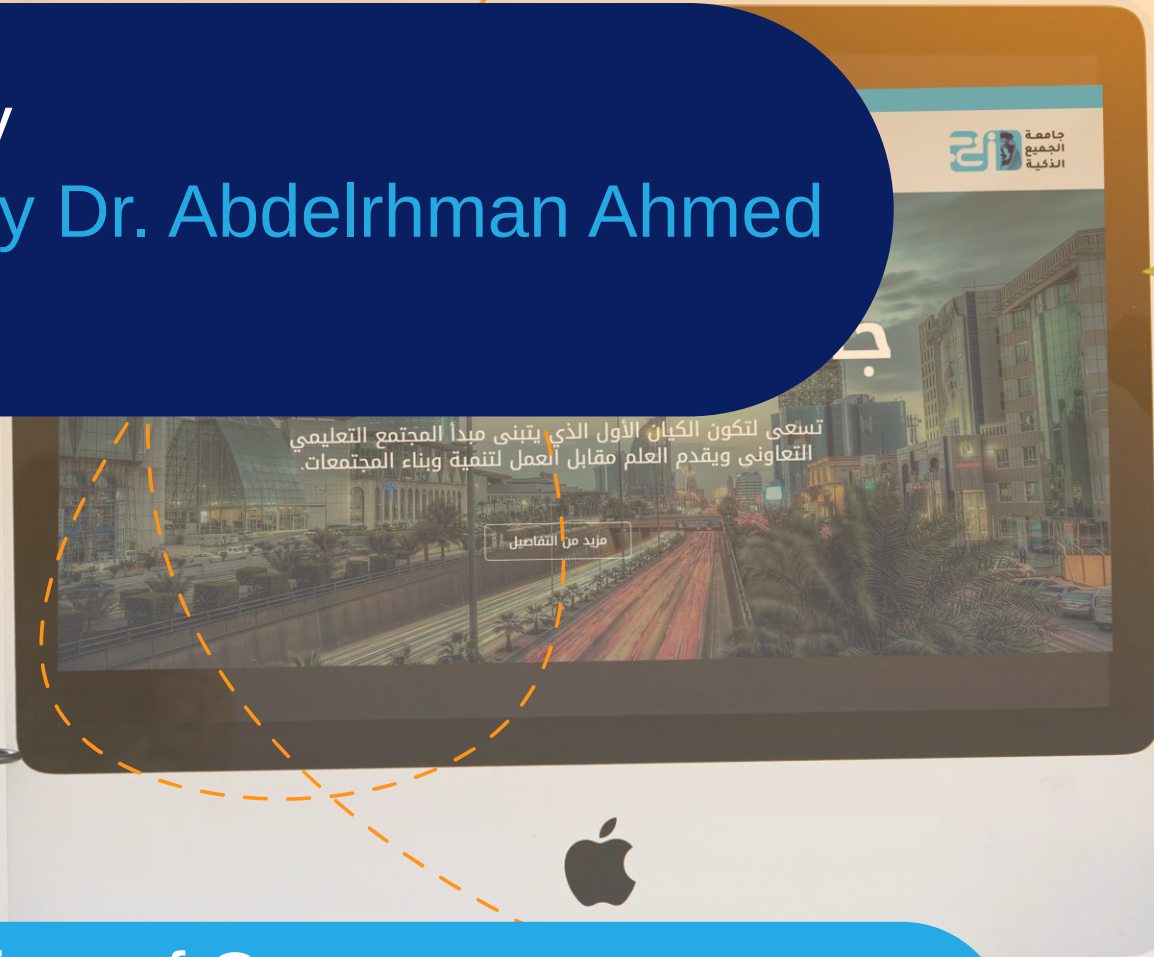


IoT security

Prepared by Dr. Abdelrhman Ahmed

Lecture 2



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

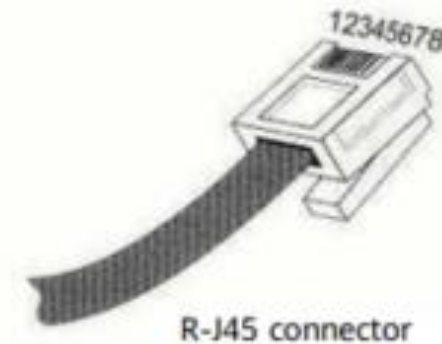
Overview of Common IoT Communications Technologies

- Communications technologies are the foundation of not only the Internet of Things (IoT), but also a fully connected world. If the IoT is a logistics system of information, then communications technologies are the various means of transportation. However, regardless of the technology adopted, the ultimate goal is to connect devices to the cloud-based applications.
- Common communications technologies can be classified into two types: wired and wireless communications technologies. In terms of their applications and technical features, the specifications of wired and wireless technologies vary considerably.

