Iceland Liechtenstein Norway grants

Computing Innovation for Technology Entrepreneurship

Information and Communications Technology based Innovation

CITE
Computing Innovation for Technology Entrepreneurship

Innovative Trends: Internet of Things, Fog Computing

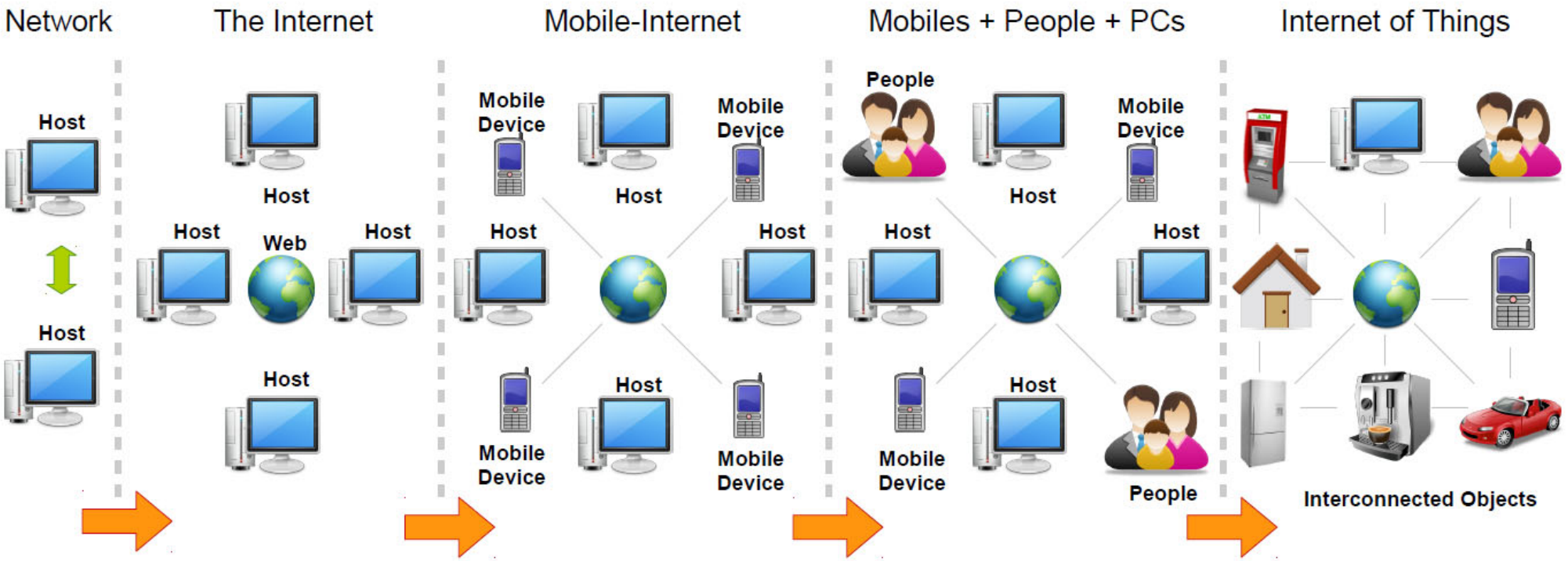
Andrei VASILĂȚEANU

Outline

- **Introduction**
- Sensor networks
- iLight
- Fog computing
- IoT Security

IoT paradigm

- another step in the evolution of the Internet we already have



C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, Context aware computing for the internet of things: A survey

Some definitions

- "Things have **identities** and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within **social, environment, and user contexts**."
- "The semantic origin of the expression is composed by two words and concepts: Internet and Thing, where Internet can be defined as the world-wide network of interconnected computer networks, based on a standard communication protocol, the Internet suite (TCP/IP), while Thing is an object not precisely identifiable. Therefore, semantically, Internet of Things means a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols."

