Background on IoT

IoT Overview

- The Internet of Things is a network of physical devices, vehicles, home appliances, etc., embedded with electronics, software, sensors, actuators, and connectivity which enables these things to connect, collect and exchange data [1]
- Allowing devices to connect to the Internet opens them up to serious vulnerabilities if they are not properly protected
- IoT security is the technology area that addresses mechanisms for safeguarding connected devices and networks in the Internet of Things

Three-layer IoT Architecture

- IoT devices are considered to have a three-layer architecture [2]
  1) **Perception Layer**
     Physical layer that gathers environment data
  2) **Network Layer**
     Wired and wireless systems that process and transmit the input obtained by the perception layer supported by corresponding communication technologies
  3) **Application Layer**
     Abstracted solutions that interact with the end users in order to satisfy their needs

IoT Elements

IoT Elements		Examples
Identification	Naming	EPC, uCode
	Addressing	IPv4, IPv6
Sensing		Smart Sensors, Wearable sensing devices, Embedded sensors, Actuators, RFID tag
Communication		RFID, NFC, UWB, Bluetooth, BLE, IEEE 802.15.4, Z-Wave, WiFi, WiFiDirect, LTE-A
Computation	Hardware	SmartThings, Arduino, Phidgets, Intel Galileo, Raspberry Pi, Gadgeteer, Z1, Tmote Sky
	Software	OS (Contiki, TinyOS, LiteOS, Riot OS, FreeRTOS, Android); Cloud (Nimbits, Hadoop)
Service		Identity-related (shipping), Information Aggregation (smart grid), Collaborative-Aware (smart home), Ubiquitous (smart city)
Semantic		RDF, OWL, EXI

IoT Common Standards

Application Protocols		DDS CoAP AMQP MQTT MQTT-SN XMPP HTTP REST
Service Discovery		mDNS DNS-SD
Infrastructure Protocols	Routing Protocols	RPL
	Network Layer	6LoWPAN IPv4/IPv6
	Link Layer	IEEE 802.15.4
	Physical/Device Layer	LTE-A EPCglobal IEEE 802.15.4 Z-Wave
Influential Protocols		IEEE 1888.3, IPSec IEEE 1905.1

IoT Challenges

- Availability
  - Hardware and software can be provided anywhere and anytime to users
- Reliability
  - Increase the success rate of IoT service delivery
  - Implemented in software and hardware at all the IoT layers
- Mobility
  - Connect users with their desired services continuously while on the move
- Performance
  - Continuously develop and improve service to meet customer requirements

IoT Challenges (cont.)

- Management
  - Efficient protocols needed to handle the management issues that will stem from the deployment of IoT in the coming years
- Scalability
  - Add new devices, services and functions for customers without negatively affecting the quality of existing services
- Interoperability
  - Handle many heterogeneous devices belonging to different platforms
- Security and privacy
  - IoT devices require specific mechanisms to protect user privacy, as well as detect and block malicious activities

References

[1] Wikipedia, “Internet of things”, https://en.wikipedia.org/wiki/Internet_of_things

[2] K. Zhao, L. Ge, “A survey on the Internet of Things security,” 9th International Conference on Computational Intelligence and Security (CIS), December 14-15, 2013, pp. 663–667.