RV College of Engineering®

UNIT - II

Unit Internet of Things (UIoT)

Prof. Narasimha Swamy S
Department of AIML
RV College of Engineering
Bengaluru-59

Go, Change the World

Content

→ Introduction UIoT

→ Sensors and Actuators
- Sensors
- Actuators

→ Ubiquitous Sensing
- RFID, Bluetooth, Wi-Fi, Ultra-Wideband (UWB), Zigbee, Infrared Data Transmission

→ Networking and Communications

→ Management and Data Centres (M&DCs)

→ Case Study for IoT

Introduction

- → Unit Internet of Things (Unit IoT) refers to a specific application, including multiple sensors, actuators, a management and data center (M&DC), and heterogeneous networks.
- → Multiple unit IoTs could jointly constitute ubiquitous IoT
- → Unit IoT can also be regarded as an interactive system referring to sensing, controlling, and networking, and it realizes the interconnections among ubiquitous things
- → In unit and ubiquitous IoT (U2IoT), objects and entities are respectively associated with the corresponding identifiers and attributes (e.g., size, color, location, and attribution) in the physical world and cyber world.
- → Such identifiers and attributes are the things' important elements, which bring new challenges for data sensing, actuation implementation, networking and communications, and information management throughout both the cyber world and physical world.

Introduction (Contd.)

→ **Toward data sensing**

- Sensors perform persistent or intermittent data collection, and sensing technologies are applied to achieve an object being mapped as an entity from the physical world into the cyber world.

→ **Toward actuation implementation**

- Actuators execute actions as responses to the collected data, for which the centralized mode and distributed mode can be launched for implementation.
- The actuators may be managed by sensors or M&DCs and perform actuations in the physical world and cyber world.

→ **Toward networking and communications**

- Heterogeneous wireless networking technologies can be combined to realize efficient and reliable data transmission.
- The next-generation mobile communication network, telecommunication network, and Internet technologies can also be connected in IoT, and bring noteworthy prospects for the interconnection between the physical world and cyber world

Introduction (Contd.)

→ **Toward information management**

- M&DC acts as a management platform to provide functions such as intelligent decisions, data processing, and systemic management.
- Raw data are addressed to extract advanced knowledge to provide smart services, based on which entity mapping from the cyber world into the physical world is achieved.

Sensors and Actuators

→ In unit IoT, sensors and actuators are mainly linked via wired or wireless networks in the sensor-actuator layer

→ The sensors and actuators are used to collect data for identifying things, gathering information, and executing tasks without direct human intervention, which realizes the interaction and coupling between the physical world and cyber world

→ In unit IoT, sensors and actuators have the following features:

- Sensing - Sensors can perform sensing on things, and the collected data are usually used by actuators to perform appointed actions.
- Communication - Sensors and actuators can establish wired or wireless communications, and can be connected into heterogeneous networks among the interconnected things
- Identification- Things can be identified by sensors via identifiers or attributes (e.g., size, location, and temperature). Therefore, physical objects' physical identities and attributes, and their corresponding cyber identities and attributes, can be correlated with the mutually mapped relationships.
- Interaction- Things can interact with the surrounding environment and the back-end systems through the sensing and controlling capabilities

Sensors and Actuators (Contd.)

Sensors

- → Sensors act as detectors and converters to capture the data of physical things, and sensors are usually low-cost and low-power devices that are equipped with limited energy, computation, and communication capabilities.
- → There are different sensors to detect and measure physical things and the surrounding environment, including acceleration, vibration, electromagnetic properties, temperature, humidity, machine vision, velocity, and positions of physical things.
- → How sensors work
  - ▪ A sensor converts the physical action to be measured into an electrical equivalent and processes it so that the electrical signals can be easily sent and further processed
  - ▪ The sensor can output whether an object is present or not present (binary) or what measurement value has been reached (analog or digital).

Sensors and Actuators (Contd.)

Types of Sensors

Inductive sensors

Inductive sensors generate an electromagnetic field. This in turn generates eddy currents in objects made of metal. The sensor detects this change.

Example: Common applications of inductive sensors include metal detectors, traffic lights, car washes, and a host of automated industrial processes

Capacitive sensors

Capacitive sensors generate a capacitive measuring field. An entering object results in a change to the measuring field. The sensor responds to this change.

Example: Digital audio players, cell phones, and tablet computers will sometimes use capacitive sensing touchscreens as input devices

Sensors and Actuators (Contd.)

Types of Sensors

Photoelectric sensors

Photoelectric sensors (light curtains) always consist of an emitter and a receiver. There are diffuse, retro-reflective and through-beam types.

Example: A photoelectric sensor is a device used to determine the distance, absence, or presence of an object by using a light transmitter, often infrared, and a photoelectric receiver.

Ultrasonic sensors

Magnetic field sensors detect an external magnet. The field strength generated by the magnet is processed.

Magnetostrictive sensors detect the position of an external magnet using propagation time measurement.

Example: Used in detecting and sensing the distance, speed, rotation, angle, and position by converting magnetic information into electrical signals.

Sensors and Actuators (Contd.)

Classification of Sensors

→ According to the sensed data, sensors can be classified into two types: identifier (ID)-based sensors, and attribute (non-ID, short for nID)-based sensors

→ ID-Based Sensors

- mainly refer to the sensors that detect physical things with identifiers.
- Such things can be organized into networks to achieve interconnection.

→ nID-based sensors

- mainly include sensors that detect physical things' attributes.
- Such sensors can detect inherent attributes and other relevant attributes.

→ Generally, ID-based sensors are applied to detect an object with identifiers (e.g., radio frequency identification [RFID] tag identifier and quick-response [QR] code) in unit IoT.

→ For ID-based sensors, multiple identifiers may be assigned to an object according to different IoT scenarios, and different identifier fields may be authorized to multiple users with different authority

Sensors and Actuators (Contd.)

Classification of Sensors

→ It turns out that:

- An object may have multiple identifiers in different applications.
- An identifier may have multiple identifier fields for different users.
- A user may access multiple identifiers of different objects or may access multiple identifier fields of an object.

→ The relationships of the object, identifier, and user reflect the interconnection between the physical world and cyber world.

→ In unit IoT, an object may have the corresponding identity information (i.e., identifier), in which the sensors are applied to transfer the attached data to point to an object by electromagnetic signals.

→ Beyond the sensors used to detect an object's ID, there are also nID-based sensors applied to detect an object's attributes (e.g., temperature and location).

→ There are several examples of nID-based sensors.

Sensors and Actuators (Contd.)

Classification of Sensors

→ For instance, image detection devices can identify the objects and their activities and can be used to monitor and evaluate the scene; radar applies electromagnetic waves to detect the object, and obtain an object's information by radar cross section, doppler, glint, and so forth.

→ In unit IoT, both ID and nID-based sensors are usually organized in the hybrid detection and identification mode, in which complementary and cooperative relationships are established among heterogeneous sensors.

Sensors and Actuators (Contd.)

Actuators

- → Actuators are defined with the functions of automation and control, which convert the collected data into action commands to enhance efficiency in self-adaptive applications
- → Concretely, actuators are usually mechanical or electronic devices (e.g., valves and switches) that execute commands and instructions, and perform appropriate actions on physical things and the surrounding environments
- → In some cases, sensors and actuators are pairwise devices to perform actions on the physical world
- → For example, a gas transducer detects that a gas concentration of carbon dioxide exceeds the standard limitation, and the switch of an air conditioner will be launched to address the abnormal situation
- → In wireless sensor-actuator networks (WSANs), actuators can be organized in different modes according to whether there is an integrated or an independent controller attached in an actuator

Sensors and Actuators (Contd.)

Actuators

- → Similarly, actuators can be organized in a centralized actuation mode and distributed actuation mode in unit IoT.
- → Centralized actuation mode
  - In the centralized mode, there are one or multiple controllers to perform management on sensors and actuators within the given jurisdiction
  - The controller is an independent functional module with sufficient computation and communication capacities.
  - The sensors transmit the collected data to a controller.
  - Thereafter, the controller executes the corresponding control algorithms, and assigns executive commands to actuators.
  - Upon receiving the control commands, the actuators perform the appointed actuations.

Sensors and Actuators (Contd.)

Actuators

→ Distributed actuation mode

- In the distributed mode, an actuator acts as both an actuator and a controller.
- The controller has the assigned control algorithms and is applied to provide an actuation strategic decision for the detailed actuation execution in the physical world.
- The sensors collect physical things–related data, which are transmitted to the corresponding actuators.
- Thereafter, the actuators invoke the predefined control algorithm to perform data processing, and to execute appropriate actions.
- Generally, the controller and actuators are logically integrated into a whole entity, and the sensed data are used by actuators with executive commands to react upon the physical world.

Ubiquitous Sensing

- → Ubiquitous sensing refers to a great variety of sensor-based technologies, and mainly serves for the sensor-actuator layer to achieve ubiquitous sensing and controlling.
- → There are wired sensing technologies and wireless sensing technologies
- → Wired sensing technologies
  - ▪ It belong to the traditional monitoring modes, and usually have more reliable communication channels
  - ▪ The wired sensing technologies have obvious limitations (e.g., mobility and expandability), and therefore wireless sensing technologies appear to be an emerging technology.

Ubiquitous Sensing (Contd.)

→ **Wireless Sensor Networks (WSN)**

- WSN is a suitable access network platform consisting of a huge number of distributed autonomous sensors for monitoring and detecting objects.
- Multiple wireless sensing technologies can be integrated into WSNs, based on which sensors cooperatively transmit the collected data into heterogeneous networks.
- During data transmission, multi-hop and self-organizing wireless routes are established with bidirectional communications.
- The sensors may actively collect data by constantly performing omnidirectional scanning and may passively gather data.
- Sensors can be called motes, which are components of the network of sensor nodes.

Ubiquitous Sensing (Contd.)

