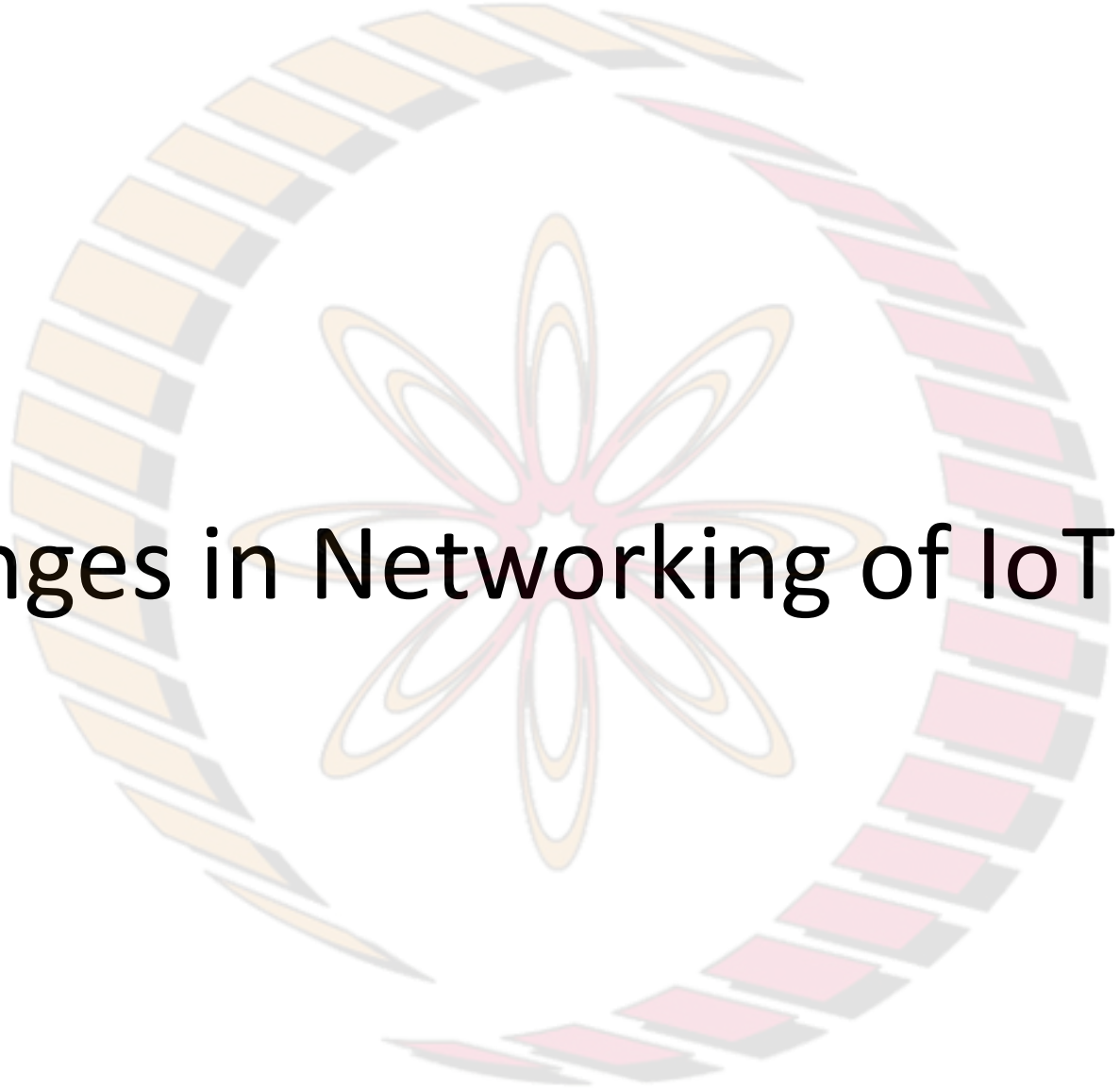
Security of the Internet of Things (IoT), Hardware Security: Part 2

Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

References

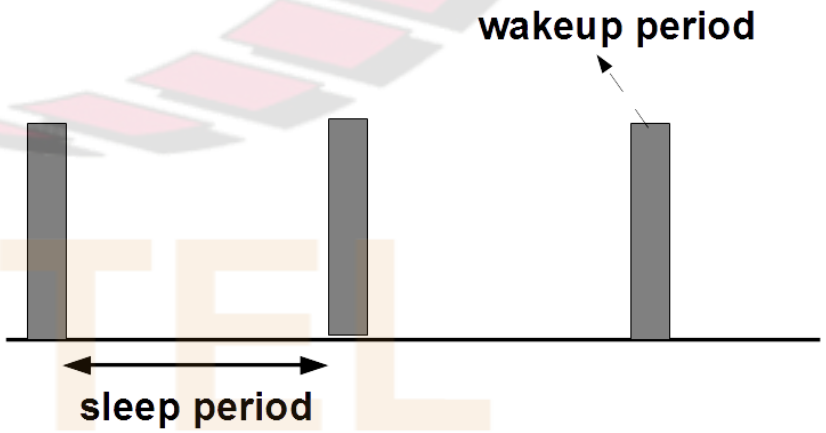
- W. Stallings, "*Cryptography and Network Security*", 8th edition, Pearson Education, 2023
- P. Lea, "*IoT and Edge Computing for Architects",* Packt Publishing Ltd., 2020
- D. Hanes, G. Salgueiro, P. Grossetete, R. Barton, and J. Henry, "*IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things",* Cisco Press, 2017

Challenges in Networking of IoT Nodes



Challenges in Networking of IoT Nodes

- Existing Internet protocols were not designed for IoT nodes
- IoT nodes (e.g., sensors, actuators) are typically designed for:
  - Low cost
  - Low power consumption
- So IoT nodes:
  - Have limited available power (often battery operated)
  - Have limited memory
  - Have limited processing resources
  - Are disabled for long time intervals (sleep periods) to save energy



Challenges in Networking of IoT Nodes (contd.)

- IoT nodes have different:
  - data traffic characteristics
  - and Quality of Service (QoS) requirements

  from those of traditional devices connected to Internet
- E.g.:
  - Network access often needs to be provided to an *extremely large number* of IoT devices (e.g., several sensors in each smart home, smart meters)
  - IoT nodes may transmit small bursts of data periodically or randomly (e.g., soil moisture, temperature sensors in precision agriculture)
  - May have stringent latency requirements or need priority access to communicate alarms (e.g., in healthcare and security applications)
  - May require highly reliable communication (e.g., in remote payment systems)
  - May require high throughput (e.g., in a video surveillance application)

