Internet of Things Security and Privacy

Lecture 5

Instructor: C. Pu (Ph.D., Assistant Professor)

puc@marshall.edu

Smart Objects

- *smart object*: an electronic device that enhances the interaction with other electronic devices as well as with people also
  - come from different technology areas and scientific disciplines
- *computing* and *telephony*: two disparate strands of development
  - play a large part in the formulation of smart objects
- the root of computing

  - computer scientists, e.g., John von Neumann; UNIX family of OS
- the root of telephony

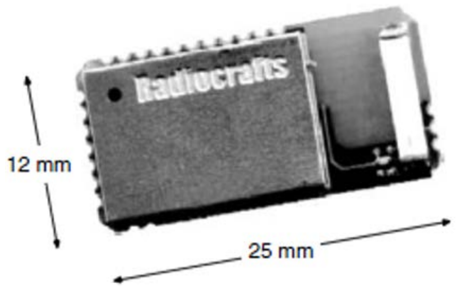
  - the first patent on telephony was filed by Alexander Graham Bell in 1876

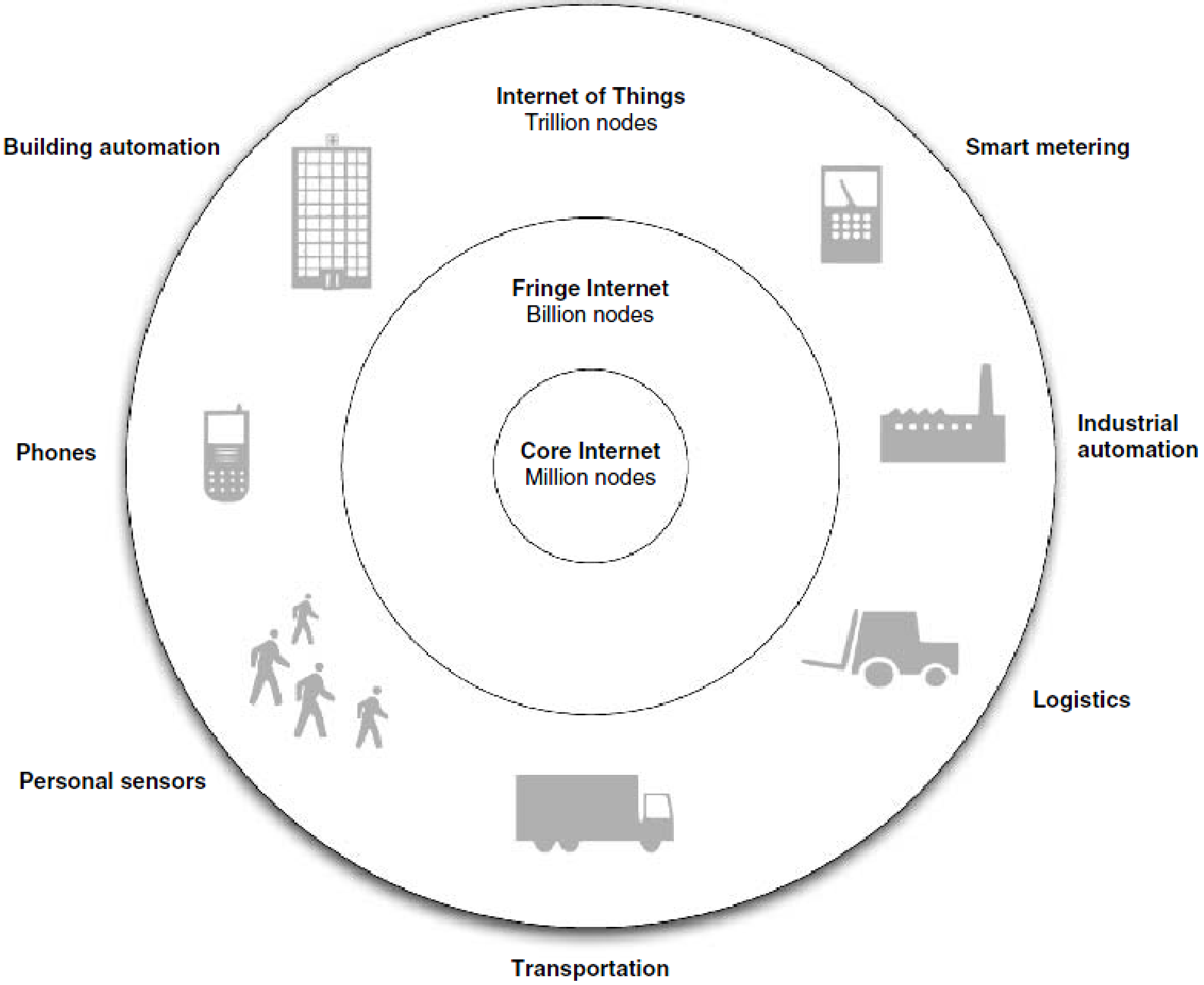
Smart Objects (cont.)