→ The wireless sensing technologies also bring several open issues, including

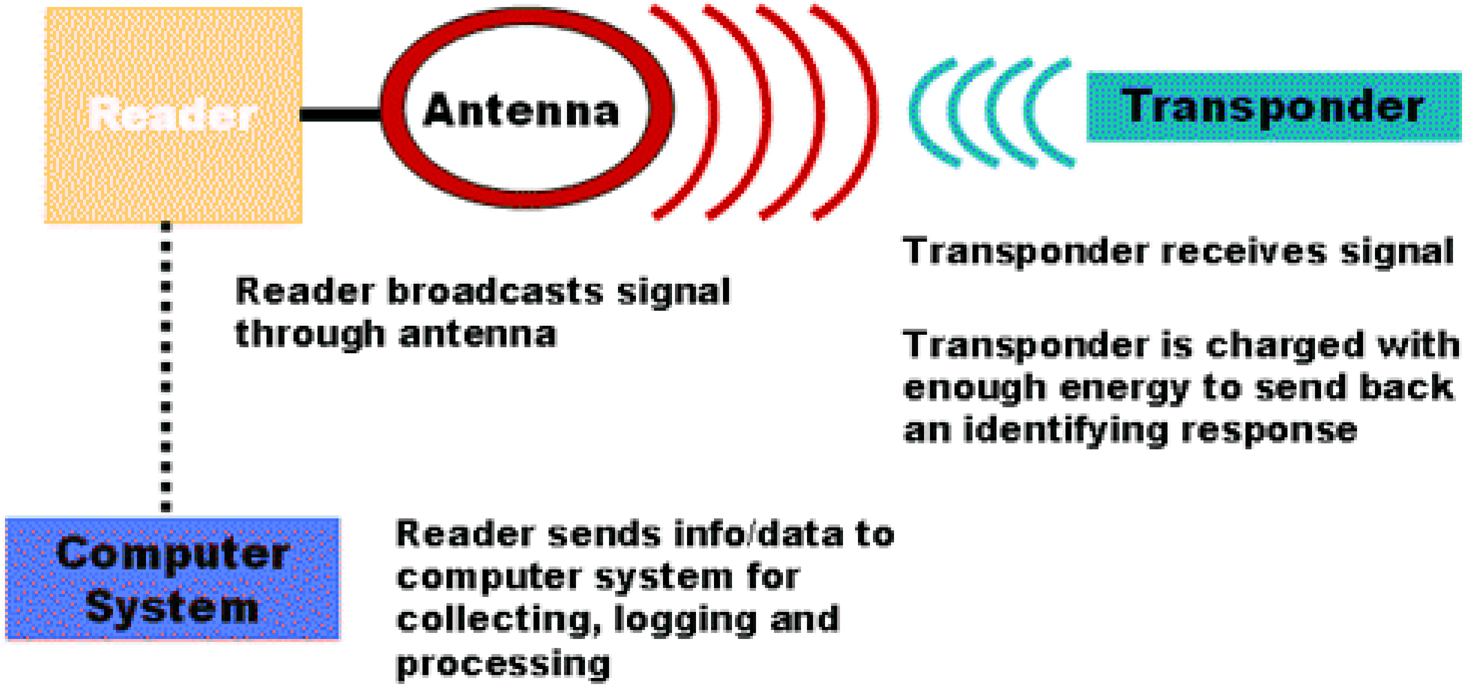
- Network Structure (e.g., heterogeneous network and hierarchical network)
- Network deployment (e.g., one time, incremental, and random)
- Communication modality (e.g., single hop and multi-hop)
- Network topology (e.g., single hop, star, multi-hop, mesh, and multitier), and
- Coverage (e.g., sparse, dense, and redundant)

→ In the following sections, the typical wireless sensing technologies are introduced, including RFID, Bluetooth, Wi-Fi, ultra-wideband (UWB), ZigBee, and infrared data transmission (IrDA)

Ubiquitous Sensing (Contd.)

Radio Frequency Identification (RFID)

- → RFID is a wireless automatic identification technology to achieve data acquisition from tagged objects by electromagnetic fields or electrostatic coupling.
- → It comes under the perception layer of architecture
- → In the open wireless air interface, there are two main components: tag and reader.



Reader broadcasts signal through antenna

Transponder receives signal

Transponder is charged with enough energy to send back an identifying response

Reader sends info/data to computer system for collecting, logging and processing

Ubiquitous Sensing (Contd.)

Radio Frequency Identification (RFID)

→ Every RFID system consists of three components: a scanning antenna, a transceiver and a transponder.

→ When the scanning antenna and transceiver are combined, they are referred to as an RFID reader or interrogator.

→ There are two types of RFID readers - fixed readers and mobile readers.

→ It uses radio waves to transmit signals that activate the tag.

→ Once activated, the tag sends a wave back to the antenna, where it is translated into data. The transponder is in the RFID tag itself.

→ The read range for RFID tags varies based on factors including the type of tag, type of reader, RFID frequency and interference in the surrounding environment or from other RFID tags and readers.

→ There are two main types of RFID tags:

- Active RFID- An active RFID tag has its own power source, often a battery.
- Passive RFID- A passive RFID tag receives its power from the reading antenna

Ubiquitous Sensing (Contd.)

Radio Frequency Identification (RFID)

Tag

→ It is embedded with a unique identifier and is attached to objects.

→ In RFID systems, the identified objects may include goods, materials, products, assembly machinery, assets, and even persons/animals.

→ The object is tagged with a tag, and the sensed data can be collected by an identifier for identification via wireless channels.

Reader

→ It emits radio signals within the electromagnetic range, which is determined upon the power output and working frequency.

→ When a tag passes through its range, it detects the reader’s activation challenge signal, which is transmitted to the back-end system for data processing and management.

→ Note that the reader may have a built-in database for offline identification and authentication in distributed systems.

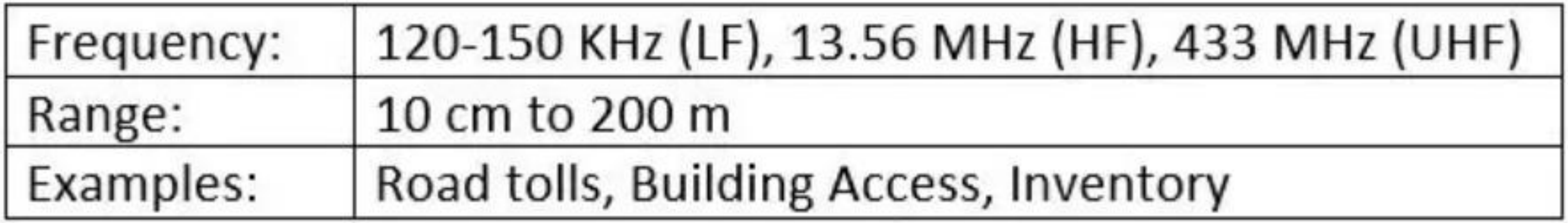
Ubiquitous Sensing (Contd.)

Radio Frequency Identification (RFID)

→ In RFID applications, near-field communication (NFC) as 13.56 MHz frequency-based RFID technology becomes noteworthy for smart phones and other mobile devices to establish radio communication, and provides services such as mobile payment, ticketing, information collection/exchange, and access control.

→ NFC standards are based on the ISO/IEC 14443 international standard to specify the communications protocols and data exchange formats.

→ The main features of NFC include physical noncontact identification, multiple applicability, open standards, inherent security, and interoperation



Frequency:	120-150 KHz (LF), 13.56 MHz (HF), 433 MHz (UHF)
Range:	10 cm to 200 m
Examples:	Road tolls, Building Access, Inventory

Ubiquitous Sensing (Contd.)

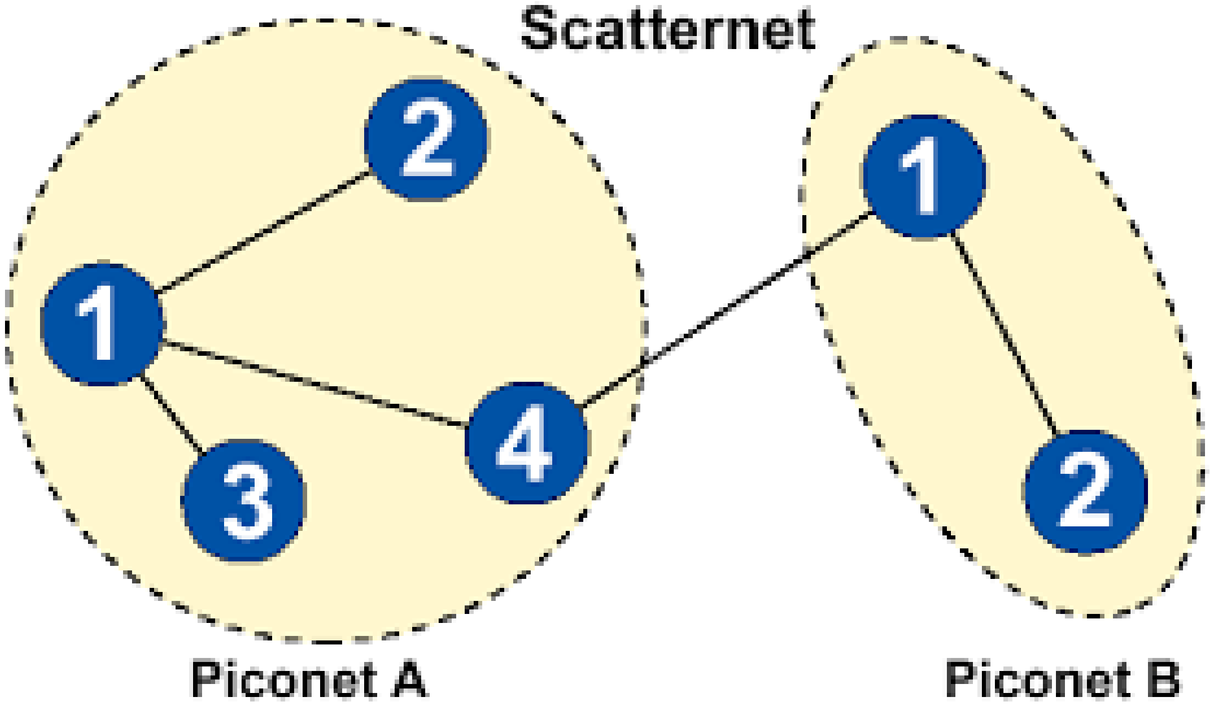
Bluetooth

- → Bluetooth is a wireless technology based on short-range radio transmissions in the 2.4 GHz frequency, and it establishes personal area networks (PANs) with high security requirements.
- → Bluetooth is a specification for low-power radio communications to establish wireless intercommunications of devices and their peripherals, including mobile phones, personal digital assistants (PDAs), wireless headsets, computers, and other network devices.
- → Based on Bluetooth technology, graph, voice, and data can be transmitted within the effective range (e.g., less than 10 m) at a low data rate. (1 Mbps or 3 Mbps depending upon the version)
- → A Bluetooth special interest group has developed wireless communications standard IEEE 802.15.1 for mobile devices.
- → In a basic Bluetooth network, there is a dynamic topology piconet, which includes a minimum of two and a maximum of eight peer devices for communication
- → The collection of interconnected piconets is called scatternet.