At the end of this course, you will have knowledge of:

- Common IoT wired communication technologies.
- The technical standards, features, and differences between various short-range wireless communications technologies.
- The characteristics and developing trends of cellular mobile communication technologies.
- The characteristics of Low Power Wide Area (LPWA) communications technologies and distinguish between their different types.

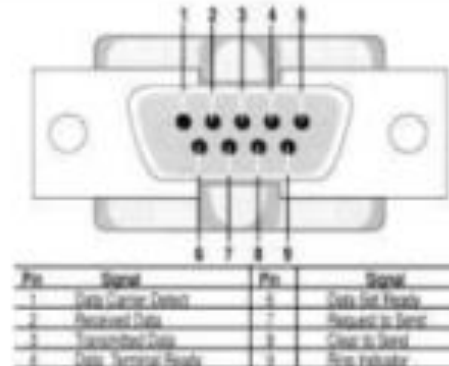
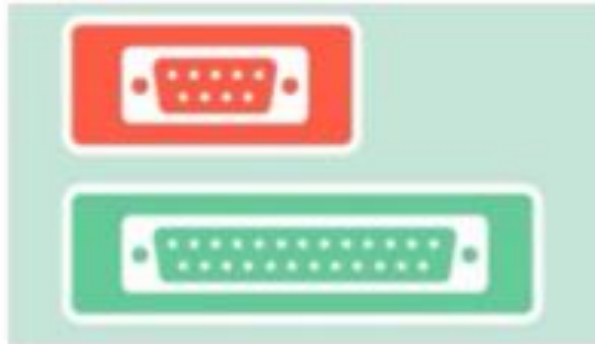
- Ethernet is the main LAN technology of TCP/IP and is named after the medium Ether, which transmits electromagnetic waves.
- A base station can use one ETH port, two FE/GE ports, or two SFP ports. ETH indicates it is a standard Ethernet, which transmits data at the rate of 10 Mbit/s. FE is short for fast Ethernet, which provides a tenfold increased transmission rate of 100 Mbit/s, and GE is short for Gigabit Ethernet, which provides a transmission rate of 1000 Mbit/s. SFP ports are gigabit optical ports, which transmit data over optical fibers. FE/GE enable autonegotiation of transmission rate with the peer switch.
- Carrier sense multiple access with collision detection (CSMA/CD) is the core Ethernet technology. "carrier sense" indicates the detection before transmission, "multi-access" indicates that data sent from one sender is received by multiple receivers, and "collision detection" indicates the detection during transmission.



