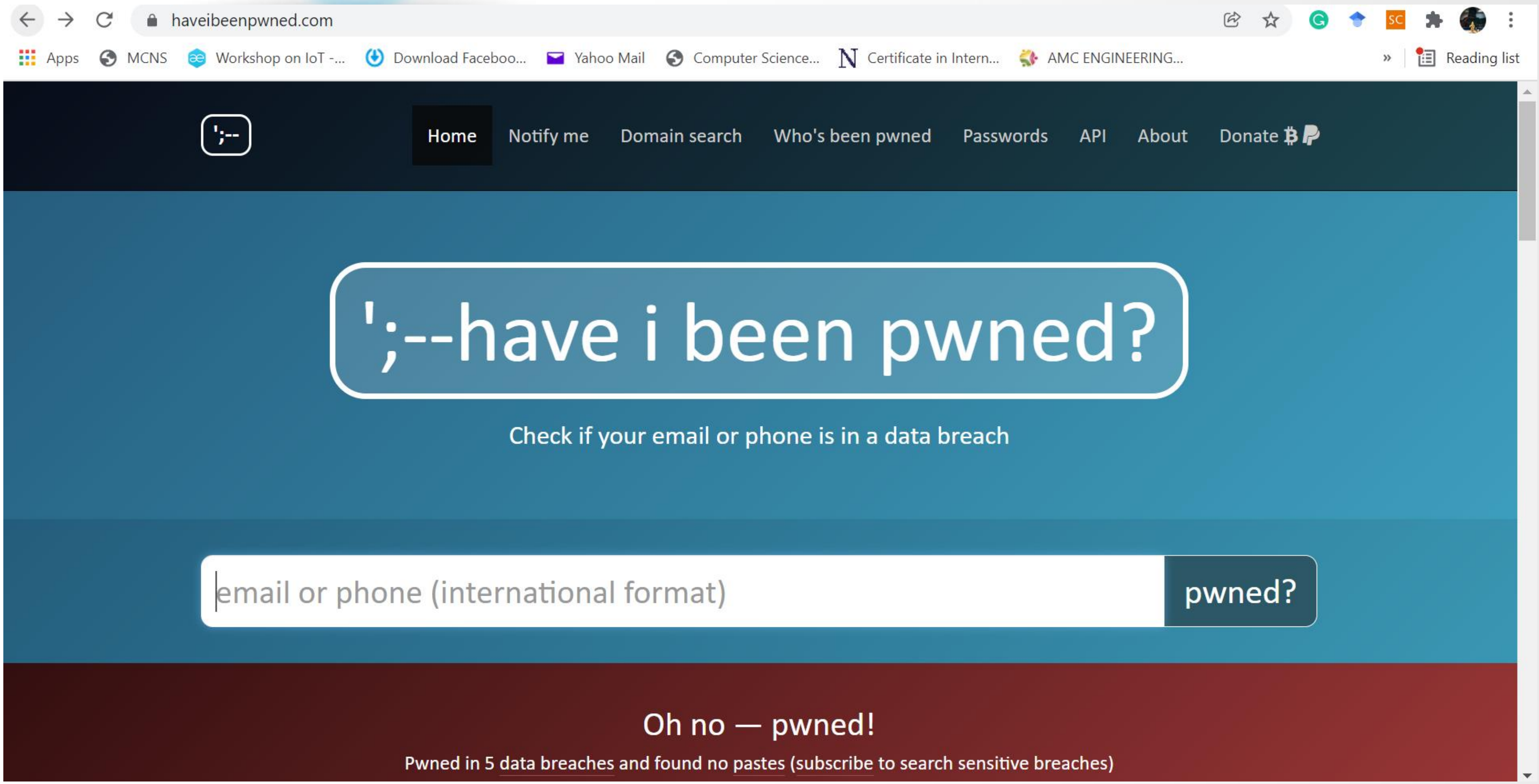
Livecam bei Neuner-Funk in Eggolsheim www.neuner-funk.eu 2022-01-29 06:03:39

Recently Viewed

- Neuner-Funk on Hart... Germany
- Live Fish Market South Korea
- Virginia Tech - Egg... United States
- St. Nicholas Cathed...

http://www.opentopia.com/webcam/6816

Security Breaches (contd..)



';--have i been pwned?

