EBU6501 - Middleware
Week 3, Day 2: Internet of Things Protocols

Gokop Goteng & Ethan Lau

Queen Mary
University of London

Original version created by: Dr. Gokop Goteng

Lecture Aim and Outcome

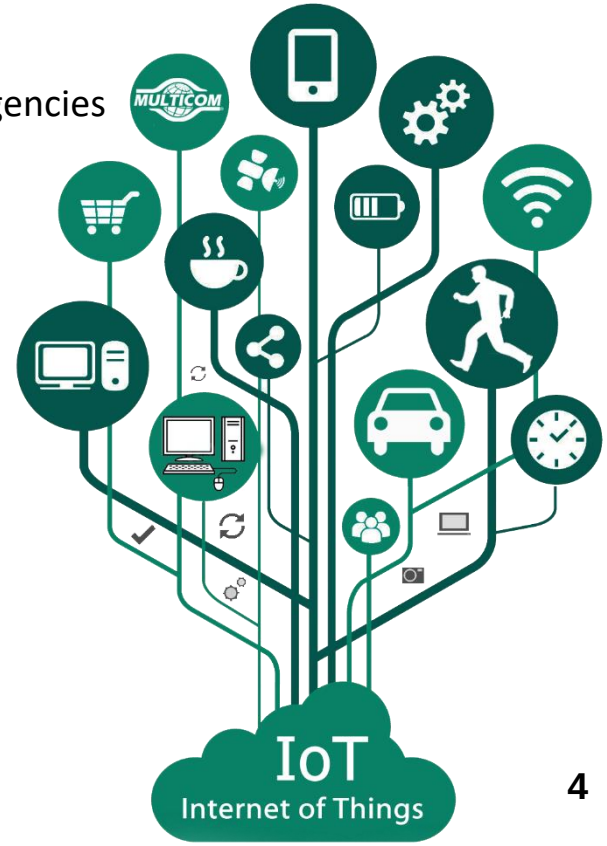
- Aim
  - The aim of this lecture is to teach students the most common protocols used in the current internet of things (IoT) framework
- Outcome
  - At the end of this lecture students should be able to:
    - Know the importance and applications of protocols within the IoT framework
    - Know the common IoT protocols and their roles
    - Know how to use IoT protocols for different applications

Lecture Outline

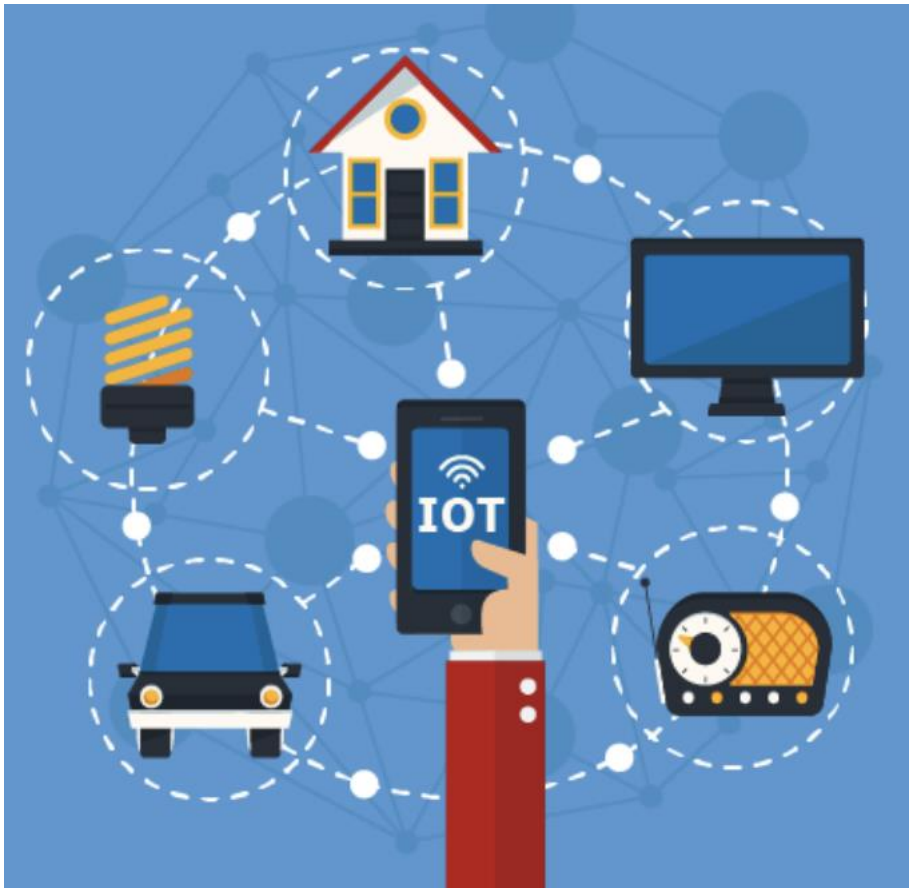
- Definition of IoT
- List of Some IoT Protocols
- Explanations of the IoT Protocols
- Class Works in Between the Session
- Summary

What is Internet of Things (IoT)?