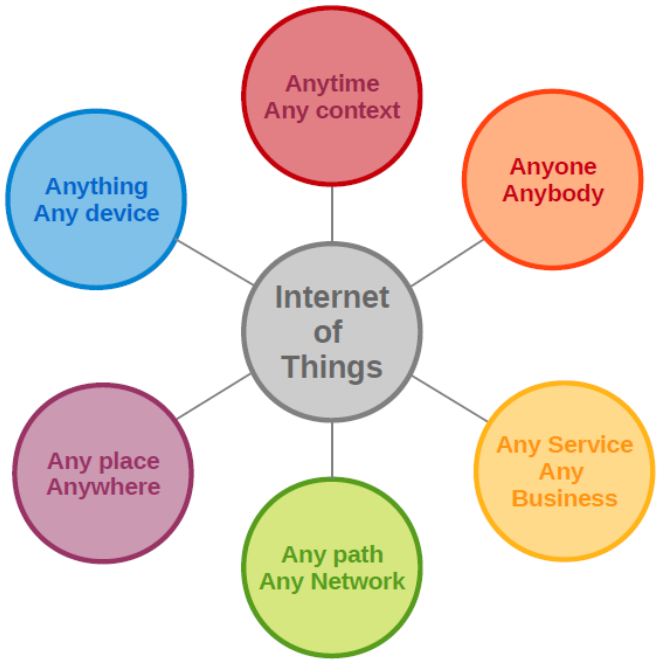
Some definitions

- "The Internet of Things allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service."
- "The IoT is what we get when we connect Things, which are not operated by humans

  to the Internet"
- Objects aware of

  their context, that can

  communicate



Evolution of definitions

- Internet of Everything – IoE "people, things and places that can expose their services to other entities"
- Industrial IoT – IIoT – eg M2M, Big Data, Machine learning used in manufacturing "Industry 4.0"
- Smartness in IoT. A smart network is characterized by:
  - Standardization, openness of the communication standards
  - Object addressability and multifunctionality (network built for one app can be available for other purposes)

What is not IoT

- Wireless sensor networks – specificity, no actuators, connectivity
- M2M (machine to machine), CPS (cyber physical system) – humans can access Things, openess

IoT application domains

- smart cities
- smart environment
- smart water
- smart metering
- security and emergencies
- retail
- logistics
- industrial control
- smart agriculture
- smart animal farming,
- domestic and home automation
- eHealth

Some statistics

- 1.5 billion Internet-enabled PCs and over 1 billion Internet-enabled mobile phones today.
- By 2020, there will be 50 to 100 billion devices connected to the Internet
- Global market for sensors is estimated at $91.5 billion by 2016