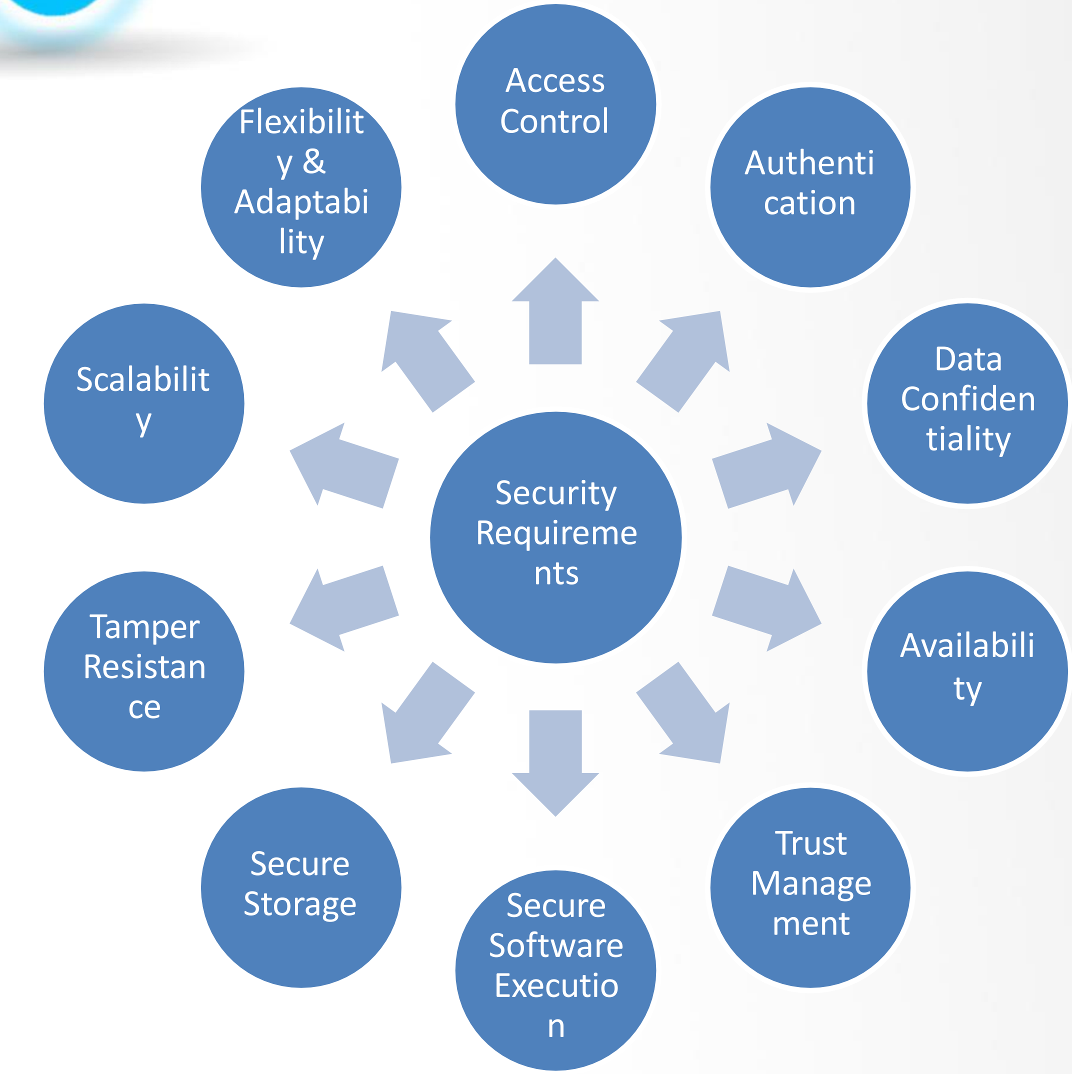
Check if your email or phone is in a data breach

Oh no — pwned!

Pwned in 5 data breaches and found no pastes (subscribe to search sensitive breaches)

https://haveibeenpwned.com/

Security Requirements



Security Requirements

Access Control

Authentication

Data Confidentiality

Availability

Trust Management

Secure Software Execution

Secure Storage

Tamper Resistance

Scalability

Flexibility & Adaptability

Security Requirements (contd..)