Ubiquitous Sensing (Contd.)

Bluetooth

→ Bluetooth Architecture



→ There are several features and requirements that should be considered

Ubiquitous Sensing (Contd.)

Bluetooth

- The same standard should be regulated around different regions in the world.
- The radio transceiver must be small and operate at low power and globally.
- The system supports peer-to-peer connectivity and separates the frequency band into hops. The spread spectrum is used to hop from one channel to another with security consideration.
- The system should support data in multimedia applications. Meanwhile, signals can be transmitted without needing a line of sight, and devices can be identified by omnidirectional signals
- Both synchronous and asynchronous applications are supported, which makes it easy to implement on different device-based services

Ubiquitous Sensing (Contd.)

Wireless Fidelity (WiFi)

→ Wi-Fi is a wireless technology that allows an electronic device to exchange data over a high-speed computer network (e.g., Internet), and it is a typical communication of wireless local area networks (WLANs) based on IEEE 802.11 family standards.

→ The Wi-Fi standard covers a relatively large area with high transmission speed.

→ The Wi-Fi alliance defines that Wi-Fi is used based on IEEE 802.11b, which supports the 2.4 GHz frequency of wireless access points.

→ Additionally, Wi-Fi alliance has expanded the generic standard to other related standards, including IEEE 802.11a, 802.11g, and 802.11n.

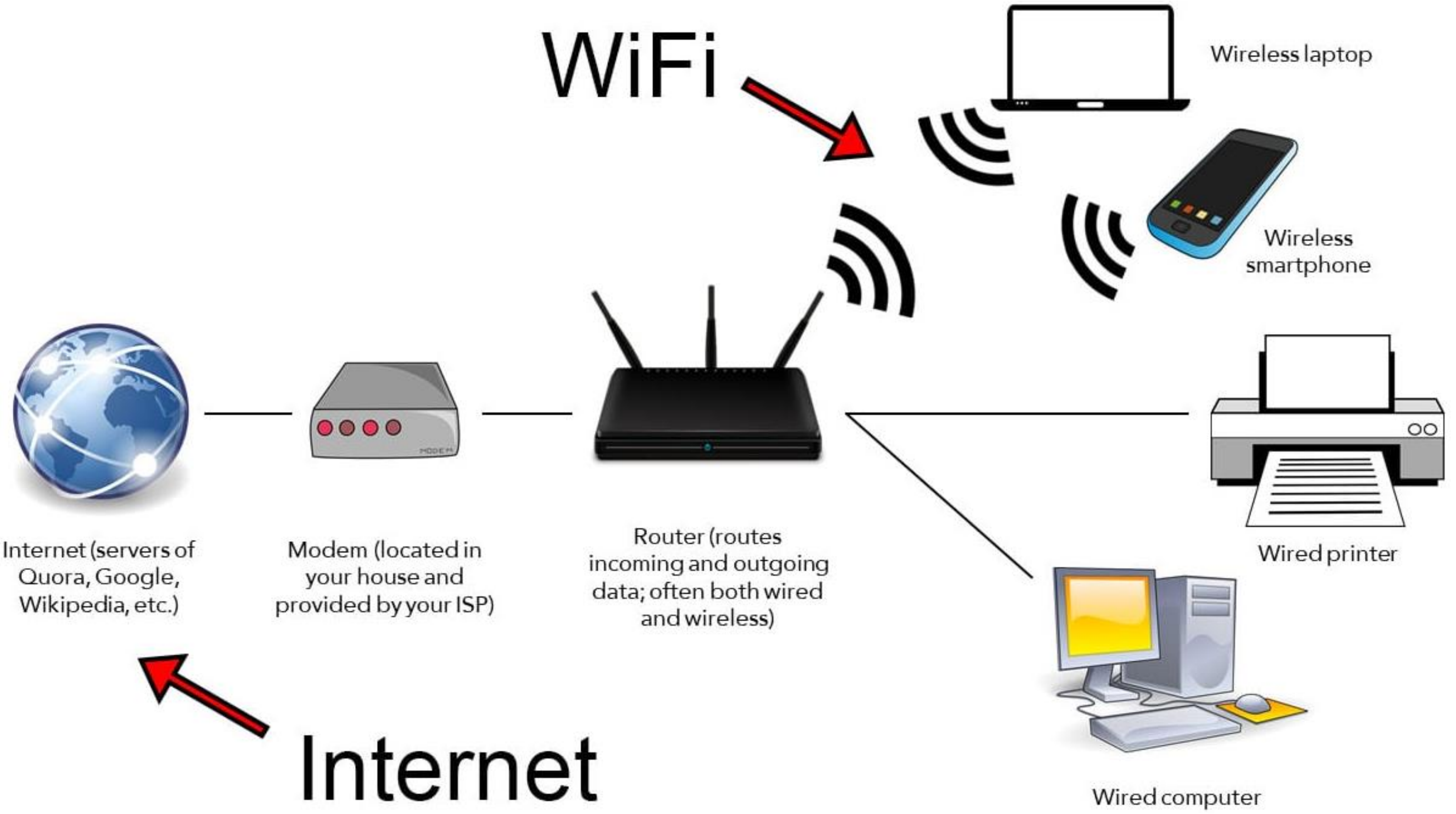
→ Wi-Fi uses radio waves to transmit information between your device and a router via frequencies.

→ There are dual-band devices that let you choose which frequency you want to use for your WiFi network.

→ The difference between the frequency bands is the range and bandwidth they provide.

Ubiquitous Sensing (Contd.)

Wireless Fidelity (WiFi)


WiFi
Wireless laptop
Wireless smartphone
Internet (servers of Quora, Google, Wikipedia, etc.)
Modem (located in your house and provided by your ISP)
MODEM
Router (routes incoming and outgoing data; often both wired and wireless)
Wired printer
Wired computer
Internet

Ubiquitous Sensing (Contd.)

Ultra-Wideband (UWB)

→ Ultra-wideband (UWB) applies wireless signals for data collection and transmission and is based on a low energy level for short-range, high-bandwidth communications with a large portion of the electromagnetic spectrum.

→ The main applications of UWB include radar imaging, target sensor data collection, and precision locating and tracking.

→ UWB offers both high-data-rate communication and high-accuracy positioning capabilities and can use a low transmitted signal power level with an extremely wide bandwidth.

→ It uses radio waves of short pulses over a spectrum of frequencies ranging from 3.1 to 10.5 GHz

→ UWB requires large bandwidth of 500 MHz which make it more accurate and faster and transfer one pulse per two nanoseconds.

→ UWB uses a pulse-based approach or a multiband orthogonal frequency division multiplexing-based approach for transmission, to achieve high-rate, short-range or low-rate, moderate-range communications

Ubiquitous Sensing (Contd.)

Ultra-Wideband (UWB)

→ There are several UWB applications, such as voice conversations and streaming, automation and control, medical monitoring, vehicular radar systems, and other high-rate data transfer applications.

→ Moreover, UWB can enable a variety of wireless personal area network (WPAN) applications, such as wireless PC peripheral connectivity, wireless multimedia connectivity for devices, cable replacement and network access for mobile computing devices, and ad hoc connections between UWB-enabled devices

→ The main features of UWB are as follows:

- Low transmission energy and high bandwidth within a short range
- Low energy density minimizes the interference on other services, and the communication is hard to intercept along with multipath immunity
- Universal signal generation and processing architectures with low cost, and frequency diversity with minimal hardware modification