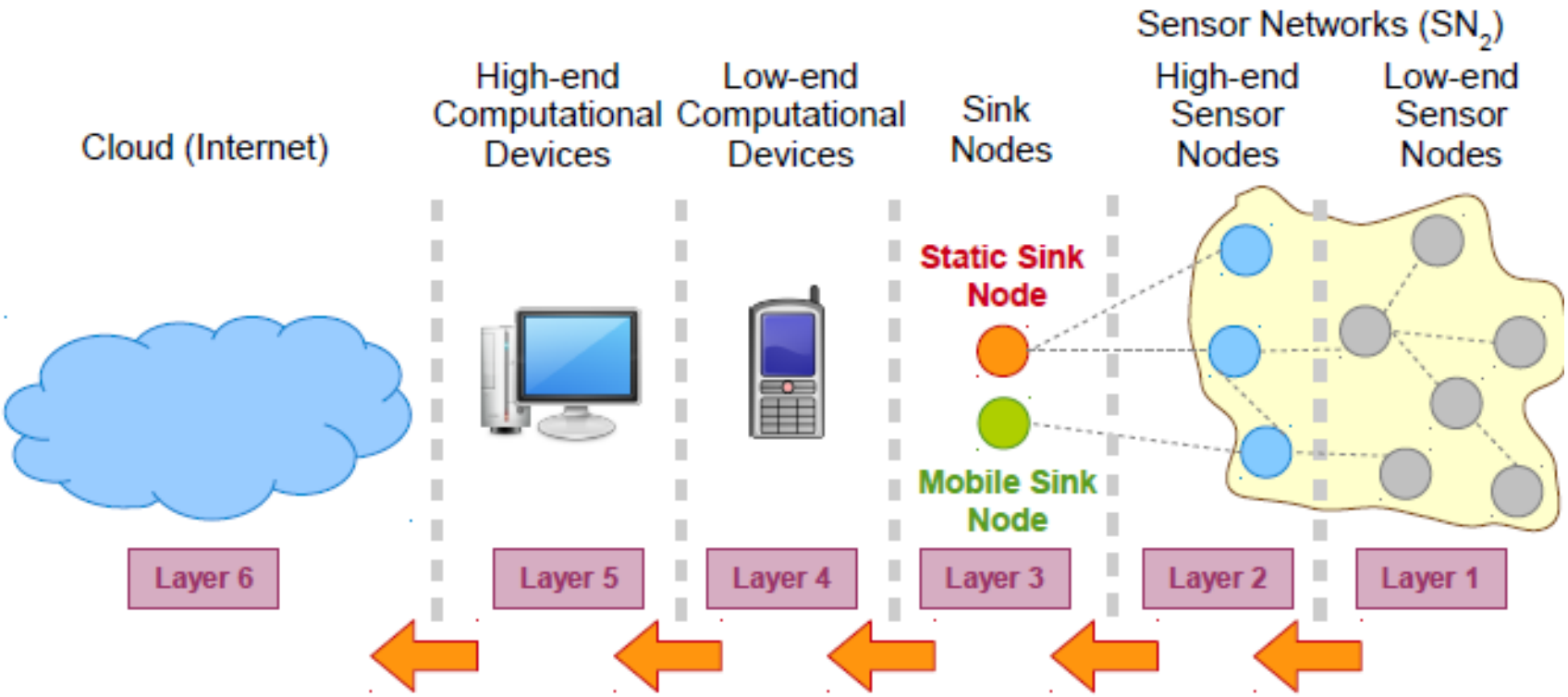
Outline

- Introduction
- **Sensor networks**
- iLight
- Fog computing
- IoT Security

Sensor networks

- Main component of IoT
- comprise one or more sensor nodes, which communicate between themselves using wired and wireless technologies
- Sensors – homogeneuos, heterogeneus
- Three main architectures
  - Flat architecture (data transfers from static sensor nodes to the sink node using a multi-hop fashion)
  - two-layer architecture (more static and mobile sink nodes are deployed to collect data from sensor nodes)
  - three-layer architecture (multiple sensor networks are connected together over the Internet).