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

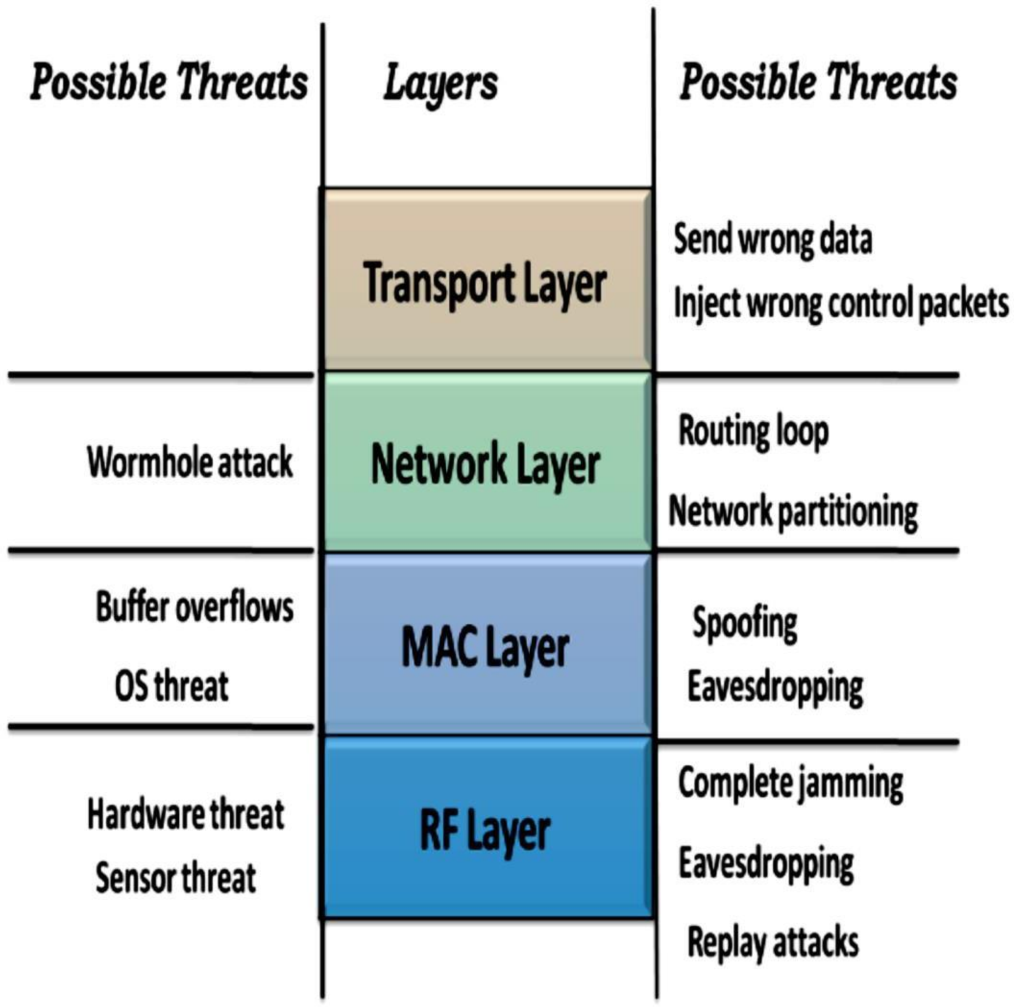
Security Requirements

- **Availability**
  - 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**
  - 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.)
- **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

IoT Security Tomography



Possible Threats	Layers	Possible Threats
	Transport Layer	Send wrong data Inject wrong control packets
Wormhole attack	Network Layer	Routing loop Network partitioning
Buffer overflows OS threat	MAC Layer	Spoofing Eavesdropping
Hardware threat Sensor threat	RF Layer	Complete jamming Eavesdropping Replay attacks

Security Protocols

Protocol	Layer	TCP/UDP	Security
6LowPAN (IPv6 over Low-Power Wireless Personal Area Networks)	**Network**	**TCP**	**SSL (Secure Sockets Layer)**
MQTT (Message Queue Telemetry Transport)	**Application**	**TCP**	**SSL**
AMQP (Advanced Message Queuing Protocol)	**Application**	**TCP**	**SSL**
CoAP (Constrained Application Protocol)	**Application**	**UDP**	**DTLS (Datagram Transport Layer Security)**
XMPP (Extensible Messaging and Presence Protocol)	**Application**	**TCP**	**SSL**
DSS (Digital Signature Standard)	**Application**	**TCP/UDP**	**SSL**

Key Elements of Security

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

Done…!!