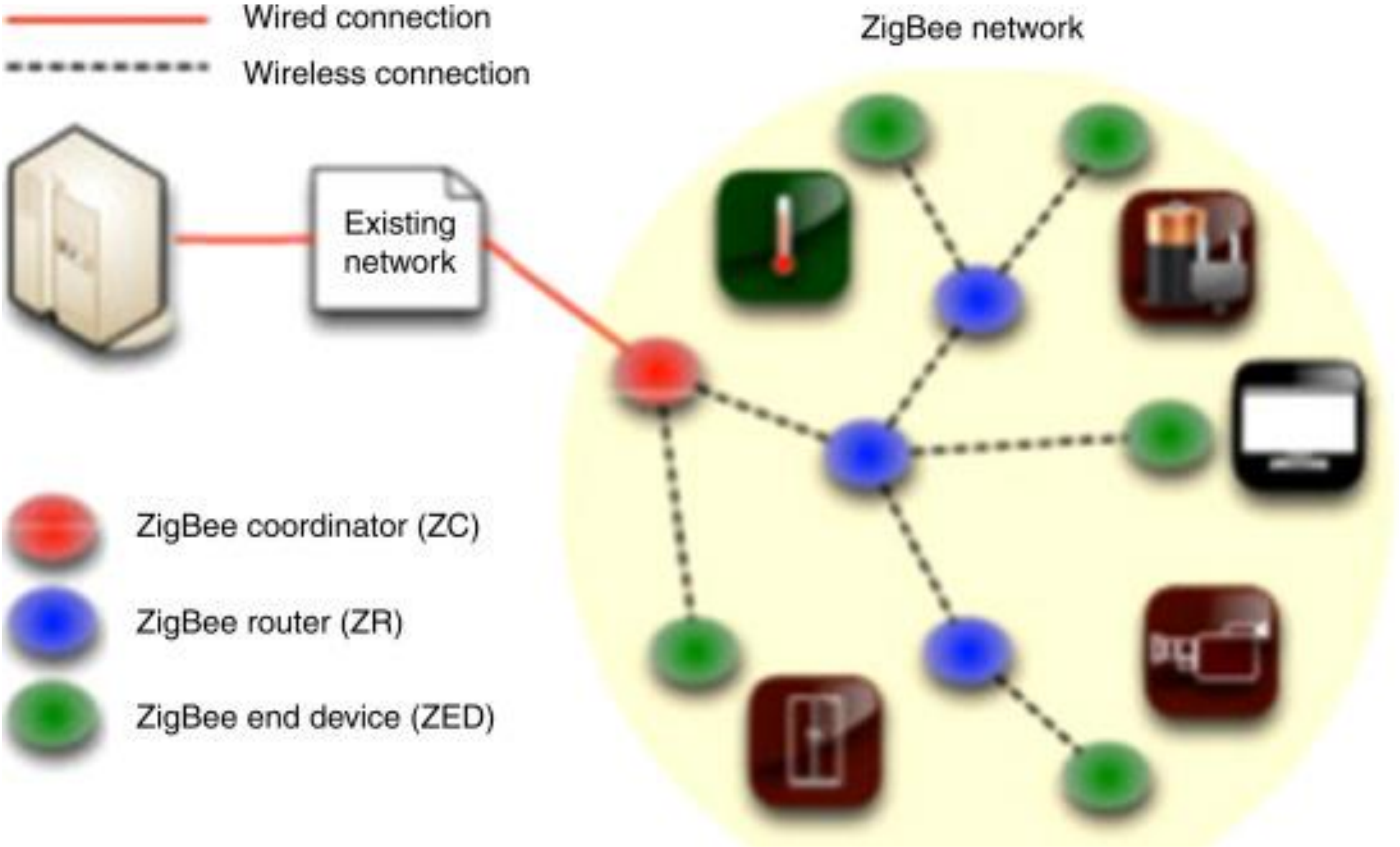
Ubiquitous Sensing (Contd.)

ZigBee

- → ZigBee is characterized by low-rate, low-power, and short-range data transmission for personal area networks.
- → The IEEE 802.15.4 physical radio specification is the ZigBee standard to operate in unlicensed bands, including 2.4 GHz, 900 MHz, and 868 MHz, that require a low data transfer rate of 250 Kb/sec
- → The range of Zigbee is between 10 meters and 100 meters.
- → Its wireless networking is simpler to design, less expensive, highly stable and offers more secure networking
- → Zigbee's system structure consists of three different devices or nodes within a single network. They are:
  - ▪ End Devices : Collects the data and send the data to the destination
  - ▪ Routers: routes the data to the destination
  - ▪ Coordinator: Connects the home and other networks

Ubiquitous Sensing (Contd.)

ZigBee

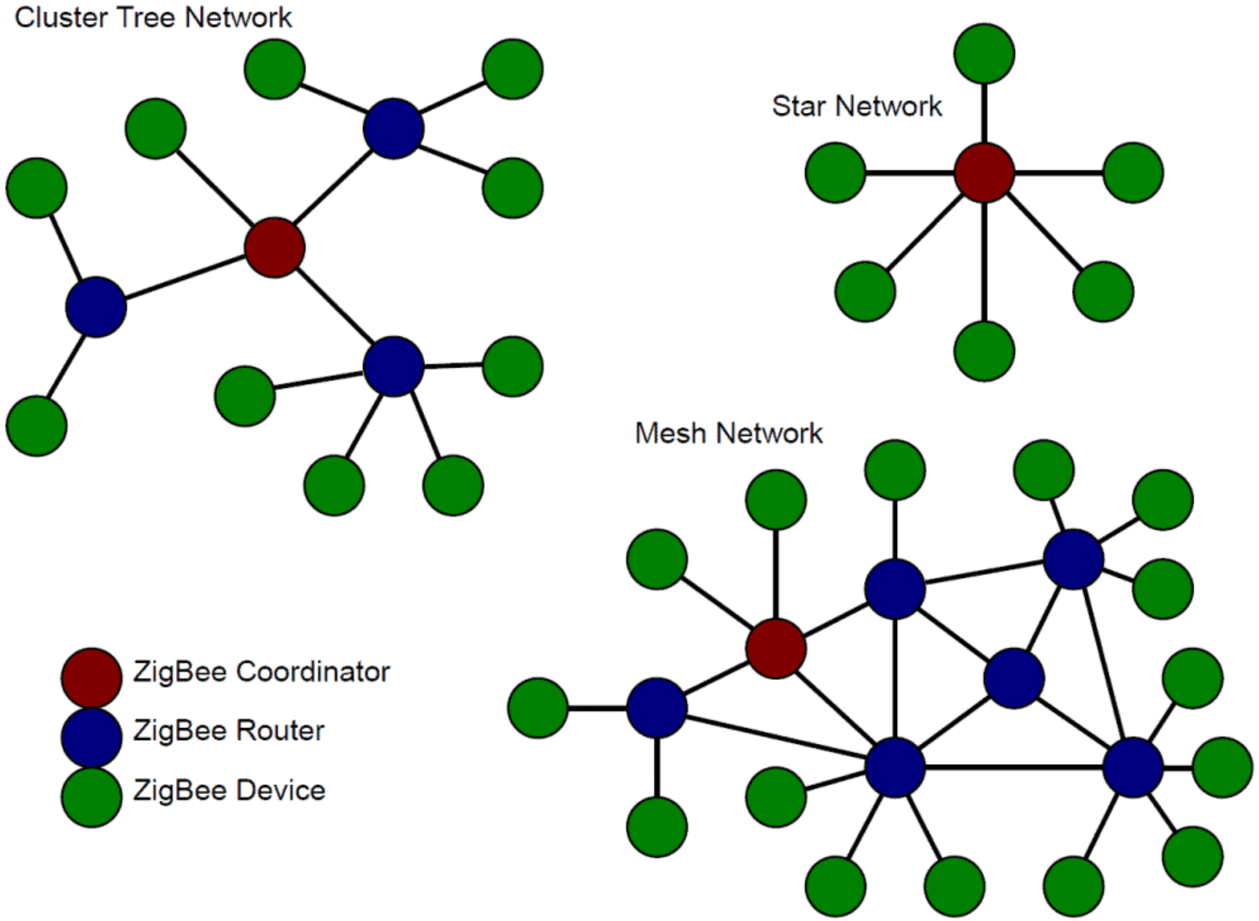


Ubiquitous Sensing (Contd.)

ZigBee

→ ZigBee is mainly organized into three network topologies: star topology, tree topology, and mesh topology.

- Star topology is mainly designed for point-to-multipoint-based communication.
- Tree topology uses a hierarchical routing mechanism.
- Mesh topology uses the mixed routing method combined with ad hoc on-demand distance vector routing and hierarchical routing.



Ubiquitous Sensing (Contd.)

ZigBee

→ The main features of ZigBee are as follows:

- Support for multiple network topologies (e.g., point-to-point, point-to-multipoint, and mesh networks)
- low rate, low power, and low latency
- Many sensor nodes per network Support security mechanism for data transmission, such as 128-bit AES encryption Collision avoidance, retries, and acknowledgments

Ubiquitous Sensing (Contd.)

Infrared Data Transmission

- → The Infrared Data Association (IrDA) is an organization that defines physical specifications communications protocol standards for wireless infrared communications between devices.
- → Infrared data transmission is a short-range infrared wireless technology to achieve point-to-point connections.
- → The IrDA commonplace operates at a touch rate of seventy-five Kbits/sec and therefore the distance varies, is up to eight meters.
- → Infrared signals require line of sight (LOS) with a short range, and provide low-cost, small-size, low-power-consumption, low-bit-error-rate (BER), cross-platform, and point-to-point communications.
- → Infrared signals support the dynamic ad hoc connectivity but has restrictions: two devices must be in short distance and line of sight.
- → Such a short-range optical communication technique is mainly used to wirelessly transfer data with point-and-shoot principles between devices, including computers, PDAs, cell phones, laptops, and cameras.

Ubiquitous Sensing (Contd.)

Infrared Data Transmission

→ The applications of infrared data transmission mainly include end-to-end digital payment systems, in which the IrDA Financial Messaging (IrFM) standard has been used for financial services infrastructures (e.g., credit cards) to realize efficient payment transactions