- smart objects represent the middle ground between computing and telephony, borrowing from both
  - from computing heritage: the culture of engineering evolvable systems
  - from telephony heritage: the principles of connecting disparate systems
    - smart objects are not manufactured by a single org., but by different people and parties
- smart objects must be both evolvable and standardized

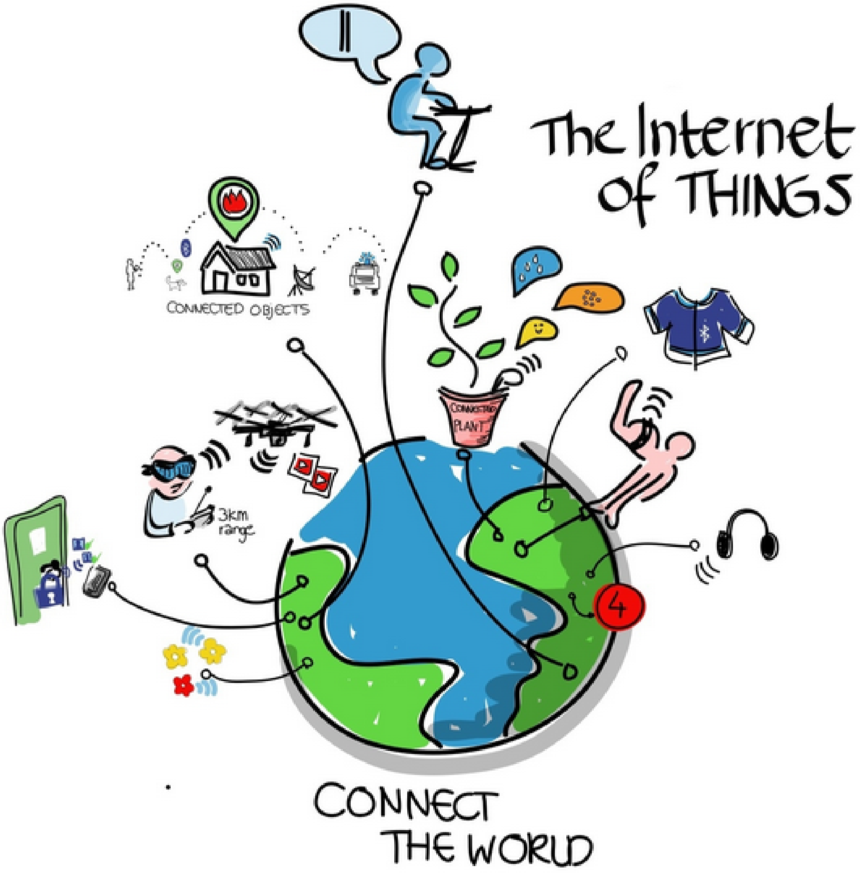
IoT Overview

- encompass all the embedded devices and networks
    - IP-enabled small objects
        - sensors, machines, positioning tags
        - radio-frequency identification (RFID)
        - automatic metering infrastructure (AMI)
        - IP Smart Objects (IPSO) Alliance (2008)
    - Internet-connected
    - wireless embedded networks
    - low-power wireless area networks (LoWPANs)
- along with the Internet services monitoring and controlling those devices




Internet of Things
Trillion nodes
Building automation
Smart metering
Fringe Internet
Billion nodes
Core Internet
Million nodes
Phones
Industrial automation
Logistics
Personal sensors
Transportation