- IoT is the:
  - Interconnection of individually unique and identifiable internet components
  - The components are embedded within the structure or framework of the internet
  - They use different protocols, domains, hardware, software and application platforms
  - The "Things" hosted by the internet can be:
    - Sensor-based automobiles
    - Devices for search and rescue operations
    - Smart thermostat systems
    - Smart washers/dryers for remote monitoring
    - Smart robots to monitor old people at home and report emergencies
    - Driverless cars
    - Heart monitoring implants
    - Biochip transponders on farm animals
  - Applications
    - Energy management
      - Smart grid
    - Health care systems
    - Home automation
    - Transport systems
    - Environmental monitoring
    - Infrastructural management
    - Large scale deployments



IoT in Smart homes



The Internet of Things

From connecting devices to human value

01 Device connection

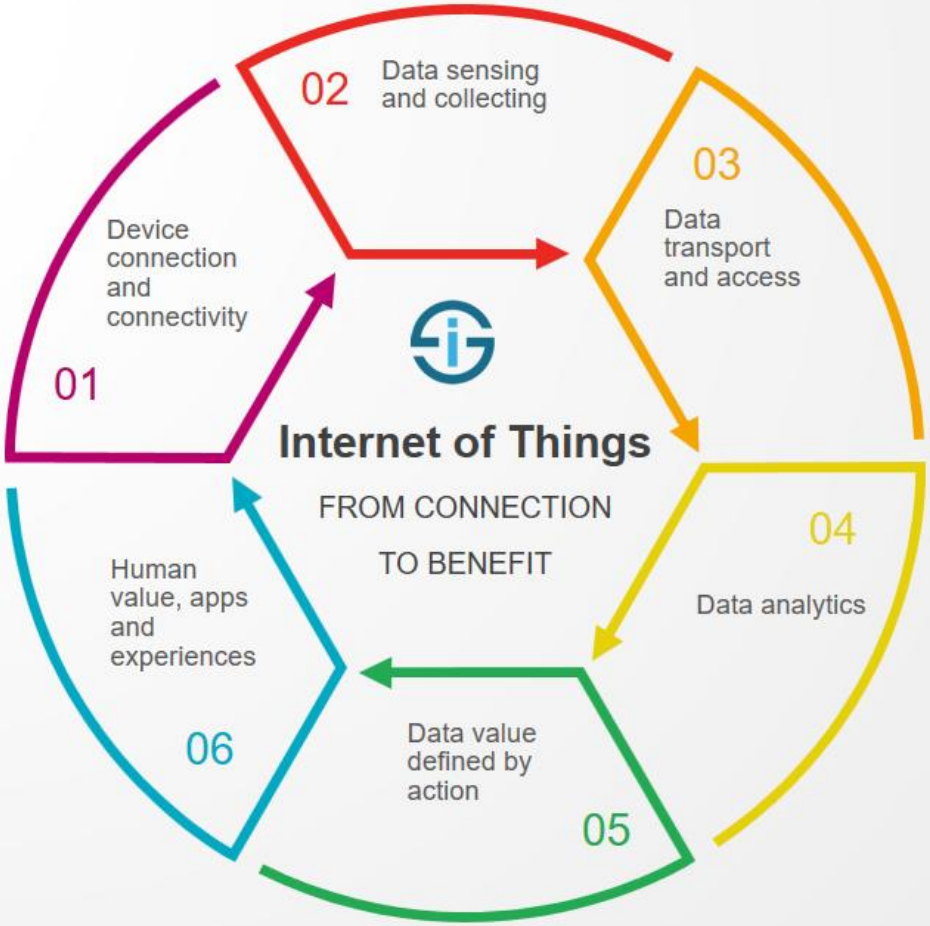
IoT devices
IoT connectivity
Embedded intelligence

02 Data sensing

Capture data
Sensors and tags
Storage

01 Communication

Focus on access
Networks, cloud, edge
Data transport



Data analytics 04

Big data analysis
AI and cognitive
Analyis at the edge

Data value 05

Analysis to action
APIs and processes
Actionable intelligence

Human value 06

Smart applications
Stakeholder benefits
Tangible benefits

Source: https://www.i-scoop.eu/internet-of-things-guide/

What are Communication Protocols?