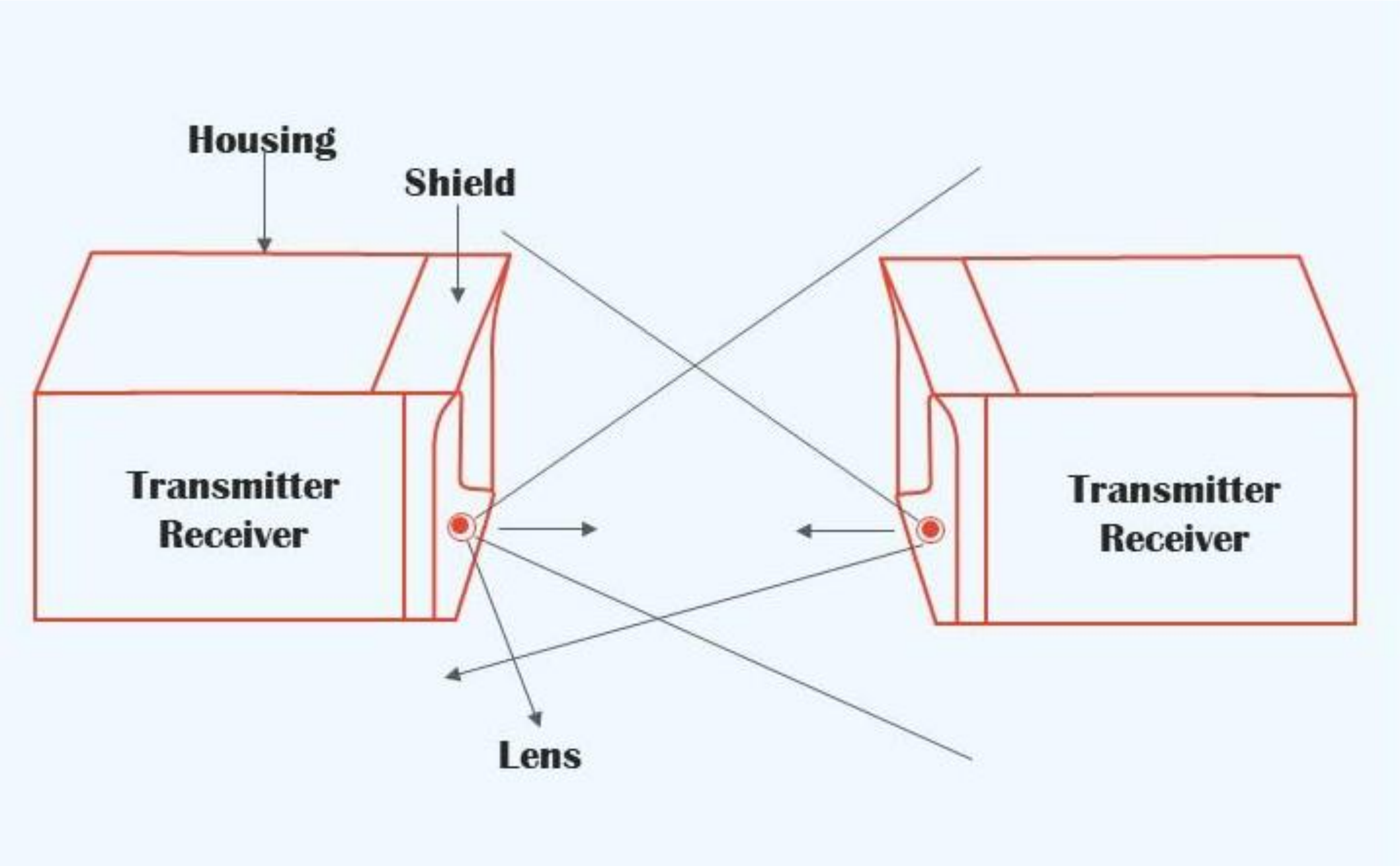
→ The standards of infrared transmissions are as follows –

- The IRDA-C standard provides the bidirectional communications standards used in cordless devices such as mouse, keyboards, joysticks and hand-held computers.
- The IRDA-0 standard operates at a bit rate of 75k bits/sec, and the distance area is up to 8 meters.
- There is another standard known as the IRDA-1 standard.
    - It supports the data rates from 115 kb/s to 4 Mb/s, with a distance of up to 1 metre.

→ Infrared light transmissions have existed for many years and their use having been limited to TV remote controls and wireless slide projector remote controls

Ubiquitous Sensing (Contd.)

Infrared Data Transmission



Networking and Communications

→ Networking and communications technologies are pivotal for interconnection among remote things, in which mobile communication and the Internet are the mainstream technologies.

Networking and Communications

Mobile Communication Technology

- → Mobile communication has developed through first-generation (1G) analog cellular networks (e.g., Advanced Mobile Phone System [AMPS]), 2G digital cellular networks (e.g., Global System for Mobile Communications [GSM]), and 2.5G (e.g., General Packet Radio Service [GPRS]), and is evolving toward 3G ,4G standards and 5G standards
- → Third-Generation Technology (3G)
  - ▪ 3G technology is a generation of standards for mobile phones and mobile telecommunication services fulfilling the International Mobile Telecommunications 2000 (IMT-2000) specifications proposed by the International Telecommunication Union.
  - ▪ Application services include wide-area wireless voice telephone, mobile Internet access, video calls, and mobile TV, all in a mobile environment.
  - ▪ The typical 3G standards include wideband code division multiple access (W-CDMA), CDMA2000, and time division-synchronous code division multiple access (TD-SCDMA).

Networking and Communications

Mobile Communication Technology

→ Third-Generation Technology (3G)

- Universal Mobile Telecommunications System (UMTS) architecture is specified by the 3G Partnership Project (3GPP) and evolved from the Global System for Mobile Communications (GSM) and general packet radio service (GPRS) of 2G/2.5G infrastructures.
- For UMTS, there are two types of standards: W-CDMA and TD-SCDMA.
  - W-CDMA applies direct sequence–code division multiple access (DS-CDMA) and frequency division duplexing (FDD) to achieve higher speeds.
  - W-CDMA supports an asynchronous operating mode and fast cell acquisition operation, which is a dominant 3G technology considering the dominance of existing 3G networks.
  - TD-SCDMA is short for time division–synchronous code division multiple access, and is only used in China.

Networking and Communications (Contd.)

Wireless Local Area Network (WLAN)

→ WLAN applies wireless distribution technologies such as spread spectrum or orthogonal frequency division multiplexing (OFDM) to achieve multiple devices interconnection.

→ It has the advantages of a high data transmission rate, and becomes ubiquitous in indoor scenarios (e.g., building environments).

→ In WLAN, no additional installation costs are needed, and multiple mobile devices can seamlessly connect to positioning systems, in which the fingerprinting method is used for position estimation.

→ Note that WLANs are mainly based on IEEE 802.11 standards, which define two basic operation modes: infrastructure mode and ad hoc mode.

→ In infrastructure mode, wireless mobile units communicate via an access point to a wired network infrastructure. In ad hoc mode, the mobile units communicate in a peer-to-peer mode.

Networking and Communications (Contd.)

Fourth-Generation Technology (4G)

→ 4G technology is an integration of 3G and WLAN technologies, and is basically an extension of 3G technology, with more bandwidth and services

→ In IoT, it is significant to merge fixed, mobile, and wireless communications to establish heterogeneous communications.

→ It becomes an open issue to achieve both high data rate and seamless mobility; therefore, hybrid communication technologies should be optimized according to the contexts of mobile applications.

→ For a 4G system, the all-IP-based secure mobile broadband communication scheme is provided for smart phones and other mobile devices.

→ In addition, other application-oriented facilities (e.g., ultra-broadband Internet access, IP telephony, and streaming multimedia) may be provided to users

→ International Mobile Telecommunications–Advanced (IMT-Advanced) are proposed to support 4G mobile phone and Internet access service.

Networking and Communications (Contd.)

Fourth-Generation Technology (4G)

→ The official designation 4G standards include Long-Term Evolution (LTE)–Advanced and Wireless MAN–Advanced (IEEE 802.16m). There are also several forerunner versions, including Mobile WiMAX, 3GPP LTE, and TD-LTE, to support 4G standardization.

→ Features of 4G

- Supports interactive multimedia, wireless Internet, and other broadband services
- High data rate, high capacity, and low cost per bit
- Mobility, service portability, and scalable mobile networks
- Seamless switching and QoS-based services
- Enhanced scheduling and call admission control techniques

Networking and Communications (Contd.)

Next-Generation Internet Technology

→ The Internet is global computer networks used to achieve connection by the standard Internet protocol suite Transmission Control Protocol/ Internet Protocol (TCP/IP), and it applies electronic, wireless, and optical networking technologies to establish a compositive network structure.

→ The network structure mainly includes multiple private, public, local, industry, and national area networks.

→ Due to the increasing address requirements, the next-generation Internet becomes attractive for IoT development and brings new challenges for network interconnections.

→ IoT accelerates the development of the next-generation Internet technology.

→ Due to the requirement of ubiquitous connectivity among a mass of things, it becomes necessary to assign more addresses to newly increasing things.

Networking and Communications (Contd.)

Next-Generation Internet Technology

- → Internet Protocol version 6 (IPv6), with its expanded address space, enables addressing, connecting, and tracking things, and is introduced to replace the traditional Internet
- → It seems that it is possible to establish convergence of heterogeneous networks and applications based on the next-generation Internet-based network.
- → The main features of IPv6 are as follows:
  - ▪ Large address space: Expanded addressing capacity (2128 addresses in IPv6, compared with 232 in IPv4)
  - ▪ Built-in security support for authentication and privacy
  - ▪ Built-in support for mobile communications
  - ▪ A new protocol for neighboring node interactions defined, and a new packet format to minimize packet header processing by routers
  - ▪ Better support for QoS with prioritization of communications
  - ▪ Plug-and-play auto configuration of network settings to achieve stateless and stateful address configurations
  - ▪ Support extensibility with hierarchical addressing and routing infrastructure

Networking and Communications (Contd.)

Next-Generation Internet Technology

- → Along with the development of heterogeneous networks, 6LoWPAN (i.e., IPv6 over low-power wireless personal area networks) has been introduced to realize that low-power devices with limited processing capabilities can participate in future IoT.
- → 6LoWPAN allows network interaction between IPv6-based Internet and IEEE 802.15.4-based wireless networks, for which connectivity, interoperability, and compatibility requirements should be considered.
- → Things linked by IP and wireless communications, usually have limited power and lower data rates, and are suitable for automation and entertainment applications in home and building area networks.
- → 6LoWPAN enables resource-limited things in wireless networks to relate to the Internet, which will bring a bright perspective for the future Internet.

Networking and Communications (Contd.)

Management and Data Centers (M&DCs)

→ The M&DCs mainly consider the aspects of pervasive management, and data fusion and data mining.

→ Pervasive Management: Pervasive management considers object/ entity, networks, and services in unit IoT, to achieve intelligent and self-adaptive management

→ Object/Entity Management: Object/entity management in unit IoT mainly refers to managing the system components, including sensors, actuators, gateways/base stations, user terminals, back-end databases, and other network elements.

→ These components include objects distributed in geographical areas, and the corresponding entities with different function abstractions.

→ In unit IoT, object/entity management mainly has the following functions:

- Monitors, controls, and supervises cyber entities, and network components in an individual network
- Controls and maintains the physical infrastructures
- Establishes things' interaction records and other statistical communication parameters
- Performs strong security protection and privacy preservation, energy maintenance, and spectrum management

Networking and Communications (Contd.)