Chapter 02

Introduction and Comparison Between RS-232 and RS-485

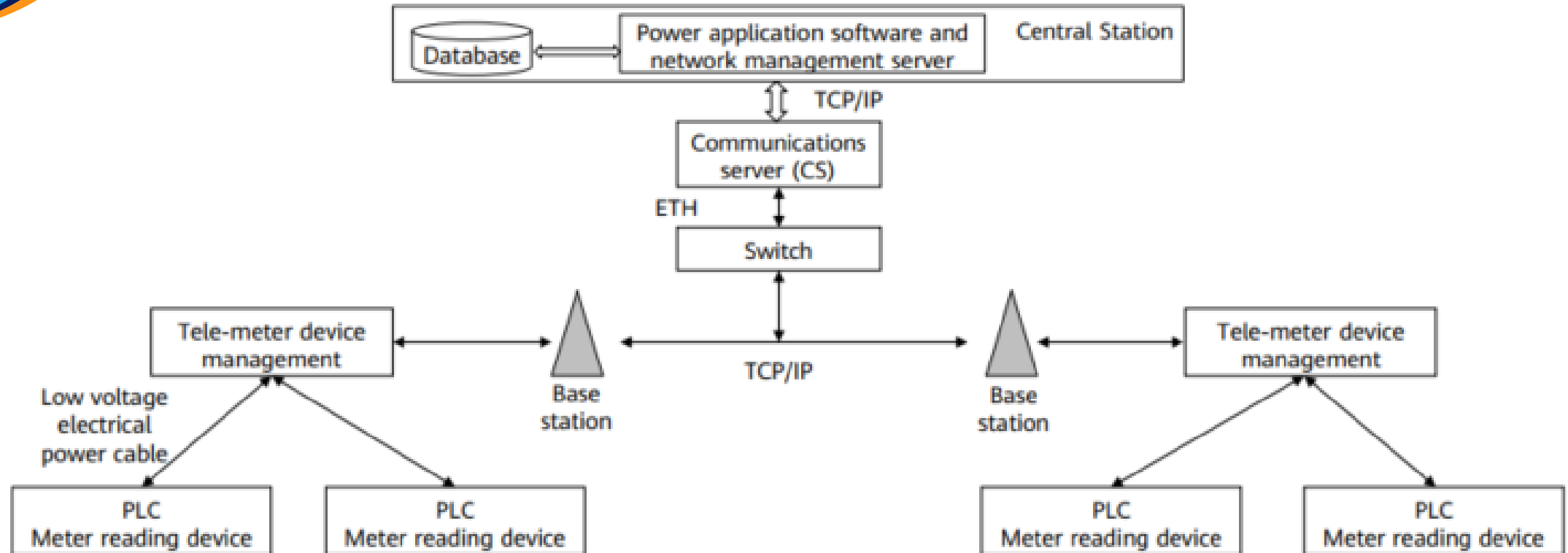
Item	RS-232	RS-485
Communication distance	Less than 20 m	1200 m theoretically; 300-500 m in reality
Transmission mode	Unbalanced transmission mode; single-end communications	Balanced transmission; differential transmission
Number of transceivers	One-to-one communications	A maximum of 128 transceivers on the bus
Transmission rate	38.4 Kbit/s	10 Mbit/s



- USB, short for Universal Serial Bus, is a serial bus standard for connecting computer systems and devices. It is also a technical specification for input and output interfaces. It is widely used with information communications products such as personal computers and mobile devices, and its use has been extended to related fields such as photography equipment, digital TVs (set-top boxes), and game consoles.
- Before USB was developed, the scalability of computer interfaces was inadequate with limited rates due to devices (such as the keyboard, mouse, modem, printer, and scanner) needing to be connected to different interfaces (such as serial/parallel interfaces), making it impossible for a computer to provide sufficient interfaces for connections. USB is designed for high speed, scalability, and ease-of-use.
- The latest-generation USB is USB 4, with a transmission rate of 40 Gbit/s.



- M-Bus, short for Meter Bus, is a data bus designed for information transmission of consumption measuring instruments and counters. M-Bus has been widely applied in business and collection of data on industrial energy consumption.
- The maximum transmission distance of the M-Bus is 1000 m. As the M-Bus can supply power to onsite devices, no power cable needs to be connected. The power supply capability of the bus is 5 A, and the current of each node needs to be less than 0.65 mA.
- The M-Bus not only fulfills the need for the networking and remote reading of utility meters but also meets the specific requirements of the remote or battery power supply system. The bus topology of the M-Bus serial communications meets the requirements of the utility meters for reliable and cost-effective networking. Hundreds of backup devices can also be connected within a distance of several kilometers.



- Power line communication (PLC) refers to a mode of communication in which data and media signals are transmitted on an electrical power cable. With PLC, high frequency signals containing information are loaded onto the current, and the adapter receives the information over the cable, separates the high-frequency signals from current, and then sends the signals to a computer or telephone.