- Set of digital rules that facilitate efficient and secure data exchange (text, video, audio, graphics, etc) between computing systems
- For this to happen:
  - There are standard data formats for different types of communications using different protocols
  - Address formats for data exchange
  - Address mapping
  - Errors checks
  - Security checks
  - Sequence control
  - Flow control

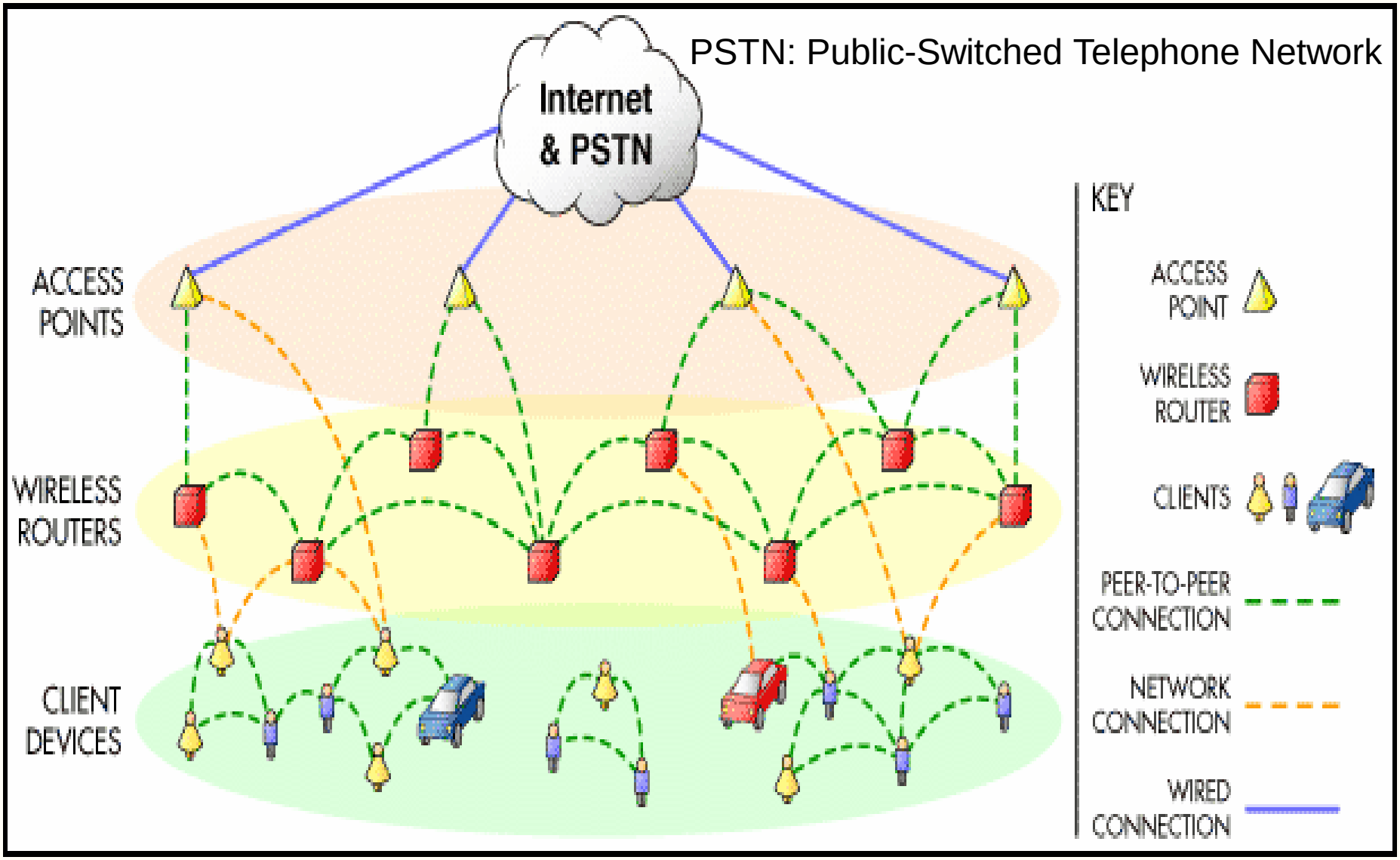
The IEEE 802 Committee Family of Protocols

- The Institute of Electrical and Electronics Engineers (IEEE) committee 802 defines physical and data link technologies and has subsets of **Open Systems Interconnection (OSI) link layer** into two sub-layers from the **Data Link Layer** as:
  - **Media-Access Control (MAC) layer**: This is located on top of the physical layer (PHY) and implements the methods used to have access to the network
    - Eg Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) used by Ethernet and Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) used by IEEE wireless protocols
    - CSMA/CD - Communications in both directions but not at the same time.
  - **Logical Link Control (LLC) layer**: This is used to format the data frames sent over the communication channels through the MAC and PHY layers.