Network Management

- → Network management focuses on networking-related actions in the cyber world.
- → The main aspects refer to the network entities’ activities, networking protocols, and accessing procedures, which work on the network operation, maintenance, and provision.
- → Network management mainly has the following functions:
  - ▪ Manages network topology and its network structural relations
  - ▪ Maintains reliable interconnection in internetwork, intra network, and cross-network; maintains network availability to avoid channels jamming and blocking
  - ▪ Designs secure communication protocols/ algorithms, and adopts efficient mechanisms for safeguard
  - ▪ Establishes heterogeneous network interfaces to improve network compatibility
  - ▪ Optimizes network resource allocation, and coordinates resource distribution to achieve enhanced network performance

Networking and Communications (Contd.)

Service Management

→ Service management mainly serves individual or group users in unit IoT.

→ Its aim is to improve the quality of services, and to provide appropriate services for users or potential users.

→ Service-oriented computing (SOC) is an important aspect of service management.

→ A service-oriented architecture introduces loose coupling and flexibility into IoT, which allows seamless integrations of heterogeneous interfaces and platforms.

→ For service management, different services are provided for applications with hybrid management structures, and shared information resources are used to support different service operations.

→ To some degree, service management directly influences the user's experiences in IoT.

Networking and Communications (Contd.)

Data Fusion and Data Mining

- → The purpose of data fusion is to integrate multiple data and knowledge of objects with a consistent, accurate, and useful representation in unit IoT.
- → It can be classified into three types: data-level fusion, feature-level fusion, and decision-level fusion.
  - ▪ Data-level fusion is based on the sensors that combine several raw data sources to obtain refined data.
  - ▪ Feature-level fusion expresses the data as a series of feature vectors, extracts the feature values, and represents things' attributes.
  - ▪ Decision-level fusion provides advanced strategic decisions for different requirements.
- → In data fusion, there are two main issues: data conflicts and data integration
- → The Data conflicts should be avoided from heterogeneous data sources, and data integration should be achieved with both data redundancy and correctness considerations

Networking and Communications (Contd.)

Data Fusion and Data Mining

→ The main features of data conflicts and data integration are as follows.

- Data conflicts mainly include data uncertainty and data contradiction.
  - Data uncertainty refers to an object’s certain data (e.g., identifier and attribute) being represented by an expression value.
  - Meanwhile, data may also be described by another expression value.
  - Such expression values may cause data uncertainty.
  - Data contradiction refers to different expression values being applied to represent the same data, which may lead to inconsistent data representation for the object.

→ Data integration mainly considers the features of completeness, conciseness, and correctness.

- Data completeness ensures the integrity in terms of data elements (e.g., identifier and attributes) that cannot be modified (e.g., deleted, added, inserted, or recombined) without authorization.

Networking and Communications (Contd.)

Data Fusion and Data Mining

- Data conciseness ensures the uniqueness of things’ representations, which are described by the integrated data in terms of the objects and the corresponding identifiers/attributes.
- Data correctness ensures the validity of data sources, which should conform to the interaction relationships between the physical world and cyber world.

Networking and Communications (Contd.)

Data Fusion and Data Mining

→ Data mining refers to knowledge discovery, which utilizes interleaving techniques of artificial intelligence, machine learning, statistics, and database technologies.

→ It mainly addresses the aspects of database management, the data structure model, data preprocessing, data complexity analysis, interestingness metrics, visualization, and online interaction.

→ The goal of data mining is to extract available knowledge from an existing data set.

→ There are four basic data mining models, including multilayer data mining, distributed data mining, grid data mining, and heterogeneous data mining, that can be applied in unit IoT.

Networking and Communications (Contd.)

Data Fusion and Data Mining

→ Hierarchical data mining

- In the hierarchical data mining model, there are four layers, including the data collection layer, data management layer, event processing layer, and data mining service layer.
- The data collection layer refers to preliminary data management.
- The data management layer mainly uses the centralized or distributed database to manage the collected data.
- The event processing layer is applied to perform multiple events–based data analysis.
- The data mining service layer is established by data management and event processing to support applications

Networking and Communications (Contd.)

Data Fusion and Data Mining

→ Distributed data mining

- The distributed data model is based on distributed storage, without needing a management and data center according to mass, distributed, space-time attributes.
- The data mining system includes a top data center and multiple data sub centers.
- The sub center receives the raw sensed data for preprocessing, data abstraction, and data compression.
- Thereafter, the preprocessed data are transmitted to the local database.
- Here, the local database performs the corresponding event filtering and event detection, and it transmits the aggregated data to the top center for further processing.
- The top center acts as the whole manager and does not directly participate in the preliminary data mining on the sensed data, and mainly controls the sub centers.
- Based on such a model, data mining is mainly performed by the multiple local data agents–based collaborative mechanism.

Networking and Communications (Contd.)

Data Fusion and Data Mining

→ Grid data mining

- A grid computing infrastructure can be introduced into data mining with the principle of breaking up the whole into parts.
- The grids are in the independent distributed system with noninteractive operations, and are suitable for loosely coupled, heterogeneous, and geographically dispersed networks.
- In a grid data mining model, a grid is a local data mining unit, and a multi agent-based collaborative management mechanism is applied for data aggregation to support different applications.

Networking and Communications (Contd.)

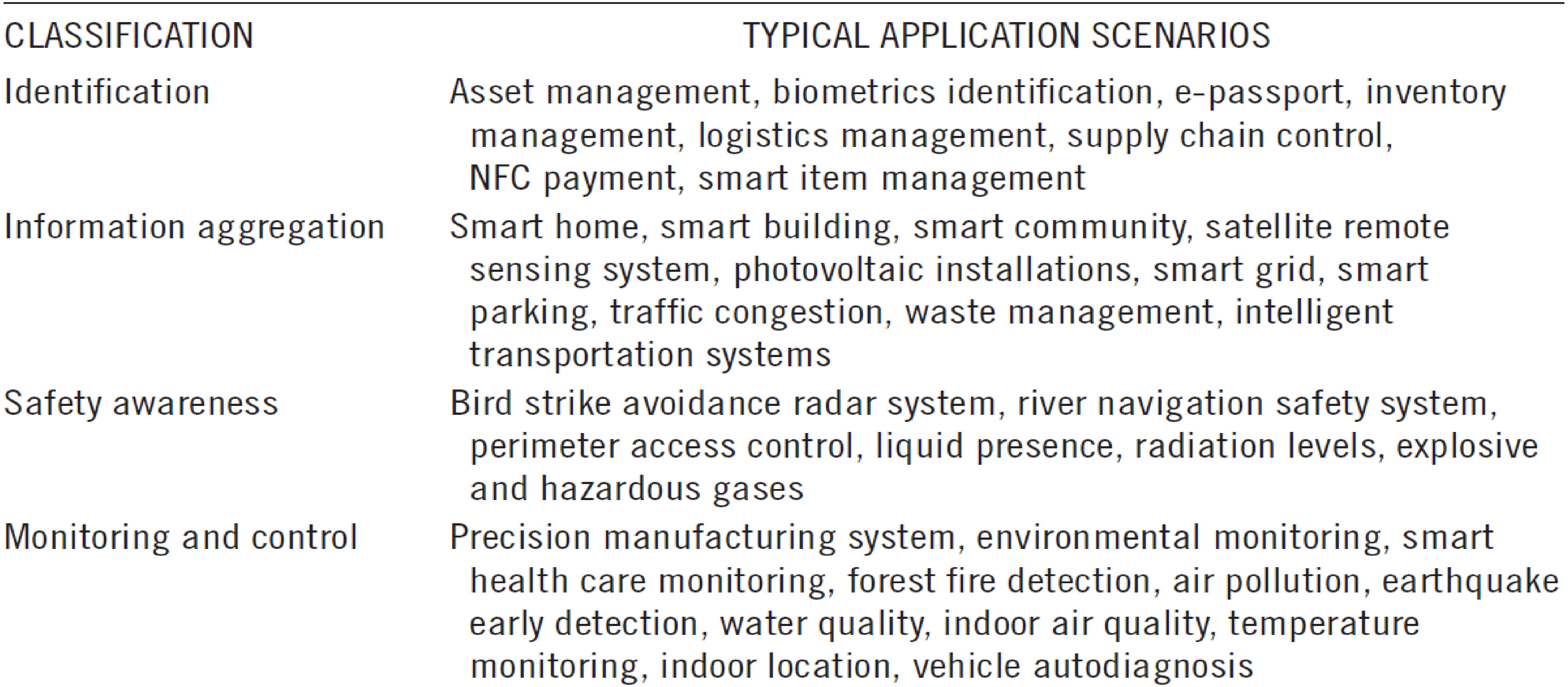
Data Fusion and Data Mining

→ Heterogeneous data mining

- Heterogeneous data may be collected by different sensor and communication networks according to the context awareness of an environment, things, and individuals.
- The integrated data mining model should be established by combining the advantages of hierarchical, distributed, and grid models.
- Self-adaptive data mining algorithms can be supporting service-oriented applications (e.g., intelligent transportation and intelligent logistics).

Case Study for Unit IoT (Revisited)

→ Unit IoTs are developed with different practical functions and requirements in which unit IoTs are classified into four aspects: identification, information aggregation, safety awareness, and monitoring and control.