IoT Overview:
Smart Objects



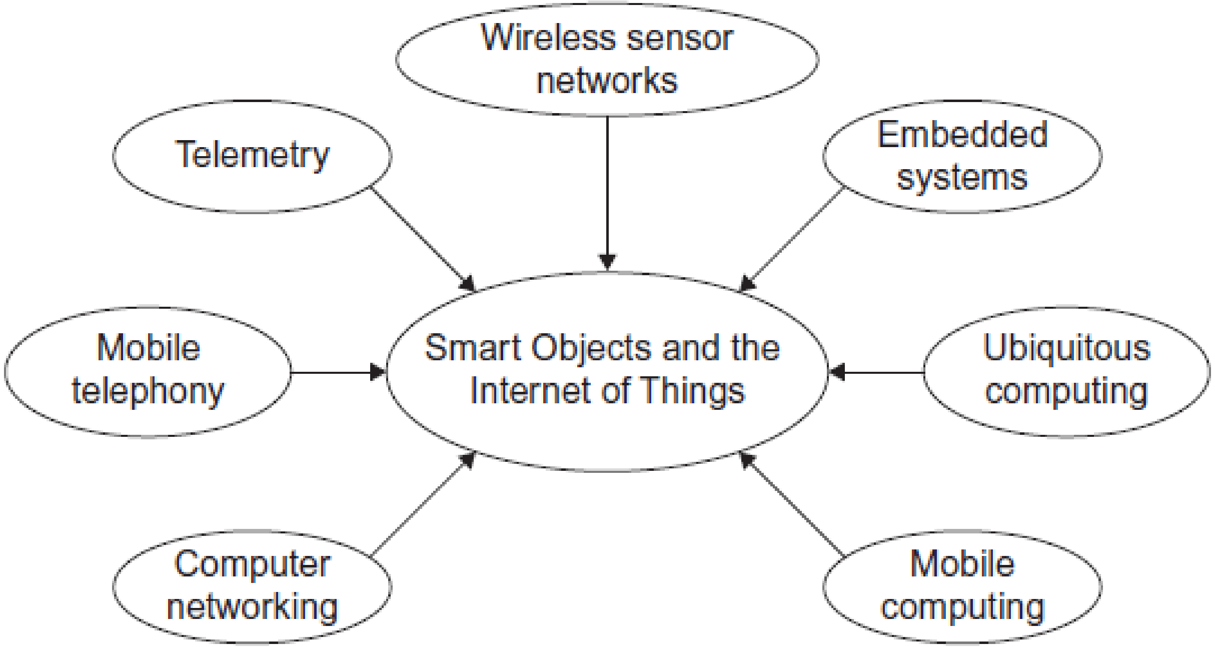
- terminologies,
  - smart objects
  - Internet of Things
  - web of objects
  - web of things
  - cooperating objects
  - use interchangeably
- smart object networks
- smart objects?
  - an item equipped with a form of
    - **sensor or actuator** – interact with the physical world
    - **a tiny microprocessor** – enable to transform/compute the captured data, limited computational capability
    - **a communication device** – communicate its sensor readings to the outside world, or receive input from other smart objects
    - **a power source** – provide the electrical energy to do its work

IoT Overview:
Smart Objects (cont.)

- what do smart objects actually do?
  - don't know exact behavior… ☹
  - depend on where and how it is used
    - e.g., monitor temperature, moisture, vibration, etc.
- two behavioral properties common to any smart object
  - interaction with the physical world
    - **sense** physical properties, e.g., air pollution, the presence of a car, etc.
    - affect the physical world using different forms of **actuators**, e.g., switching a LED, switching the heat in the building, etc.
  - communication
    - smart object networks

IoT Overview

- where do smart objects come from?
  - intersection of …



IoT Overview:
An Embedded System

- computing systems are everywhere
- most of us think of “desktop” computers,
  - PC’s, laptops, mainframes, servers
- but there’s another type of computing system
  - far more common...

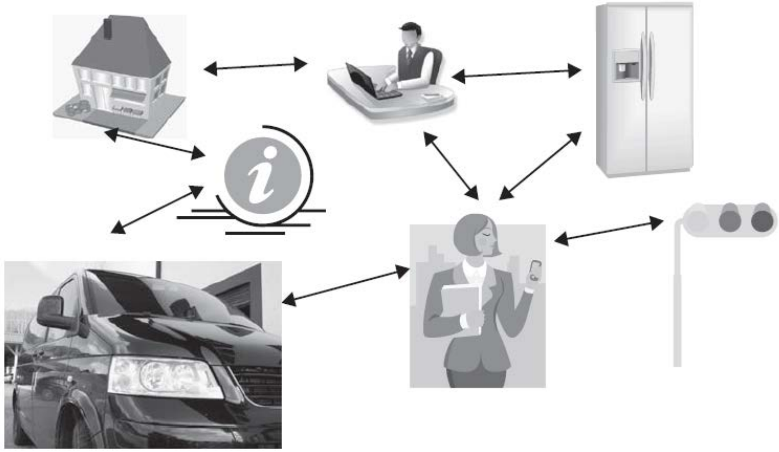
- an embedded system is an application that contains,
  - at least one programmable computer (i.e., **micro-processor** or **micro-controller**), which is used by individuals who are unaware that the system is computer-based
- embedded systems are computers with constraints
  - i.e., applications and form factors, power, systems resource, user assumptions, etc.