IP-Based Protocols

- Most of the IEEE 802 (eg 802.15.4) protocols and battery-powered networks are considered incapable of running IP (Internet Protocols).
  - In homes and industrial automation networks, LANs (Local Area networks) are used in the 1980s
  - But LANs and WANs (Wide Area Networks) now use IP for communication
- **6LoWPAN** and **RPL**
  - 6LoWPAN stands for **IPv6 over Low Power Wireless Personal Area Networks**
    - 6LoWPAN is created with specification by the Internet Engineering Task Force (IETF) to allow even the smallest and low power devices to use IP so that they can participate in IoT applications.
  - RPL stands for **Routing Protocol for Low power and Lossy networks** and is created with specification of IETF
    - This is created to create an IP level routing protocol that can adapt to requirements of mesh networking for IoT
    - RPL is specifically created for the needs of IPv6 communication over low power networks

Mesh Networks



Source: http://www.meshnetworks.com/

Why is it important?

Representational State Transfer (REST)

- REST specification says that all interfaces must be **uniform** based on the concept of exchanging resources between the client and the server
- Communication should be **stateless and each request** from **client to server must contain all the information needed** (data, metadata, etc)
- These constraints make REST sometimes **too rigid (hard/inflexible)** to be used in some IoT applications

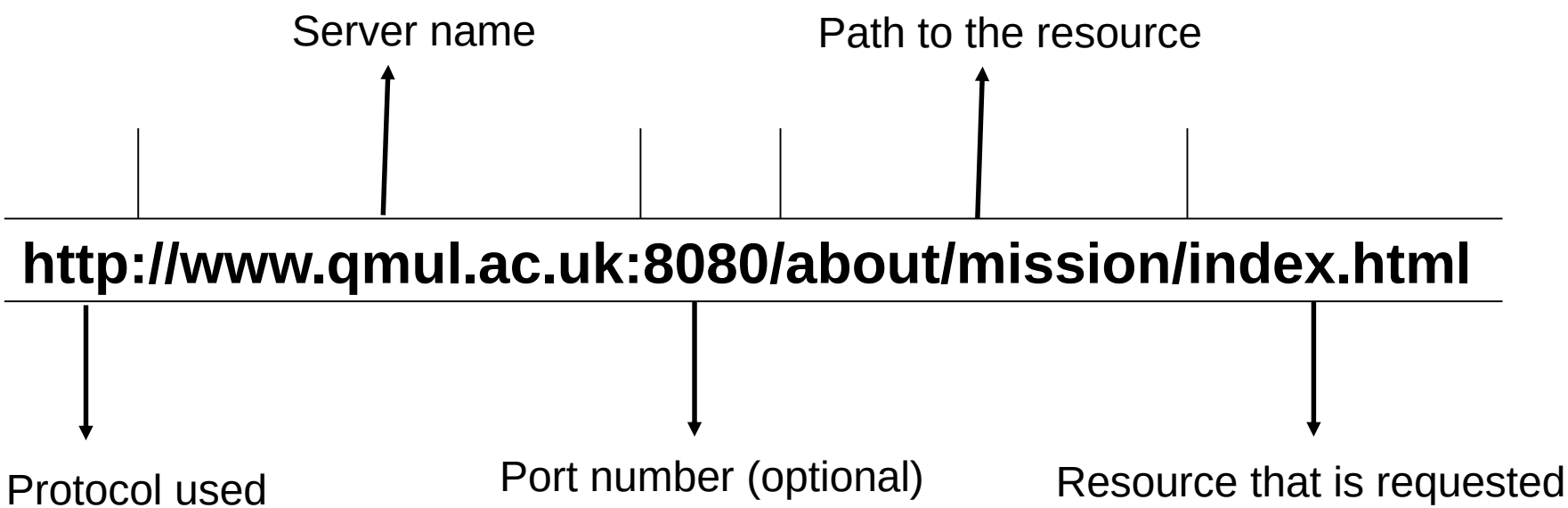
Some IoT Protocols

- HTTP-Hypertext Transfer Protocol
- HTTPS- Hypertext Transfer Protocol Secure or Secure Hypertext Transfer Protocol
- Internet Protocol Suite (IPS) or popularly know as TCP/IP- Transmission Control Protocol/Internet Protocol
- UDP-User Datagram Protocol
- SOAP-Simple Object Access Protocol
- FTP-File Transfer Protocol
- SFTP-Secure File Transfer Protocol
- SSH-Secure Shell
- REST-Representational State Transfer
- MQTT-Message Queue Telemetry Transport
- XMPP-Extensible Messaging and Presence Protocol
- DDS- Data Distribution Service
- AMQP-Advanced Message Queuing Protocol
- Bluetooth Protocols
- RTPSP – Real Time Publish-Subscribe Protocol
- SSL-Secure Socket Layer
- TLS-Transport Layer Security
- POP-Post Office Protocol
- PPP-Point to point Protocol
- NTP-Network Time Protocol
- IMAP-Internet Network Access Protocol
- LDAP-Lightweight Directory Access Protocol
- Bitcoin Protocol