Chapter 02

Comparison of Wired Communications Technologies

Communication Mode	Characteristics	Application Scenario
ETH	Comprehensive protocol, universal, cost-effective	Intelligent terminal, video surveillance
RS-232	One-to-one communications, cost-effective, short transmission distance	A few instruments, industrial control
RS-485	Bus topology, cost-effective, strong anti-interference capability	Industrial instruments, meter reading
USB	One-to-one communications, universal, fast transmission	Smart home, office, mobile devices
M-Bus	Designed for meter reading, common twisted-pair cables, strong anti-interference capability	Industrial energy consumption data collection
PLC	For power line communication, wide coverage, easy installation	Power grid transmission, electricity meter

Chapter 02

Short-Range Wireless Communications Technology: Bluetooth



- Bluetooth is a large-capacity wireless digital communications technology standard for exchanging data over short distances. The latest Bluetooth 5.0 supports a maximum transmission rate of 3 Mbit/s and a transmission distance of about 300 meters. The technology has been divided into two types: Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR) and Bluetooth low energy (BLE). The BR/EDR type supports only point-to-point (one-to-one) communications, whereas the BLE type supports point-to-point, broadcast (one-to-many), mesh (many-to-many), and other modes of communications. The BLE type is mainly used in the IoT field to provide services with higher performance that consume little power for smart home appliances.
- Advantages: high rates, high security, and low power consumption
- Disadvantages: The EDR type, with few network nodes, is not suitable for multi-point deployment.

Chapter 02

Short-Range Wireless Communications Technology: Wi-Fi



Master
concentrator

Trunk and
hotspot

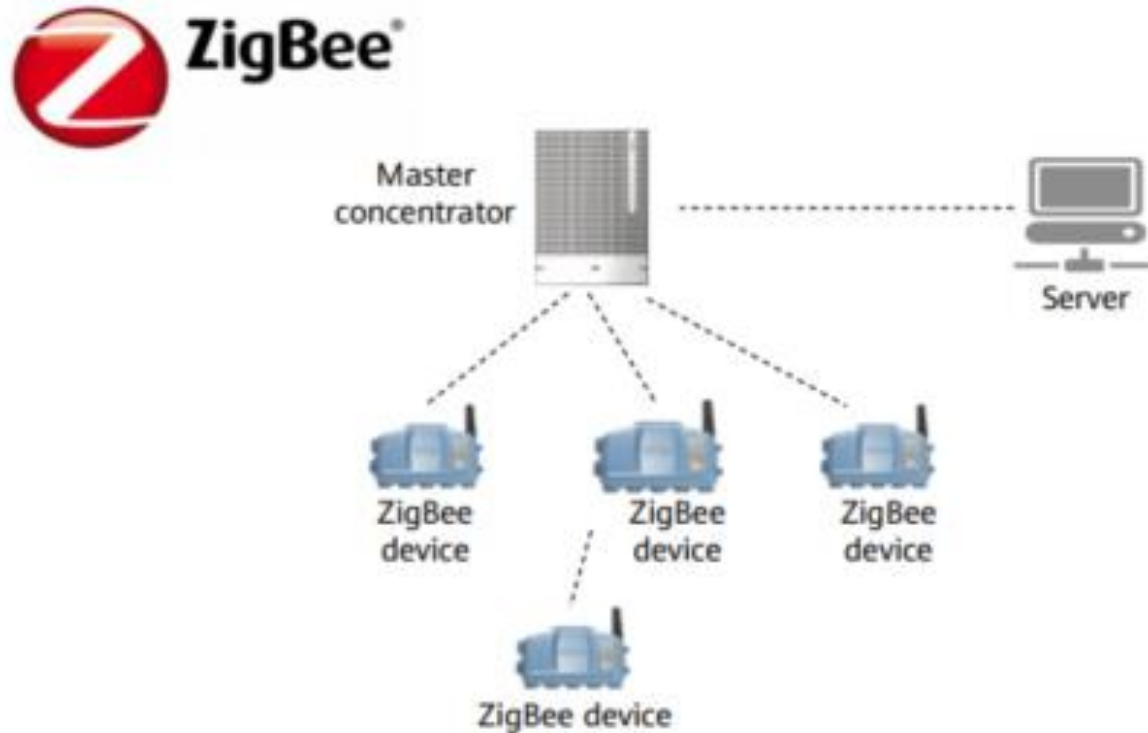
Device



- Wi-Fi enables an electronic device to connect to a wireless local area network (WLAN) using the 2.4 GHz UHF or 5 GHz SHF ISM radio frequency band. The latest Wi-Fi 6 supports a transmission rate of 9.6 Gbit/s and a latency of 20 ms.
- Advantages: wide coverage, fast data transmission rate
- Disadvantages: low transmission security, low stability, high power consumption, poor networking capability