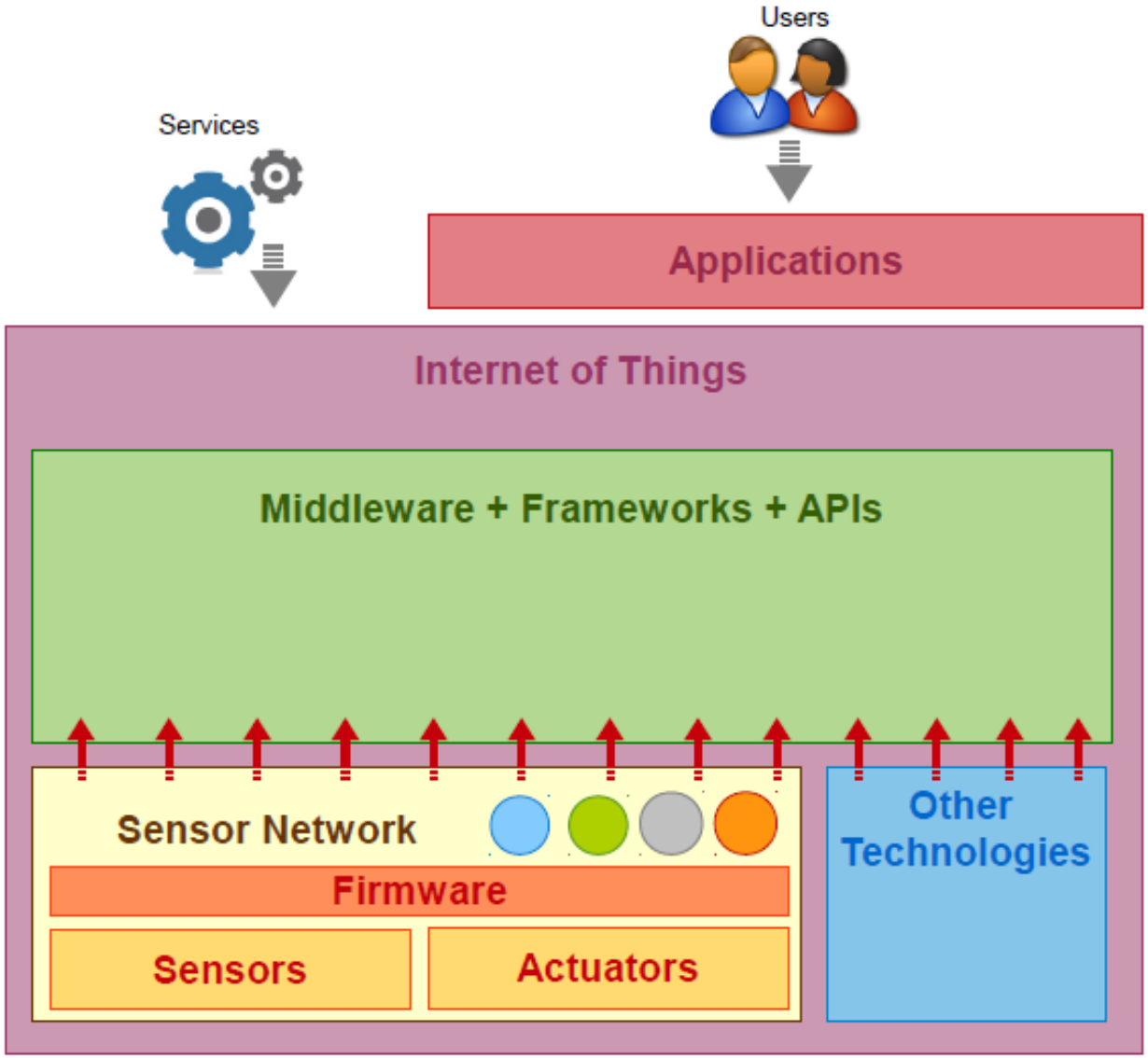
Layers in sensor networks



Sensor Networks and IoT

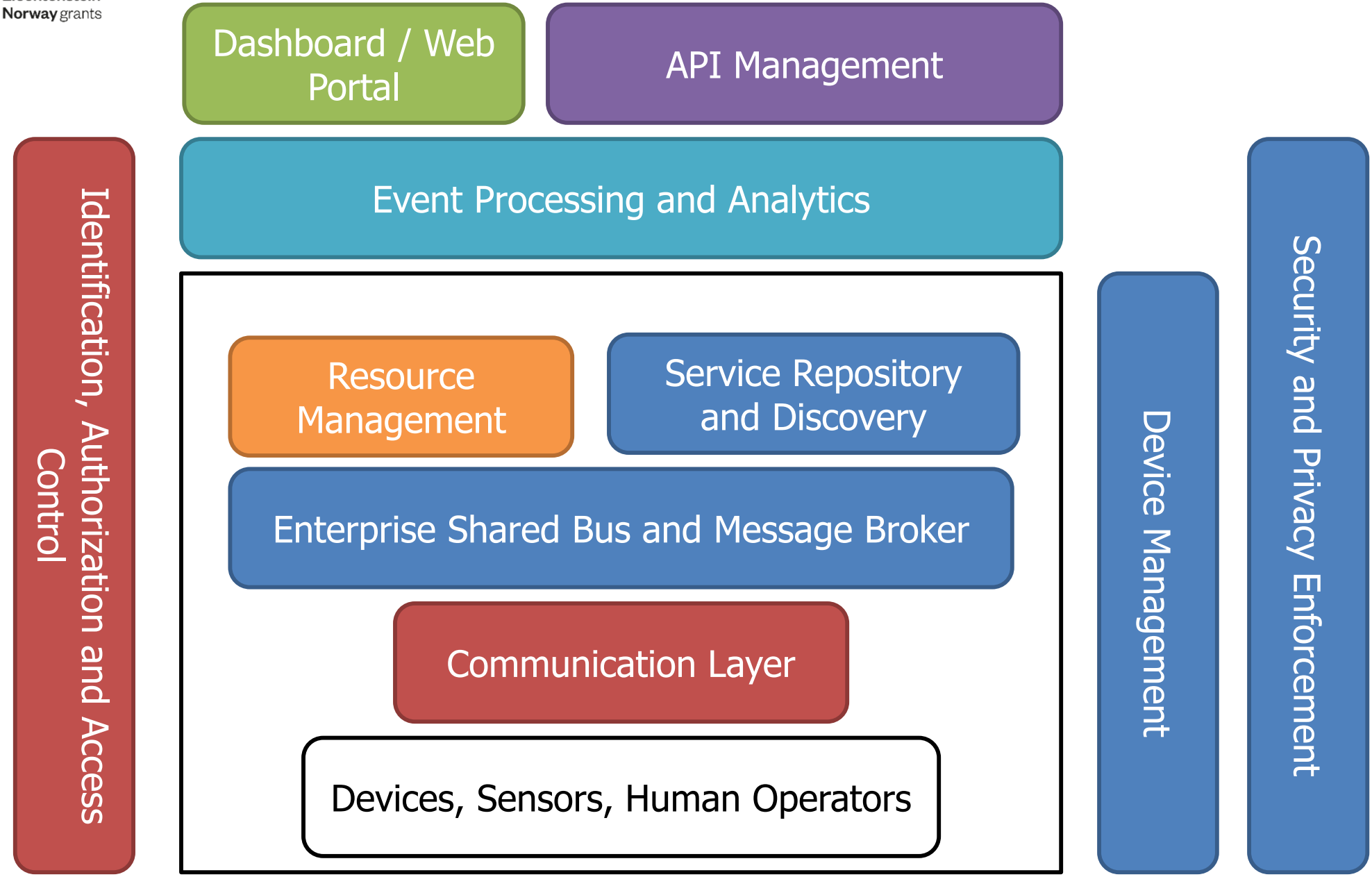
- SN comprises of the sensor hardware (sensors and actuators), firmware and a thin layer of software. IoT comprises everything that SN comprises and further it comprises actuators, a thick layer of software such as middleware systems, frameworks, APIs and many more software components.
- SNs are designed for specific application purposes, IoT can support new applications
- SN are a part of the IoT. However, the IoT is not a part of SN

Sensor Networks and IoT



IoT characteristics

- Intelligence: collecting raw data, transforming it into knowledge
- Architecture: event driven, time driven
- Complex system: large number of different objects, different capabilities, intelligence
- Size considerations: increasing number of objects and interactions
- Time considerations: real-time computation
- Space considerations: interactions depend on location
- Everything-as-a-service: share data, for example sensing-as-a-service


Dashboard / Web Portal
API Management
Event Processing and Analytics
Resource Management
Service Repository and Discovery
Enterprise Shared Bus and Message Broker
Communication Layer
Devices, Sensors, Human Operators
Identification, Authorization and Access Control
Device Management
Security and Privacy Enforcement