HTTP-Hypertext Transfer Protocol

- The **main building block** for data communication for the world wide web (WWW)
- It is an **application level communication** protocol
- It is the **main facilitating protocol** for collaboration and distributed systems over the web
- It's major function is to implement the **request and response functionalities** of **web applications**
- It is typically used in a **client-server applications**
  - Web-browsers serve as the client and remote systems serve as the servers

HTTP Structure



HTTPS?

- Discussion based on HTTP

TCP/IP-Transport Control Protocol/Internet Protocol

- Set of **computer networking communication protocols**
- Considered as a suite of communication protocols
- It is used for **internet communications** as well as other forms of communication networks such as LAN, WAN, etc.
- It is an **end-to-end communication protocol**
- It consists of "**Linked Layers**" that perform different tasks of sending data across between networks
  - **Internet layer**
    - **Sends packets of data** from the source network **to single or multiple destination networks**
    - Uses the "**IP Address**" (e.g. 10.20.40.8) as the host address for identification
    - The concept of sending packets of data across is known as "**packet routing**"
  - **Transport layer**
    - It is a **connection-oriented end-to-end message transmission layer**
    - It provides reliable data transmission that
      - Data will arrive destination in the order it was sent
      - The should be correct without errors
      - Data that could not be sent will be resent
      - Controls traffic problems
      - Duplication of data is avoided
  - **Application layer**
    - This consists of **other application specific protocols** that allow exchange of data or provides some services
    - This includes the FTP, HTTP, simple mail transfer protocol (SMTP), etc

UDP-User Datagram Protocol

- It is a **connectionless-oriented** communication transmission protocol
- It is part of the TCP/IP suite
- It **does not** have a reliable system for data order, data error checks, and checking to correct duplication of data
- It is good for transmitting data that **accuracy and reliability are not necessary**
- It is used for **transmitting video**, **music, graphics**, etc
- It is faster than TCP/IP as it **does not** check for accuracy and data duplications

SOAP-Simple Object Access Protocol

- It is a **specification** for **exchanging structured d**ata across the web as web services
- It uses the **application layer protocols** in the TCP/IP suite
- It uses the XML (**Extensible Mark-up Language**) syntax
- It has some good features
  - **Neutrality:** Can run on all platforms and works well with most protocols
  - **Non-platform dependence**: It can run on any programming models and languages
  - **Scalability and extensibility**: It can perform well with additional functionalities as well as extends its web services security capabilies without problem.

FTP/SFTP – File Transfer Protocol?

- Class discussions

FTP

- The **File Transfer Protocol** (**FTP**) is a standard network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the internet.
- It is built on a client-server architecture
- It is not secure
  - SFTP is the secure version of FTP