Chapter 02

Short-Range Wireless Communications Technology - ZigBee

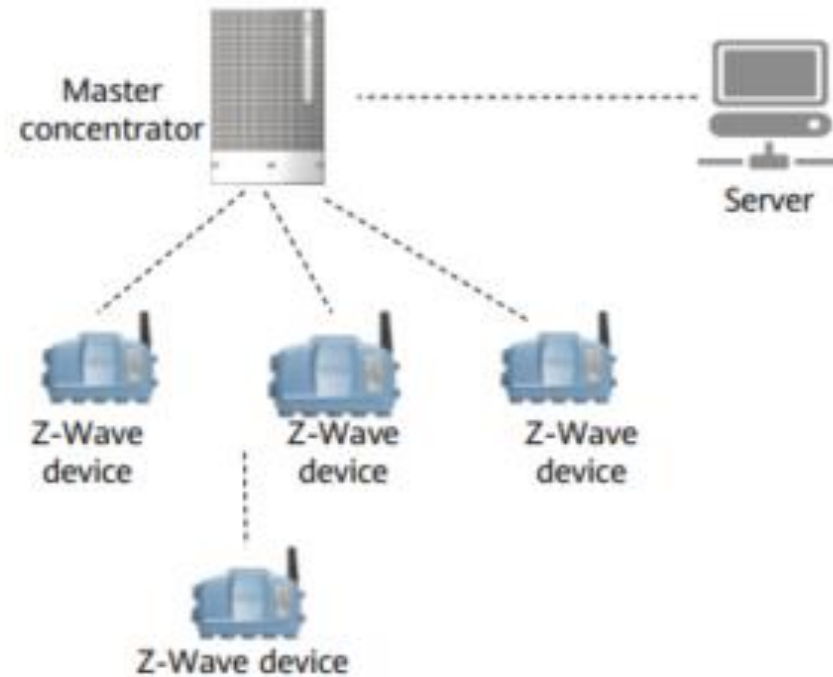


- ZigBee is a short-range wireless communications technology featuring low power consumption.
- Characteristics: short transmission distance, low complexity, self-organization, low power consumption, and low data rate.
Widely used in industrial and smart home fields.

ZigBee	
Low power consumption	Two batteries can support the device for 6-24 months.
Low cost	No patent fee is required and the cost is about US\$2.
Low rate	20-250 Kbit/s
Short distance	10-100 m
Low latency	15-30 ms
Large capacity	The number of nodes theoretically is 254.
High security	Three security levels
Grant free	915 MHz, 868 MHz, 2.4 GHz
Easy networking	Mesh networking, ad hoc networking
Low compatibility	The compatibility of different chips is low.
Difficult maintenance	Difficult to maintain due to high networking flexibility

Chapter 02

Short-Range Wireless Communications Technology - Z-Wave



- Z-Wave is an emerging RF-based wireless communications technology with a short transmission distance and high reliability at low costs and little power consumption.
- Advantages: simple structure, high reliability, low rates, low power consumption, low costs
- Disadvantages: The standard is not open. The chip can only be obtained from Sigma Designs.