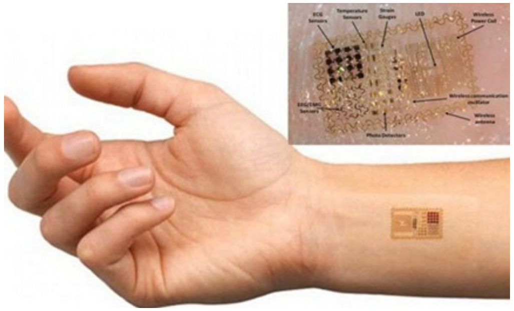
IoT Overview: Some Common Characteristics of Embedded Systems

- single-functioned:
  - execute a specific program, repeatedly
- tightly-coupled:
  - have constraints on design metrics
  - low cost, low power, small, fast, etc.
- reactive and real-time:
  - continually react to changes in the system's environment
  - must compute certain results in real-time without delay

IoT Overview: Ubiquitous and Pervasive Computing

- concept:
  - what happens when computers are mobile and become immersed in the surrounding environment?
- wearable computing, an emerging field out of the ubiquitous computing community
  - e.g., Google Glass, Fitbit, even under the skin, etc.

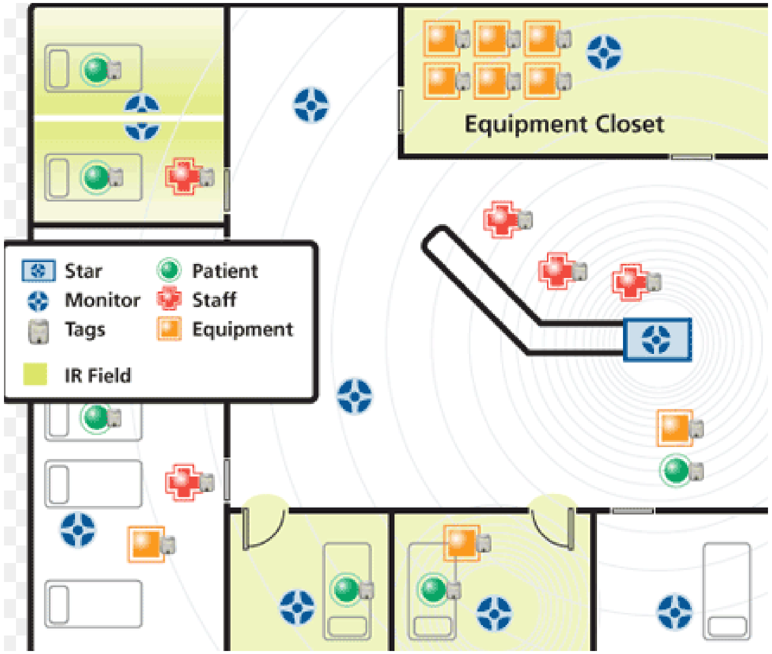




IoT Overview: Ubiquitous and Pervasive Computing (cont.)

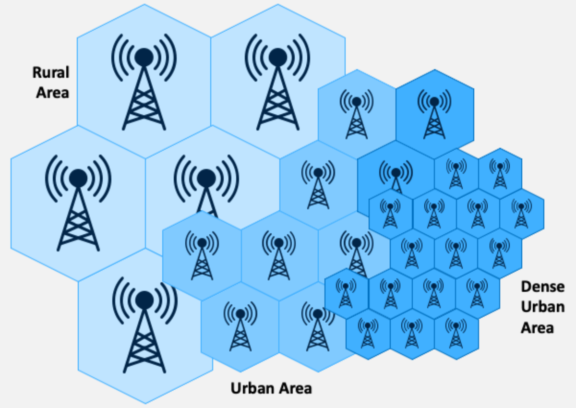
- for example,
  - active badge, AT&T laboratory in Cambridge, UK