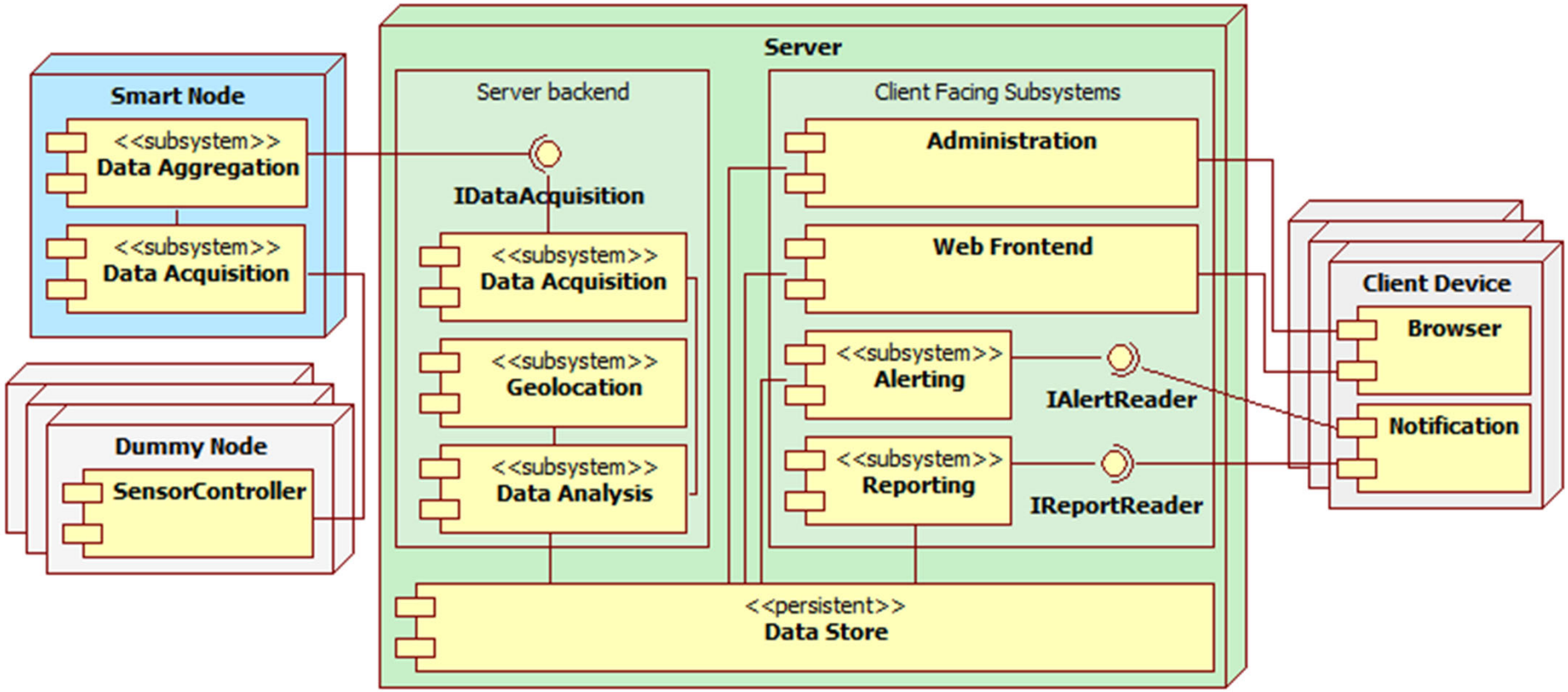
Outline

- Introduction
- Sensor networks
- **iLight**
- Fog computing
- IoT Security

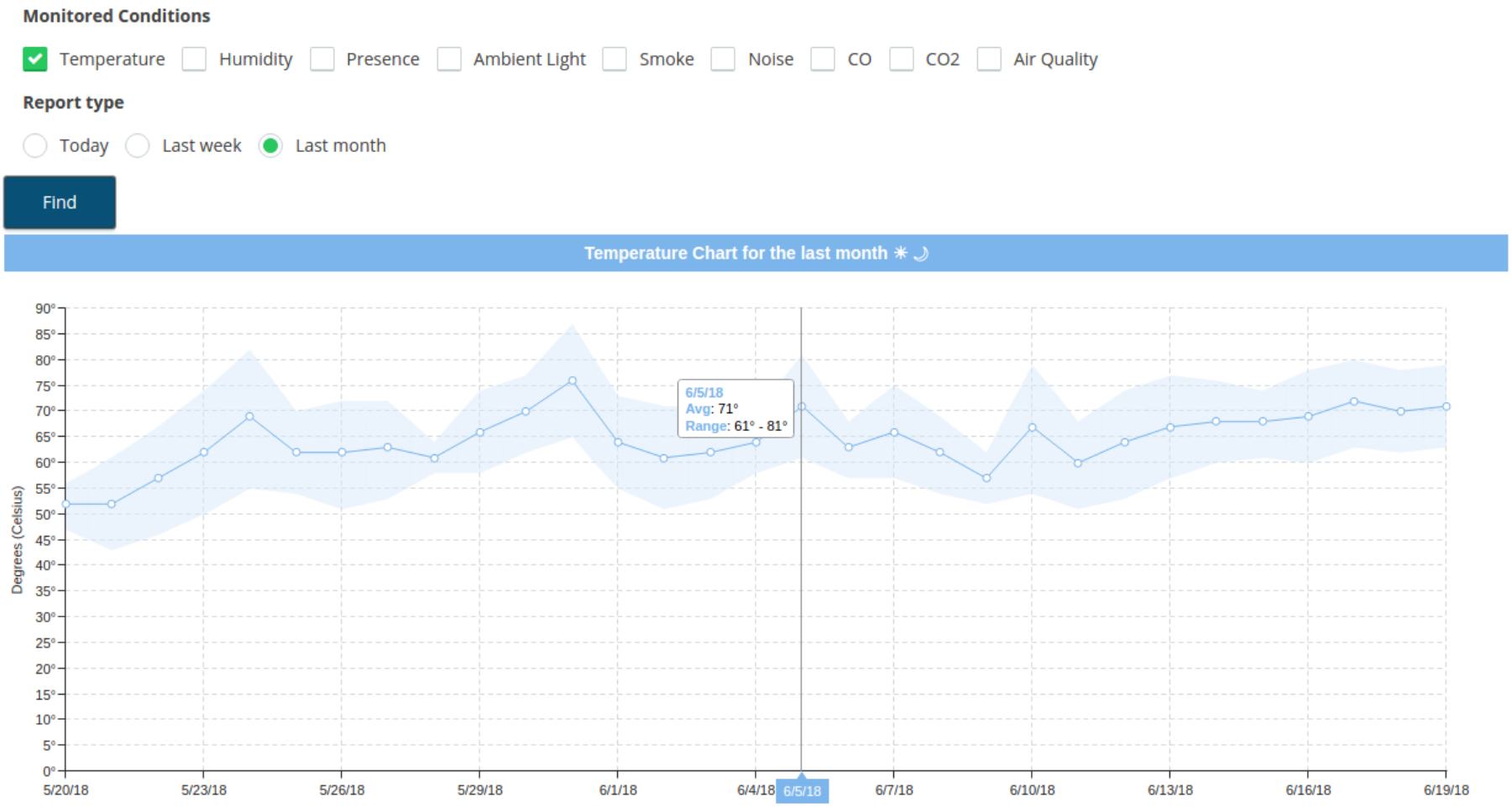
Example - iLight

- Ambient Assisted Living
- i-Light, a pervasive cyber-physical system targeted toward older adult supervision and home monitoring
- Features
  - Continuous supervision of the monitored person's whereabouts and activities through localization.
  - Constant monitoring of indoor ambient conditions in order to ensure the safety of monitored persons.
  - Real-time alerts and notifications provided to the monitored person and selected caregivers in case of emergency situations.
  - Interoperability with third-party medical devices for telehealth purposes.