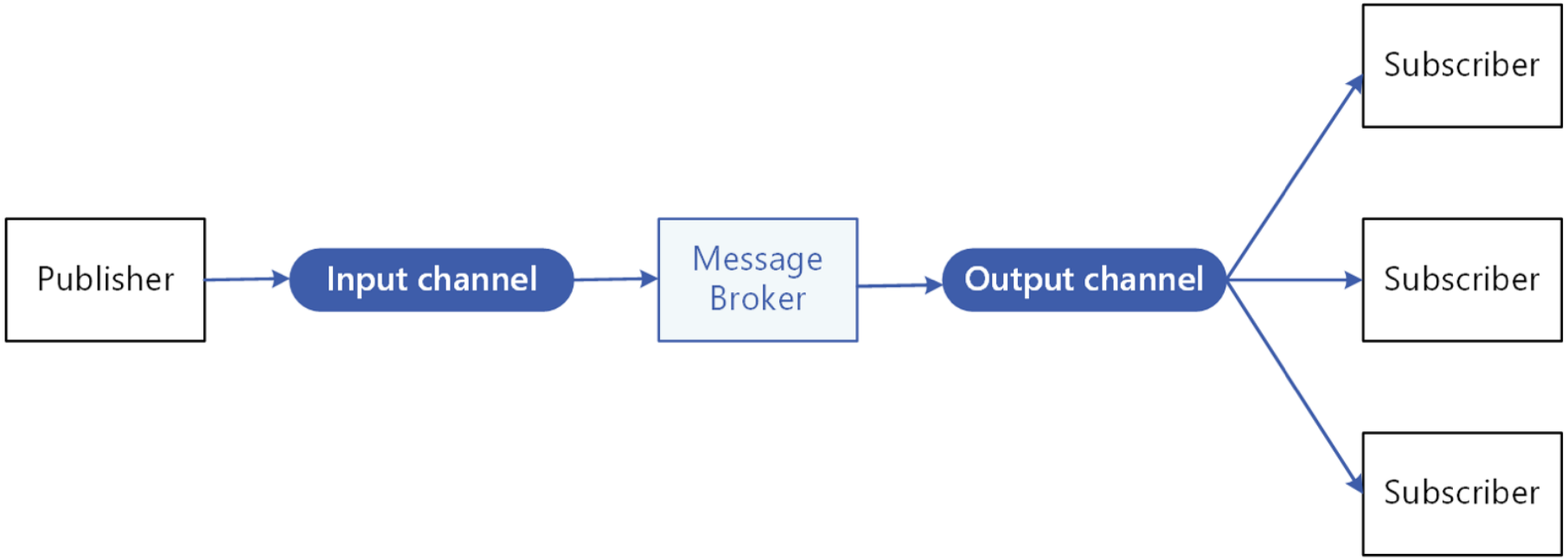
SSH-Secure Shell

- It is the most popular communication and login protocol for UNIX (Linux) systems
- It can also be used on Windows systems
- It **encrypts data** and **communication/login information**
- It uses the **public key infrastructure (PKI) cryptography technology** for **authentication**
- It uses **port "22"** as a standard for communication
- Popular applications that use SSH are Putty, VNC and WinSCP

MQTT-Message Queue Telemetry Transport

- This is a **messaging service protocol**
- It is based on the **publish-subscribe messaging service model**
- It is used on top of TCP/IP protocol
- It is used to improve network communication where the network bandwidth is poor for remote communications
- It uses **brokers** that **publish messages**
- It is used by **Facebook Messenger**