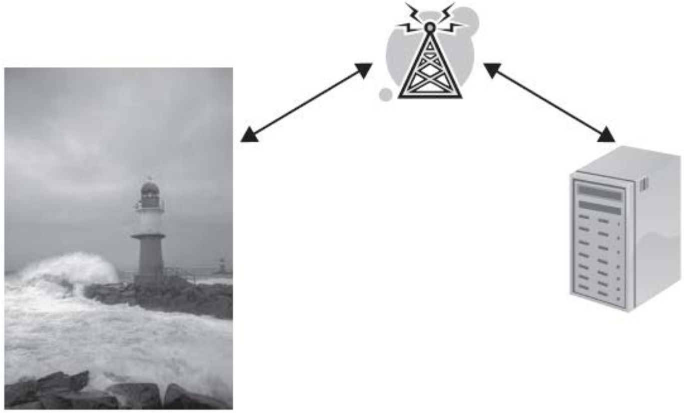
active 433MHz RFID badge tag



IoT Overview:
Mobile Telephony

- often called cellular telephony
  - long-range wireless networking technology
    - Global System for Mobile communications (GSM)
    - General Packet Radio Service (GPRS)
    - Universal Mobile Telecommunications Systems (UMTS)
  - short-range wireless communication
    - Bluetooth (IEEE 802.15.1)
    - M2M communication

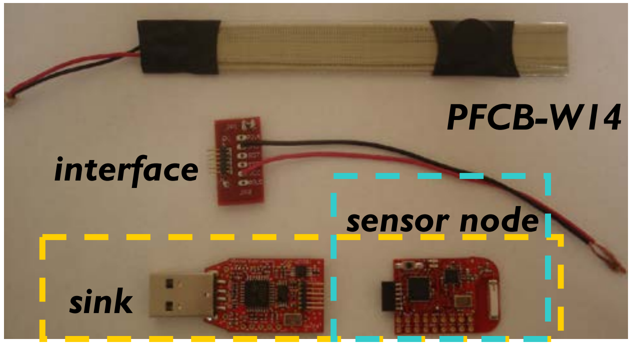




IoT Overview: Wireless Sensor and Ubiquitous Sensor Networks

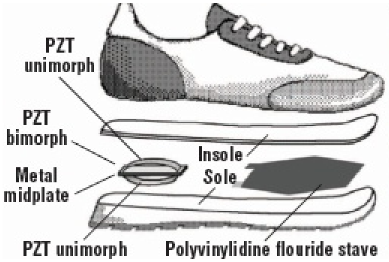
- small wireless sensors
- collect information from the physical environment
  - wild fire tracking, animal observation, agricultural management, industrial monitoring, etc.

IoT Overview: Wireless Sensor and Ubiquitous Sensor Networks

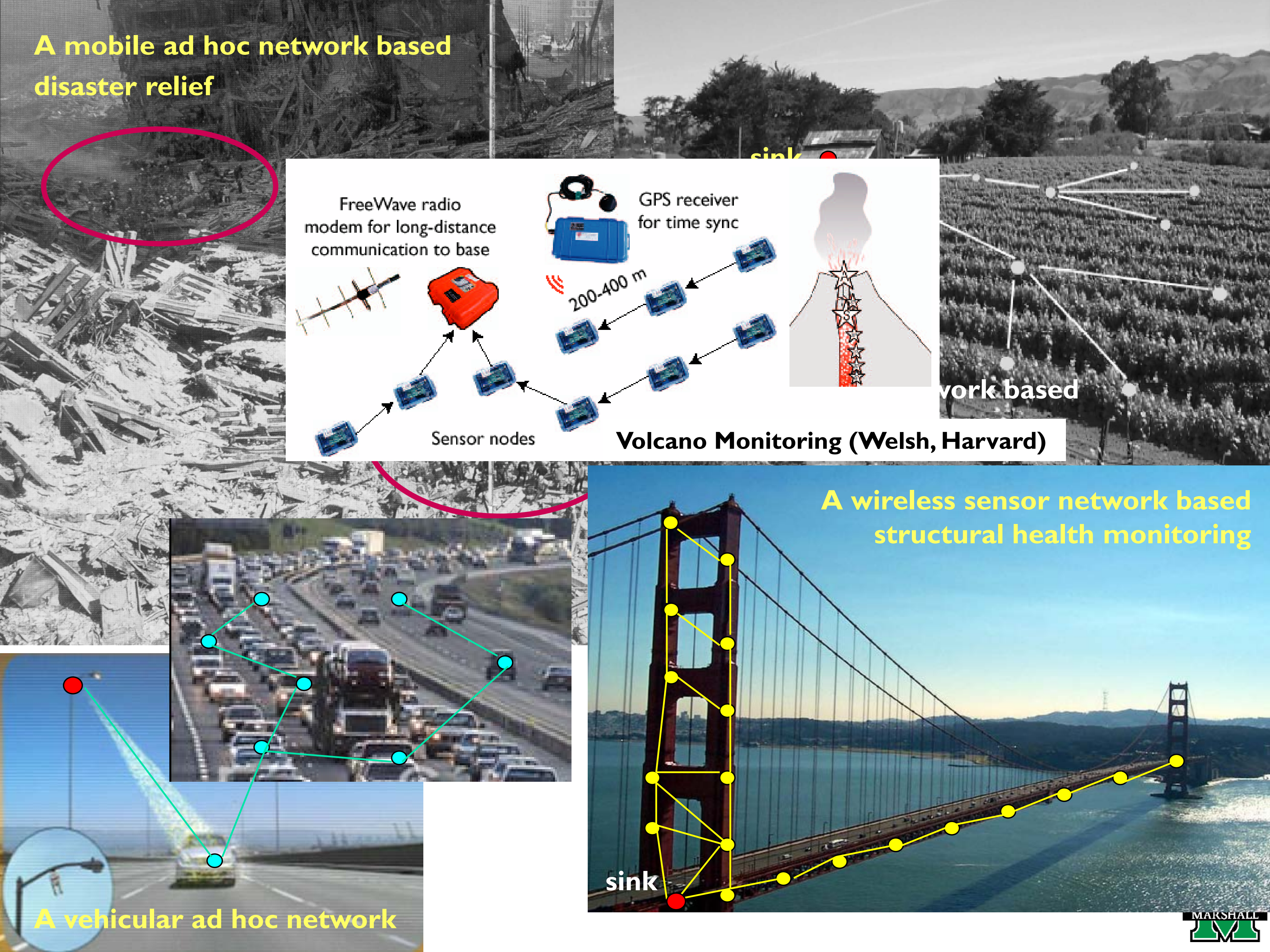
- **wireless sensor networks**,
  - deployed in an unattended environment
  - required to operate for a long period time
  - hard to replace (or replenish) battery
- environmental **energy harvesting (or scavenging)**,
  - extracting an electric energy from various environmental sources for easy of battery energy replenishment
  - vibrations, magnetic fields, thermal gradients, lights, kinetic motions, and shock waves
- **Vibration-Sensitive Energy Harvesting WSNs**
  - 