Chapter 02

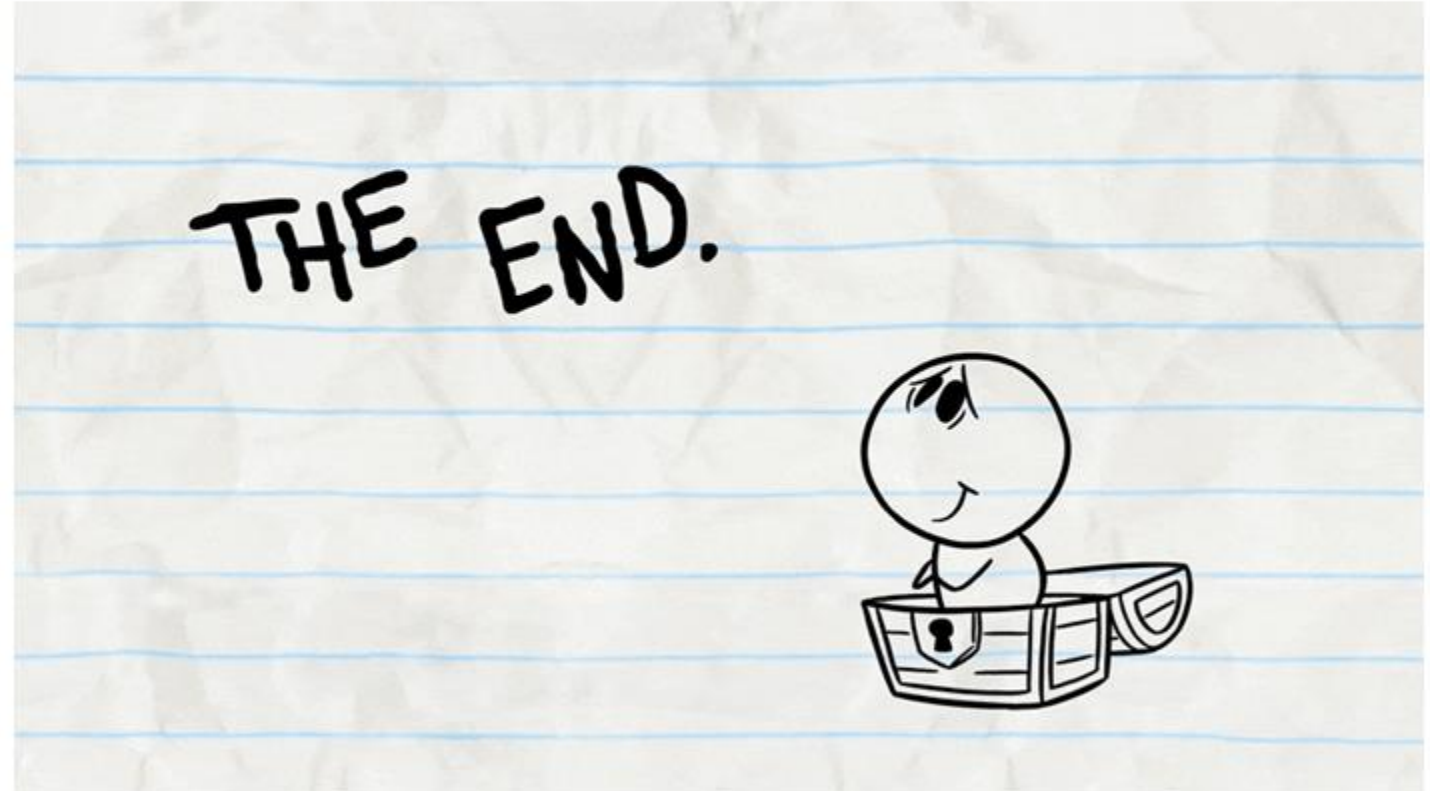
Comparison of Short-Range Wireless Communications Technologies

	Bluetooth	Wi-Fi	ZigBee	Z-Wave
Frequency band	2.4 GHz	2.4 GHz 5 GHz	868 MHz/915 MHz 2.4 GHz	868.42 MHz (Europe) 908.42 MHz (USA)
Transmission rate	1–3 Mbit/s (24 Mbit/s over 802.11 links)	802.11b: 11 Mbit/s 802.11g: 54 Mbit/s 802.11n: 600 Mbit/s 802.11ac: 1 Gbit/s 802.11ax: 9.6 Gbit/s	868 MHz: 20 kbit/s 915 MHz: 40 kbit/s 2.4 GHz: 250 kbit/s	9.6 kbit/s or 40 kbit/s
Typical distance	1–300 m	50–100 m	2.4 GHz band: 10–100 m	30 m (indoor) to 100 m (outdoor)
Typical application	Data exchange between nearby nodes such as a mouse, wireless headset, mobile device, and computer	WLAN, high-speed Internet access at home and other indoor areas	Home automation, building automation, and remote control	Smart home appliance, monitoring and control

The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة القادسية
EVERYONE'S SMART UNIVERSITY