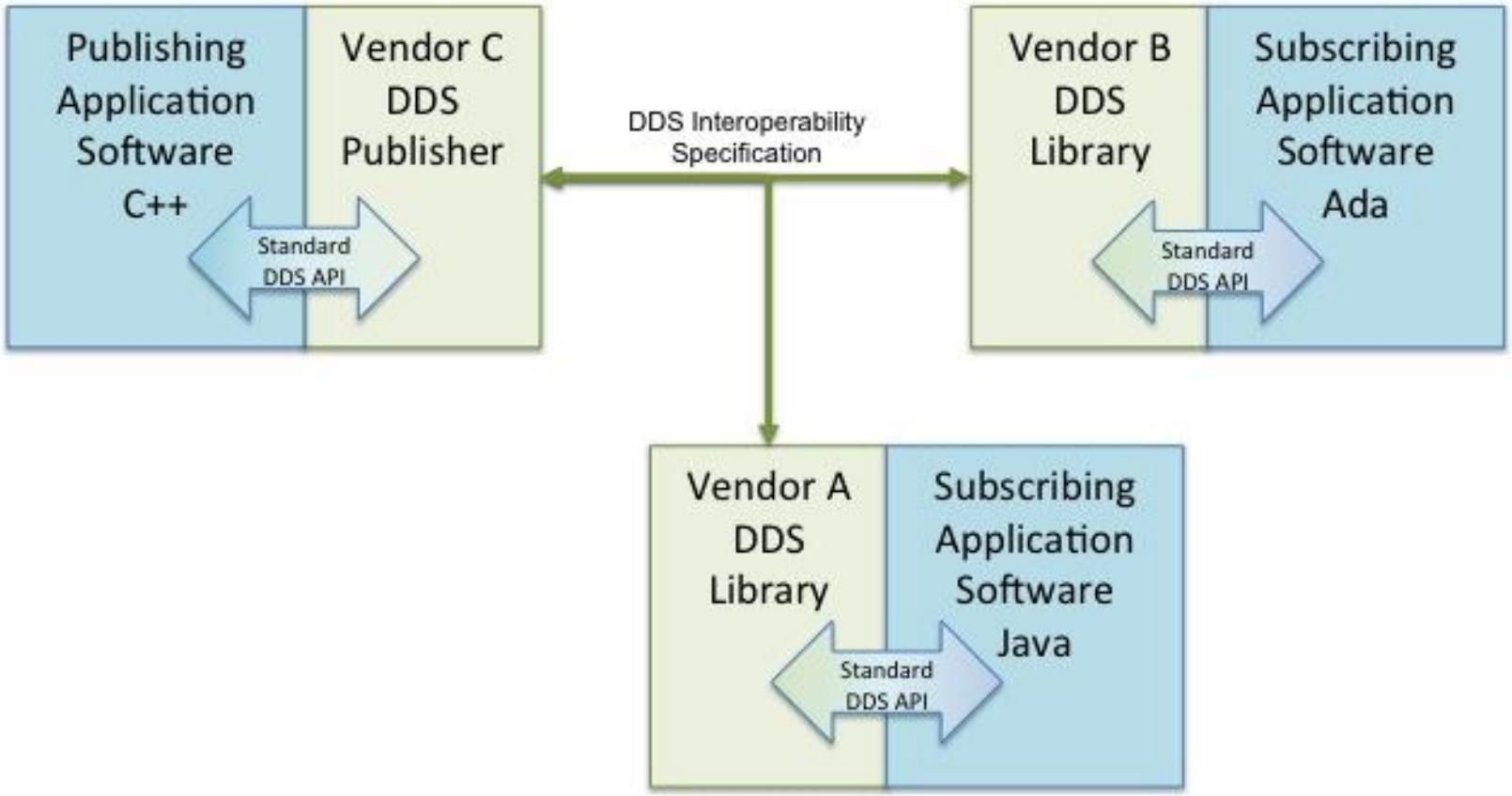
Publish-subscribe pattern



DDS-Data Distribution Service

- This is a machine-to-machine (M2M) middleware standard
- It enables **reliable exchange of data between heterogeneous systems** used by **cloud service** providers and subscribers
- It works on a **real-time basis** to manage **dynamic data exchange** and communication in cloud systems
- It is managed by the Object Management Group (OMG)

DDS-Data Distribution Service Heterogeneous Model



Source: Object Management Group (OMG) Documentations

AMQP-Advanced Message Queuing Protocol

- This is a **message-oriented middleware** (MOM) protocol
- It is based on the open standard application layer model
- In enables heterogeneous clients and servers to communicate using **point-to-point** or **publish-subscribe messaging** methods
- It is the main protocol used by Apache Qpid framework

RTPSP – Real Time Publish-Subscribe Protocol

- It is a **message oriented protocol**
- It works on **delivering real-time message exchange** services using the **publish-subscribe method**
- **Cloud-based messages** use RTPSP to exchange data between heterogeneous systems
- Cloud providers use it to implement multi-vendor DDS systems
- It enforces **Quality of Service (QoS)** for cloud service providers based on performance metrics defined in the service level agreements

SSL/TLS-Secure Socket Layer/ Transport Layer Security

- These are **cryptographic protocols for secure communication over the internet**
- They are based on Kerberos X-509 cryptography
- They use **digital certificates** for authentication
- They implement **data confidentiality** and **data integrity**

NTP-Network Time Protocol

- It is a **global networking protocol** for **synchronising time zone settings** on computer systems
- It **stabilises** the **variations in network latency** for distributed systems communicating with each other
- It is used in some applications that depend on accuracy of time to function correctly
- It is not a secure protocol and is prune to "**man-in-the-middle-attacks** (MIMA)", e.g. eavesdropping

IMAP-Internet Message Access Protocol

- This protocol enables users to **retrieve their emails and also for data storage**
- It is an **internet application layer** protocol
- It is similar to the Post Office Protocol (POP), but unlike POP, allows **multiple users to simultaneously access the same mailbox**
  - POP is an application layer protocol for local email clients to retrieve email from a server over a TCP/IP network
- It has many versions now such as IMAP2, IMAP3, etc

LDAP-Lightweight Directory Access Protocol

- It is an **application layer protocol**
- It used for **accessing distributed directory information services** over TCP/IP network
- It is the most popular tools to **share and use information record**s on users, systems, networks and services over an entire network
- LDAP is used to manage **large scale authentication** and **authorisation** systems for distributed **cloud** systems

Applications of IoT Protocols

- Smart Grid
  - This is an electrical grid which is equipped with smart meter readings, efficient energy usage, etc
- Home appliances automation
  - Control of home appliances such as fridge, cooker, heater, etc remotely
- Car hiring services
  - Uber, etc
- Food collection/delivery services
  - Uber, etc

Applications of IoT Protocols

Food collection/delivery services

小编推荐

百度外卖
2018-04-23 / 17.0M
下载
推荐理由：百度外卖App由百度打造的一个生活服务类平台，目前已开通城市：北京，上海，杭州，南京，苏州，更多城市
版本：PC版 | 安卓版 | 苹果版

最多下载

饿了么app
2018-05-10 / 31.1M
下载
推荐理由：饿了么App网上订餐非常简单，只要你有订餐需求，只需在饿了么app平台上搜索目标餐馆，查看上面的菜单
版本：PC版 | 安卓版 | 苹果版