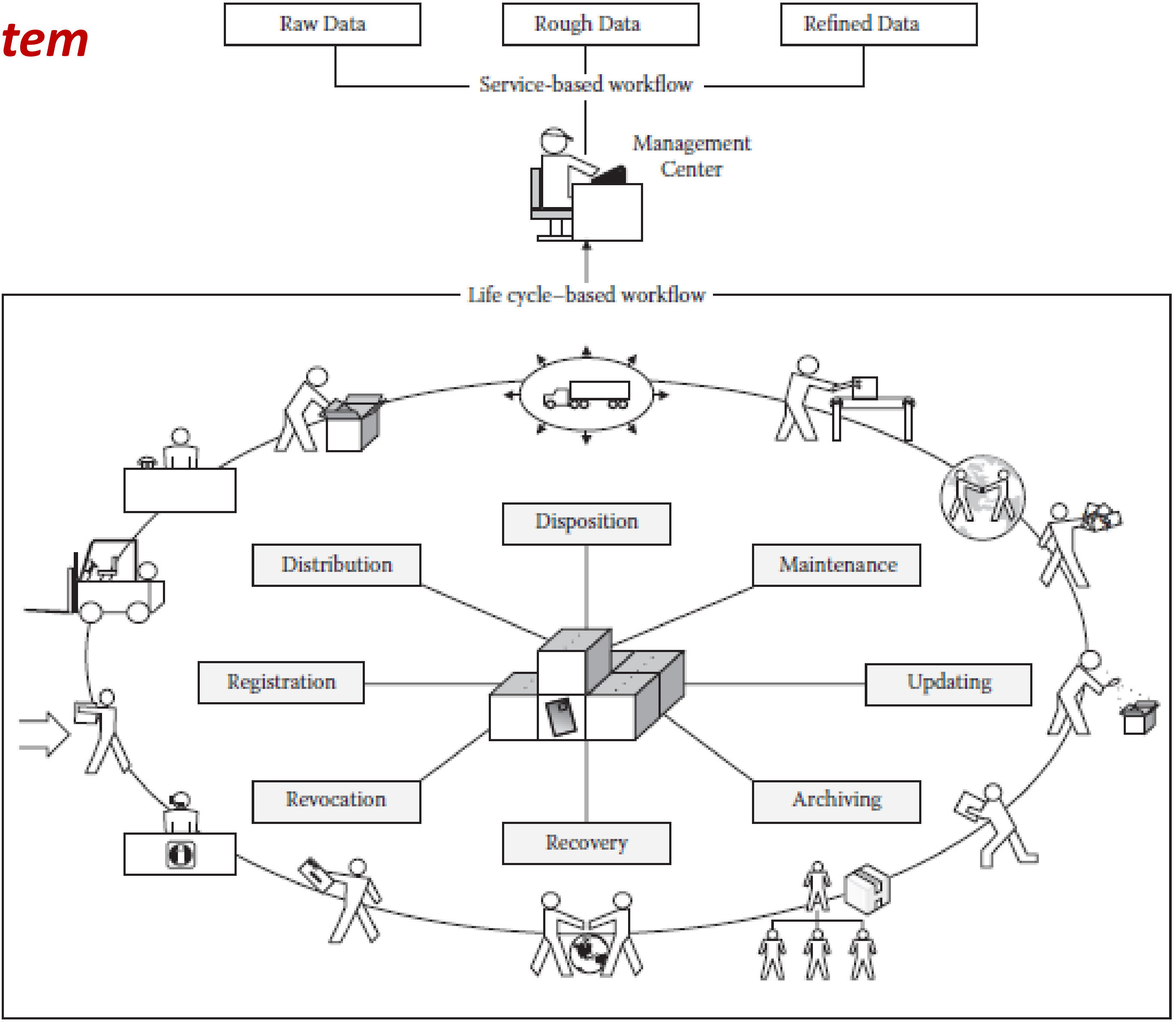
CLASSIFICATION	TYPICAL APPLICATION SCENARIOS
Identification	Asset management, biometrics identification, e-passport, inventory management, logistics management, supply chain control, NFC payment, smart item management
Information aggregation	Smart home, smart building, smart community, satellite remote sensing system, photovoltaic installations, smart grid, smart parking, traffic congestion, waste management, intelligent transportation systems
Safety awareness	Bird strike avoidance radar system, river navigation safety system, perimeter access control, liquid presence, radiation levels, explosive and hazardous gases
Monitoring and control	Precision manufacturing system, environmental monitoring, smart health care monitoring, forest fire detection, air pollution, earthquake early detection, water quality, indoor air quality, temperature monitoring, indoor location, vehicle autodiagnosis

Case Study for Unit IoT (Contd.)

Case Studey-1: Asset management System

→ Fig shows an asset management system model with two main workflows: life cycle–based workflow and service-based dataflow.

→ Life cycle–based workflow addresses inventory management according to the involved operations during an asset's life cycle. Management mainly includes phases such as registration, distribution, disposition, maintenance, upgrading, archiving, recovery, and revocation. Note that the phases may be performed in parallel or sequential modes.



Case Study for Unit IoT (Contd.)

Case Studey-1: Asset management System

→ Service-based dataflow considers asset data and interactive data during interoperation, and performs management to provide intelligent decision and support

→ The related data can be classified into three types providing different services: raw data, rough data, and refined data.

- The Raw data are persistently acquired by sensors, to provide the primal data source for a back-end management system.
- The rough data are periodically obtained according to dynamic conditions and behaviors, to provide further data fusion and mining, and to achieve dynamic supervision.
- The refined data are obtained by performing intelligent management algorithms considering multiple data factors, to support efficient allocation, scheduling, and assistant decisions.

Case Study for Unit IoT (Contd.)

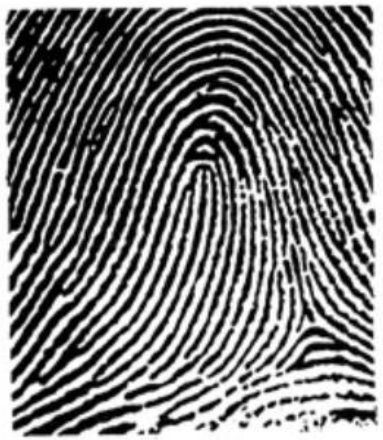
Case Studey-2: Biometric identification System

→ Biometrics Identification

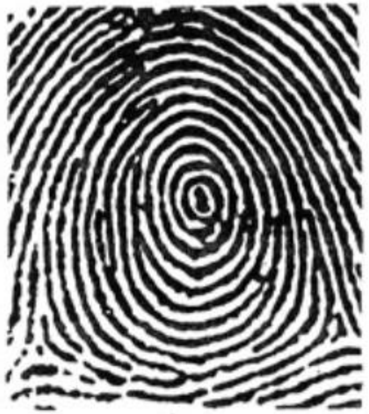
- Biometrics identification belongs to nID-based identification technologies.
- Typical biometrics identification attributes include fingerprint, hand geometry, palm vein, retina/iris, face, signature, and voice

→ Fingerprint

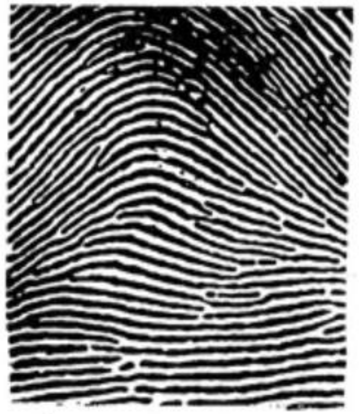
- A fingerprint is congenitally formed and progressively grows with age. However, the relationship between the ridges in a fingerprint always remains the same, which can be used for identification
- Fingerprint identification is based on pattern recognition where the arches, loops and whorls of the fingerprint ridges are compared with stored data.



Loop



Whorl



Arch

Case Study for Unit IoT (Contd.)

Case Studey-2: Biometric identification System

- Identification is performed in three parts.
  - A picture is taken of the fingerprint.
  - The picture can be taken optically with a camera in the reader or electronically, or as a combination of these two methods.
  - The end result is a digital black and white photograph of the ridges in the fingerprint.
  - The fingerprint is then transformed into a numerical model which stores the fingerprint’s unique characteristics, such as the arches and loops and their distance from each other, as a series of numbers.
  - A recognized numerical model is compared with a stored numerical model (or models) to find similarities

Case Study for Unit IoT (Contd.)

Case Studey-2: Biometric identification System

→ Hand geometry

- Hand geometry is used to measure and compare the hands’ physical features, including different shapes of points, lines, and combined shapes, with the feature value location and distribution.
- Note that hand geometry is gradually changing along with the external environment, and internal physical/health condition, but it is relatively invariable during a certain period.

Case Study for Unit IoT (Contd.)

Case Studey-2: Biometric identification System

→ Hand geometry

- Hand geometry systems use a camera to capture a silhouette image of the hand.
- The hand of the subject is placed on the plate, palm down, and guided by five pegs that sense when the hand is in place.
- The resulting data capture by a Charge-Coupled Device (CCD) camera of the top view of the hand including example distance measurements.
- The image captures both the top surface of the hand and a “side image” that is captured using an angled mirror. Upon capture of the silhouette image, 31,000 points are analyzed, and 90 measurements are taken; the measurements range from the length of the fingers, to the distance between knuckles, to the height or thickness of the hand and fingers.
- This information is stored in nine bytes of data; an extremely low number compared to the storage needs of other biometric systems.

Case Study for Unit IoT (Contd.)

Case Studey-2: Biometric identification System

→ Palm vein

- Palm vein identification applies palm vascular patterns as identification data, which indicate complicated biological information with distinguishable features for personal identification.
- Such identification applies an infrared beam to penetrate the hand, and the veins within the palm are returned as visualization information.
- Due to the complexity of internal vein patterns of the palm, it provides high authentication accuracy.
- The contactless identification consists of image sensing and data processing. The palm vein sensor is used to capture a palm infrared ray image for data analysis.
- Palm vein authentication works by comparing the pattern of veins in the palm (which appear as blue lines) of a person being authenticated with a pattern stored in a database

Case Study for Unit IoT (Contd.)

Case Studey-2: Biometric identification System

→ Palm vein

- Vascular patterns are unique to each individual
- A near-infrared light translates your palm vein pattern into a secure digital template

Case Study for Unit IoT (Contd.)