IoT Node Access Methods

IoT Node Access Methods

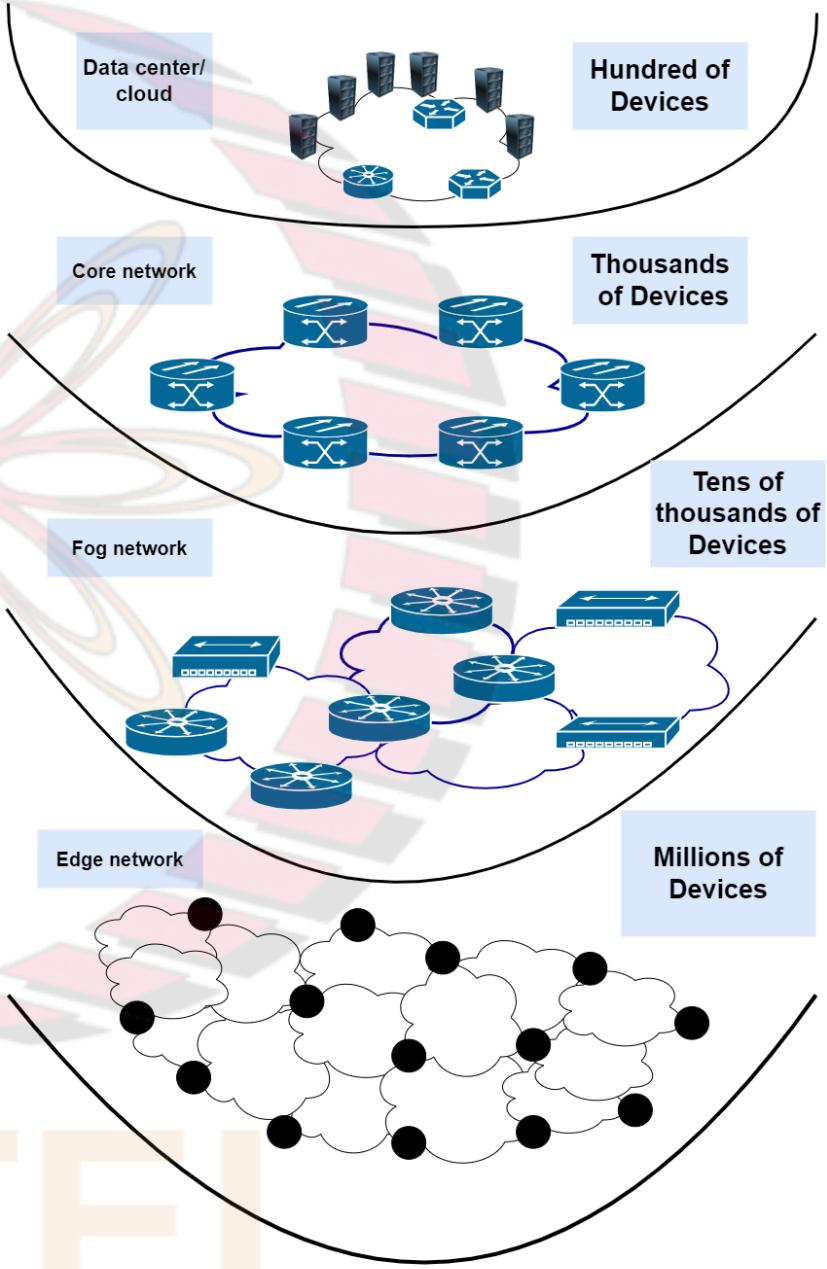
- Access network connects IoT nodes to infrastructure (e.g., Internet)
- Access network can be either wired (e.g., cable, DSL, optical) or wireless
- Wired access:
  - ❑Advantages:
    - can provide high reliability, high data rates, small delay
  - ❑Disadvantages:
    - expensive, difficult to scale, cannot support mobile IoT nodes
- Wireless access:
  - ❑Short-range (e.g., Wi-Fi, IEEE 802.15.4)
  - ❑Wide-area/ Cellular (e.g., LTE-Advanced, 5G)
  - ❑Low Power Wide Area Networks

IoT Node Access Methods (contd.)

- Short-range wireless (e.g., Wi-Fi, IEEE 802.15.4):
  - ❑ Advantages:
    - Inexpensive, scalable, low power
  - ❑ Disadvantages:
    - Low data rates, interference, lack of universal coverage
- Wide-area/ Cellular (e.g., LTE-Advanced, 5G)
  - ❑ Advantages:
    - Provides ubiquitous coverage and mobility, no interference from other networks
  - ❑ Disadvantages:
    - Due to high demand for human-to-human communication services (e.g., voice, data), only a limited amount of radio spectrum is available with cellular operators to support IoT node communication