*"the **U.S. Army** has invested about $4.2 million in the development of **military Apps** and the study of **smart phone** technology"*

LIMITED BATTERY ENERGY!!!



*"the **U.S. Army** will eliminate all the military batteries. Each soldier will equip **self-powered (or battery-less)** communication devices"*



A mobile ad hoc network based disaster relief

Volcano Monitoring (Welsh, Harvard)

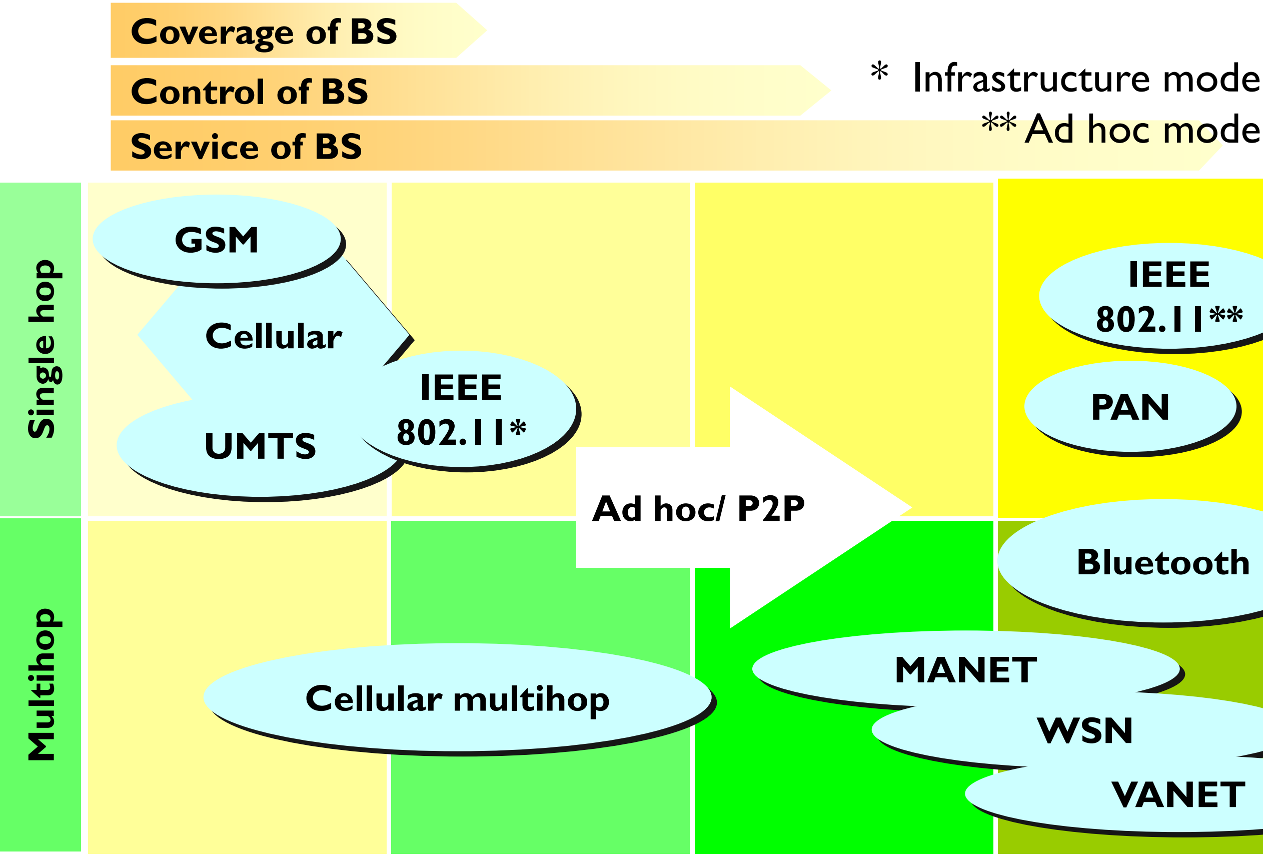
FreeWave radio modem for long-distance communication to base
GPS receiver for time sync
200-400 m
Sensor nodes
sink
vork based