最受欢迎

美团外卖
2018-05-02 / 25.8M
下载
推荐理由：美团外卖App是一款手机叫外卖软件，手机订外卖，吃货新时代。美团外卖App对于那些爱吃又很宅的人来
版本：PC版 | 安卓版 | 苹果版

推荐

口碑外卖app
2018-05-19 / 44.5M
下载
推荐理由：口碑外卖app是一款手机外卖软件，下雨天点个外卖还是挺方便的。小编特别喜欢周四的优惠券，约朋友吃饭真
版本：安卓版 | 苹果版

推荐

外卖超人
2016-04-04 / 4.7M
下载
推荐理由：外卖超人是全球最大的在线订餐平台之一，服务覆盖四大洲13个国家，实时提供外卖资源...
版本：PC版 | 安卓版 | 苹果版

推荐

肯德基宅急送
2016-10-06 / 5.2M
下载
推荐理由：肯德基宅急送是肯德基官方制作的一款订餐app，除了在手机上快速实现订餐功能外，还有优惠活动、查询订单
版本：安卓版 | 苹果版

麦当劳麦乐送
2016-05-21 / 9.0M
下载
推荐理由：麦当劳麦乐送是著名餐饮品牌麦当劳的外送品牌，麦当劳中国全新推出的手机订餐APP客户端，立即下载订餐
版本：安卓版 | 苹果版

点我吧外卖
2016-10-09 / 9.1M
下载
推荐理由：点我吧外卖是一款很力的外卖软件，支持点我吧外卖的餐厅饭菜好吃哇哇的，送餐小哥速度飕飕的，点我吧外
版本：安卓版 | 苹果版

我有外卖
2017-04-06 / 6.8M
下载
推荐理由：我有外卖App，登陆北京，上海，深圳，广州
头啦，引爆五地美食盛事，一键轻松解决吃饭烦恼，还
版本：安卓版 | 苹果版

Bitcoin Protocol ?

- Discussions in the class
- Bitcoin network
- Bitcoin currency

Bitcoin in Finance and e-Commerce

- **Bitcoin** is an experimental, **decentralized digital currency** that enables instant payments to anyone, anywhere in the world.
- **Bitcoin** uses **peer-to-peer technology** to operate with **no central authority**
  - managing transactions and issuing money are carried out collectively by the network
- **Transactions:**
  - Are **irreversible** by design
  - Are **fast**. Funds received are available for spending within minutes.
  - **Cost very little**, especially compared to other payment networks.
  - The supply of bitcoins is **regulated by software and the agreement of users** of the system and **cannot be manipulated** by any government, bank, organization or individual.
  - The limited inflation of the Bitcoin system's money supply is distributed evenly (by CPU power) to miners who help secure the network.
- **Bank:**
  - Everyone collectively is the bank
- **Pioneers**
  - **Satoshi Nakamoto** is the pseudonymous person or group of people who designed and created the original Bitcoin software

Bitcoin in Finance and e-Commerce

- **Bitcoin** - **new currency** that was created in 2009 by an unknown person using the alias Satoshi Nakamoto.
- **Transactions** are made with no middle men
  - Meaning, no banks!
  - There are no transaction fees and no need to give your real name.
  - More merchants are beginning to accept them:
    - You can buy webhosting services, pizza or even manicures.
- **Why Bitcoins?**
  - Bitcoins can be used to **buy merchandise anonymously**.
  - In addition, international payments are easy and cheap because **bitcoins are not tied to any country or subject to regulation**.
  - Small businesses may like them because there are **no credit card fees**.
  - Some people just buy bitcoins as an investment, hoping that they'll go up in value.
- **How to Own Bitcoins?**
  - Bitcoins are stored in a "**digital wallet**," which exists either in the cloud or on a user's computer.
  - The wallet is a kind of virtual bank account that allows users to send or receive bitcoins, pay for goods or save their money.

Bitcoin as a Technology

- Bitcoin uses a peer-to-peer (P2P) network protocol
- Uses the SHA-2 cryptographic hash functions
  - SHA: **Secure Hash Algorithm**
  - Consists of six hash functions with hash values that are 224, 256, 384 or 512 bits: **SHA-224 (Secure Hash Algorithm 224), SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256**.
- Uses DSA to sign transactions digitally
  - **DSA: Digital Signature Algorithm**
- Transactions verification
  - Transactions are **cryptographically signed** records that reassign ownership of Bitcoins to new addresses.
  - Transactions have
    - ***Inputs*** - records which reference the funds from other previous transactions
    - ***Outputs*** - records which determine the new owner of the transferred Bitcoins, and which will be referenced as inputs in future transactions as those funds are re-spent.

Summary

- IoT Protocols
- Applications of IoT Protocols
- Class Work
- Reflection on Pre-Class Work