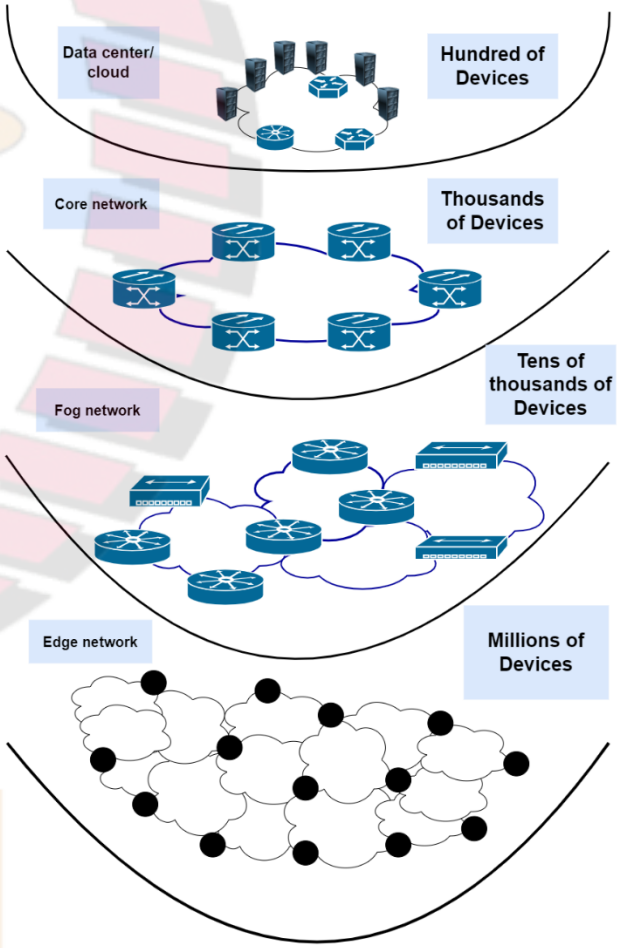
IoT, Fog, and Cloud

- Fig. shows a typical network with IoT devices, fog nodes, core network, and cloud
- **Edge**:
  - There is a network of IoT-enabled devices, consisting of sensors and actuators
  - These devices send their data to each other and/ or to gateways
  - Gateways perform translation between protocols used in the IoT devices and those in the core network
  - Gateways may also perform a basic data aggregation function



IoT, Fog, and Cloud (contd.)

- **Fog Nodes**:
  - In many IoT deployments, massive amounts of data (e.g., several terabytes a day) may be generated by a distributed network of sensors
  - This volume of data generated by IoT devices can be so great that it can easily overrun the capabilities of the cloud
  - Solution to above challenges is to distribute data management throughout the IoT system, as close to edge of IP network as possible
  - Best-known embodiment of edge services in IoT is *fog computing*
  - Any device with computing, storage, and network connectivity can be a fog node
  - E.g., industrial controller, switches, routers, embedded servers, IoT gateways
  - Advantages of analyzing IoT data close to where it is collected:
    - Latency is minimized
    - Gigabytes of network traffic is offloaded from core network
    - Sensitive data is kept inside the local network
- **Core Network**:
  - Also known as backbone network
  - Connects geographically dispersed fog networks to the data center/ cloud
  - Typically uses very high performance routers and high-capacity transmission lines
- **Cloud**:
  - Provides storage and processing capabilities for the massive amounts of data that originate in IoT devices at edge



IoT Security Objectives

- Restricting Access to IoT Network:
  - This may include: using unidirectional gateways, using firewalls, and strictly enforcing authentication mechanisms and credentials for users of the IoT network
- Restricting Physical Access to IoT Network and Components:
  - A combination of physical access controls should be used, e.g., locks, card readers, and/ or guards
- Protecting Individual IoT Components from Exploitation:
  - Deploying security patches in an expeditious manner
  - Disabling all unused ports and services
  - Restricting IoT user privileges to only those that are required for each person's role
  - Using antivirus software and file integrity checking where feasible
- Preventing Unauthorized Modification of Data:
  - This includes data in transit and at rest
- Detecting Security Events and Incidents:
  - Detecting security events early enough to break the attack chain before attackers attain their objectives
  - This includes capability to detect failed IoT components, unavailable services, and exhausted resources

IoT Security Objectives (contd.)

- Maintaining Functionality During Adverse Conditions:
  - Designing IoT systems so that each critical component has a redundant counterpart
  - If a component fails, it should fail in a manner that does not generate unnecessary traffic on IoT or other networks, or does not cause another problem elsewhere
  - IoT systems should also allow for graceful degradation such as moving from normal operation with full automation to emergency operation with operators more involved and less automation to manual operation with no automation
- Restoring the System After an Incident:
  - Incidents are inevitable and an incident response plan is essential
  - The IoT system should be recovered quickly after an incident has occurred