A wireless sensor network based structural health monitoring

A vehicular ad hoc network

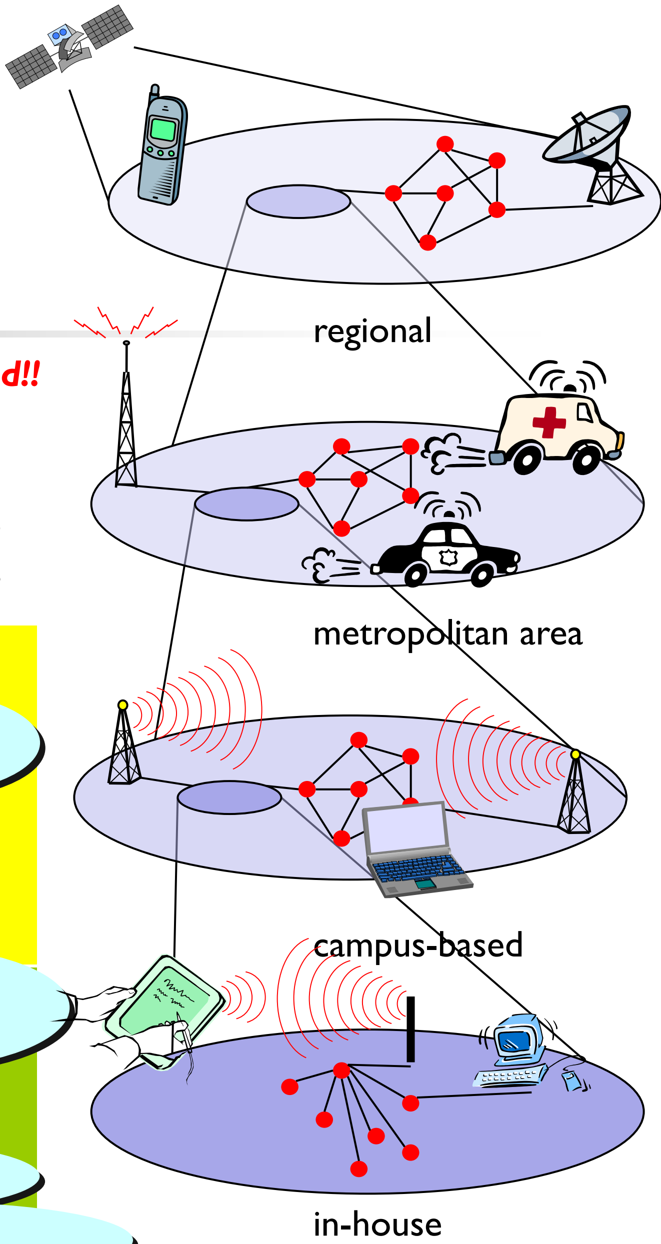
IoT Overview:
Mobile Computing

Multi-hop is still required!!