Case Studey-2: Biometric identification System

→ Retina/iris

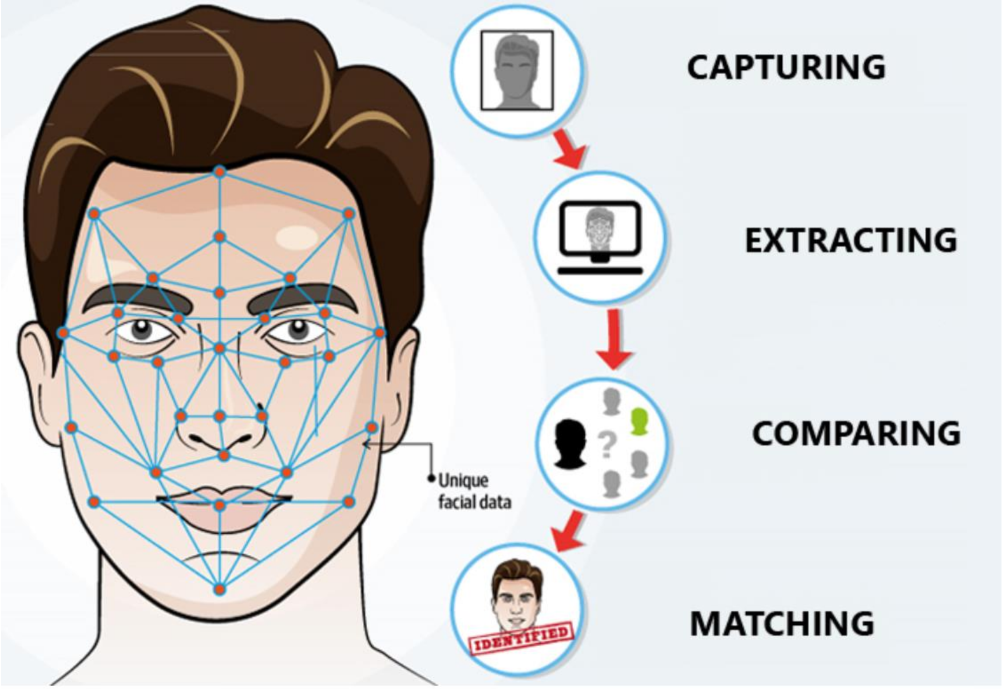
- A retina scan provides data of the capillary blood vessels located in the back of the eye for identification, by using a low-intensity light to establish a pattern formed by the blood vessels.
- Although each retina pattern is unique, it has built-in limitations for being affected by disease, such as glaucoma, diabetes, and autoimmune deficiency syndrome.
- Iris identification refers to the combined technologies, including computer vision, pattern recognition, statistical interference, and optics.
- An iris scan provides an analysis of the rings, furrows, and freckles in the colored ring that surrounds the pupil.
- Both retina and iris identification are used to achieve near-instant, highly accurate recognition based on a digitally represented image of the scanned eye, and can be regarded as a lifelong password for an individual's identity.

Case Study for Unit IoT (Contd.)

Case Studey-2: Biometric identification System

→ Face Identification/ Recognition

- Face recognition is based on facial characteristics (e.g., size, shape, and facial relationship) according to geometric/feature and photometric/view features.
- There are several predominant approaches for identification, including principal component analysis, linear discriminant analysis, and elastic bunch graph matching.



Case Study for Unit IoT (Contd.)

Case Studey-2: Biometric identification System

→ Signature

- Signature identification refers to handwriting style-based recognition. The offline and online modes are used for signature scanning, character extraction, and character recognition.
- Therefore, an offline signature is easier to be forged than an online signature.
- Signature identification is still an open issue due to the non vision-based technology, in which an individual's handwriting is a dynamic representation.

→ Voice

- Voice analysis focuses on key parameters, including pitch, tone, cadence, and frequency.

Case Study for Unit IoT (Contd.)

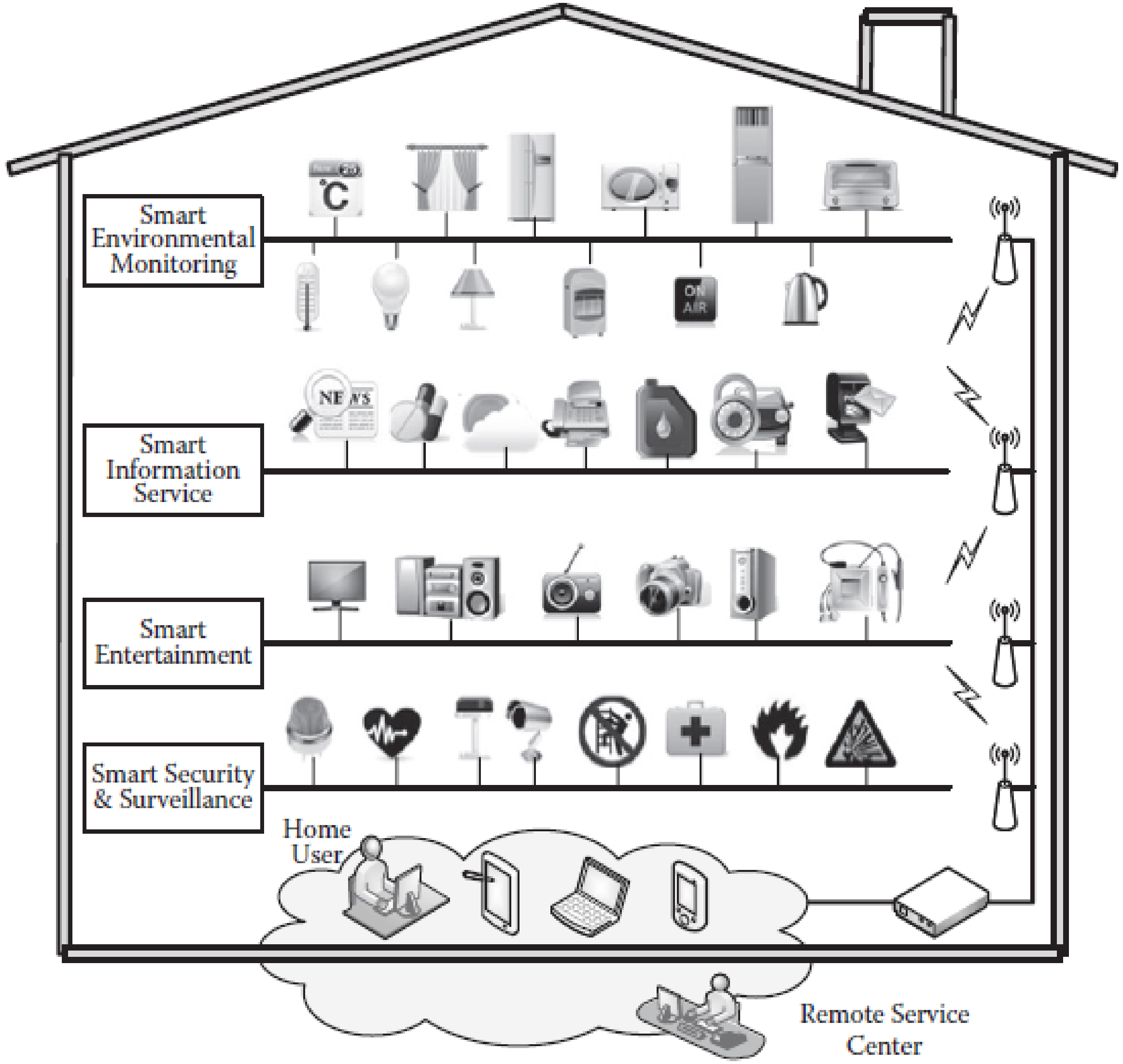
Case Studey-3: Smart Homes

→ Smart home has been established to realize intelligent and convenient human-inhabited environments.

→ In the application, sensors and actuators are distributed around the environment to automatically monitor environmental parameters and launch control actions (e.g., switch on/off lighting), and to proactively adapt to users' demands/expectations.

→ Such a scenario involves information from multiple heterogeneous sensors and requires high standardization to ensure interoperability.

→ Smart home has received much attention from industry;


Smart Environmental Monitoring
Smart Information Service
Smart Entertainment
Smart Security & Surveillance
Home User
Remote Service Center

Case Study for Unit IoT (Contd.)

Case Studey-3: Smart Homes

→ Smart Environmental Monitoring

- Environmental monitoring mainly considers the factors of temperature, humidity, and lighting to realize user comfort and energy conservation.
- Users may locally and remotely manage temperature by controlling smart heating and cooling devices by mobile communications and the Internet.
- sers may be notified in the case that an environmental emergency occurs (e.g., smoke, flood, or fire).
- Users may be provided an energy-saving heating/cooling proposal to lessen energy wasting.
- Users can control any light from any switch at home, and can also remotely control a light via a smart phone or Internet. The lights can automatically adjust their brightness according to the surroundings.

Case Study for Unit IoT (Contd.)

Case Studey-3: Smart Homes

→ Smart information service

- A smart information service aims to provide appropriate recommended information for users.
- One aspect includes custom-defined information can be subscribed by a user's active behaviors, and will be periodically transmitted to the user.
- The information covers the weather, newspaper, billing, and subscribe-and-save–related products.
- Another aspect includes providing information according to dynamic scenes.
- For example, when a user puts vegetables in the refrigerator, the sensors may detect the detailed nutrient content and provide health knowledge or recipes via the Internet and smart phone.
- The information service is provided in push mode and pull mode.

Case Study for Unit IoT (Contd.)

Case Studey-3: Smart Homes

→ Smart entertainment

- Smart entertainment establishes an intelligent smart home theater based on smart multimedia, including multiple video and audio (V/A) devices (e.g., flat-screen TV and speakers).
- V/A systems refer to centralized networks to distribute music and video signals in the home.
- Users can enjoy multimedia entertainment by optical and coax wiring communications, and control V/A systems by wireless infrared or radio signals.
- Meanwhile, multimedia content can be loaded locally or remotely downloaded according to users’ interests.

Case Study for Unit IoT (Contd.)

Case Studey-3: Smart Homes

→ Smart security and surveillance

- A smart security system mainly uses sensors to detect conditions such as door/window contact, glass break, motion, smoke, and flood.
- A wireless controller is used for safety monitoring on various sensors and actuators.
- In the case that an abnormality occurs, a controller will launch the emergency response mechanisms, and notify users with an alarm.
- A smart surveillance system mainly provides on-site supervision with data acquisition devices (e.g., camera, recorder, and viewer) to assist in remote controlling.

Thank you