* Infrastructure mode

** Ad hoc mode



IoT Overview:
Challenges for Smart Objects

- node-level
  - power consumption
    - battery-powered or energy harvesting
  - physical node size and cost
- network-level
  - large-scale of the smart object networks
  - network and data size
  - design of the routing protocols
  - lossy nature of smart object networks
  - etc.
- standardization
  - a critical success factor for smart objects
- interoperability
  - from different vendors to operate together

IoT Security Threats

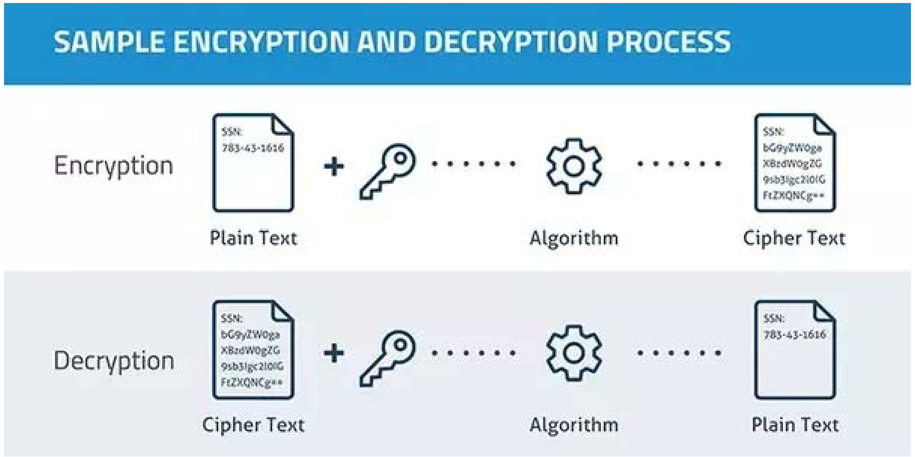
- three broad categories of threats:
  - capture
    - capturing the system or information
  - disrupt
    - denying, destroying, and disrupting the system
  - manipulate
    - manipulating data, identity, time-series data, etc.
- simplest type of passive threat: eavesdropping or monitoring
- capture attack: gain control of physical or logical systems; gain access to information or data
- active threats: masquerading; replay attacks; DoS attacks

IoT Security Requirements

- basic security properties:
  - confidentiality:
    - transmitted data can be read only by the communication endpoints;
  - availability:
    - the comm. endpoints can always be reached and cannot be made inaccessible;
  - integrity:
    - received data are not tampered with during transmission, and assured of the accuracy and completeness over its entire lifecycle;
  - authenticity:
    - data sender can be verified and receiver cannot be spoofed

Encryption

- used for centuries: ensure the confidentiality of secret communication
  - core idea: transformation of information from readable to unreadable
    - cipher: certain (shared) algorithm


SAMPLE ENCRYPTION AND DECRYPTION PROCESS
Encryption
SSN: 783-43-1616
Plain Text
+
Algorithm
SSN: bG9yZW0ga XBzdW0gZG 9sb3Igc2l0IG FtZXQNCg==
Cipher Text
Decryption
SSN: bG9yZW0ga XBzdW0gZG 9sb3Igc2l0IG FtZXQNCg==
Cipher Text
+
Algorithm
SSN: 783-43-1616
Plain Text

Ciphers

- cipher: algorithm performing encryption or decryption operations
  - input: plaintext
  - output: ciphertext
  - key
- cipher classification based on key
  - symmetric
  - asymmetric
- cipher classification based on input
  - block
  - stream

Authentication

- authentication: identity verification
  - complimentary to encryption

- symmetric authentication
  - message authentication code (MAC) authenticating a message
    - hash functions

- asymmetric authentication
  - digital signature (different from MAC)
    - using the private key of a public/private key pair

Threats to IoT Systems

- IoT will be susceptible to a plethora of threats:
    - Denial of Service attacks
    - sybil attacks
    - privacy attacks
    - physical attacks

Denial of Service Attacks

- the most common and easiest to implement attacks
  - many forms
  - core idea: undermine the network or systems' capacity to perform expected functions
- e.g., wireless network
  - jamming channel with interrupting signal
- DoS attack on four layers
  - jamming ⟹ physical layer
  - collision ⟹ link layer
  - flooding ⟹ transport layer
  - path-based DoS attack ⟹ application layer

Sybil Attacks

- sybil attack: adversary taking on multiple identities
- sybil attack on two layers
  - compromising or fabricating → physical layer
  - compromising routing path → network layer

Other Attacks

- privacy attacks: monitoring and eavesdropping
  - listening on a wired or wireless channel (difficult to detect)
- hole attacks: advertise routes through malicious nodes
- physical attacks: compromising physical integrity
  - devices destroyed
  - loss of devices