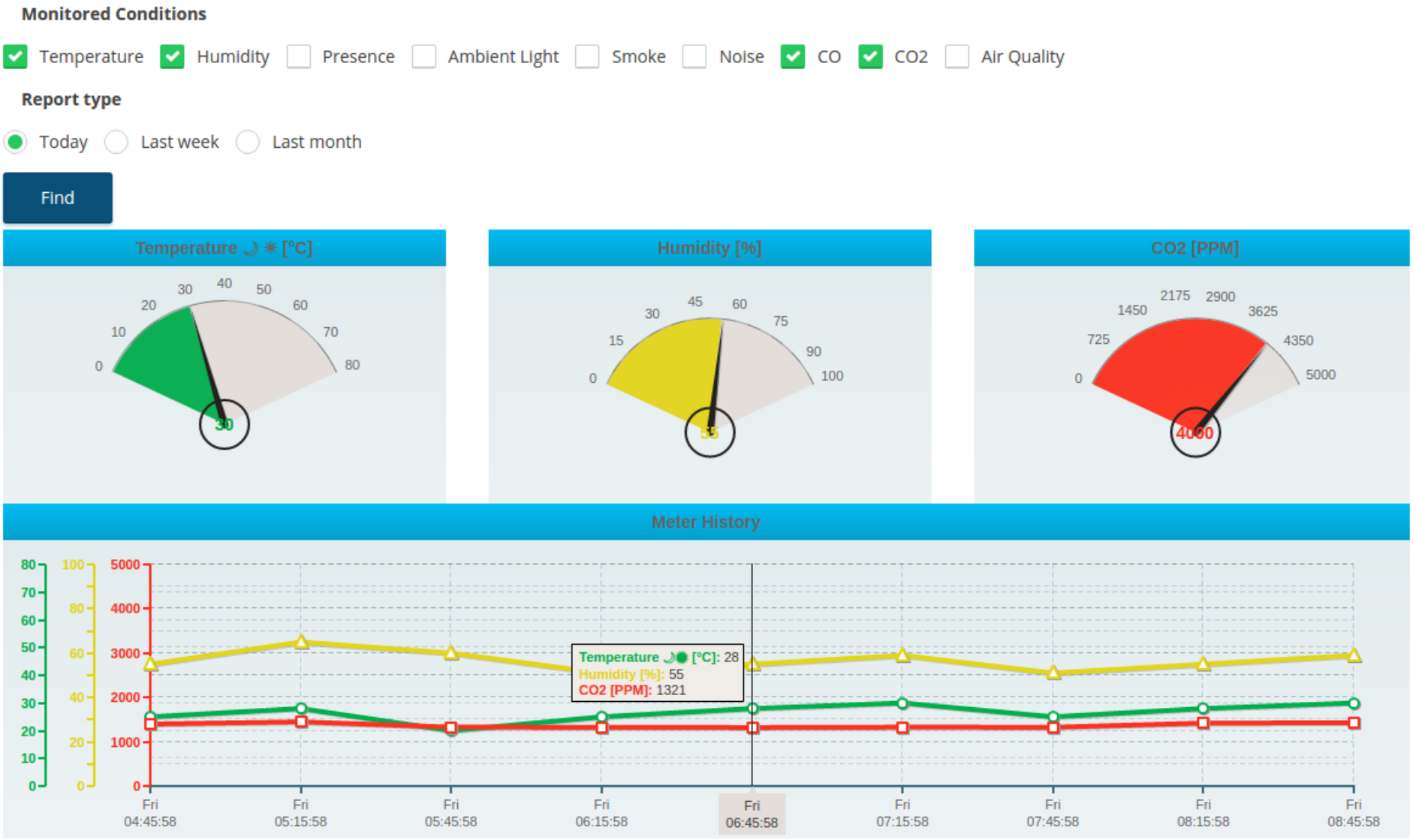
Software architecture



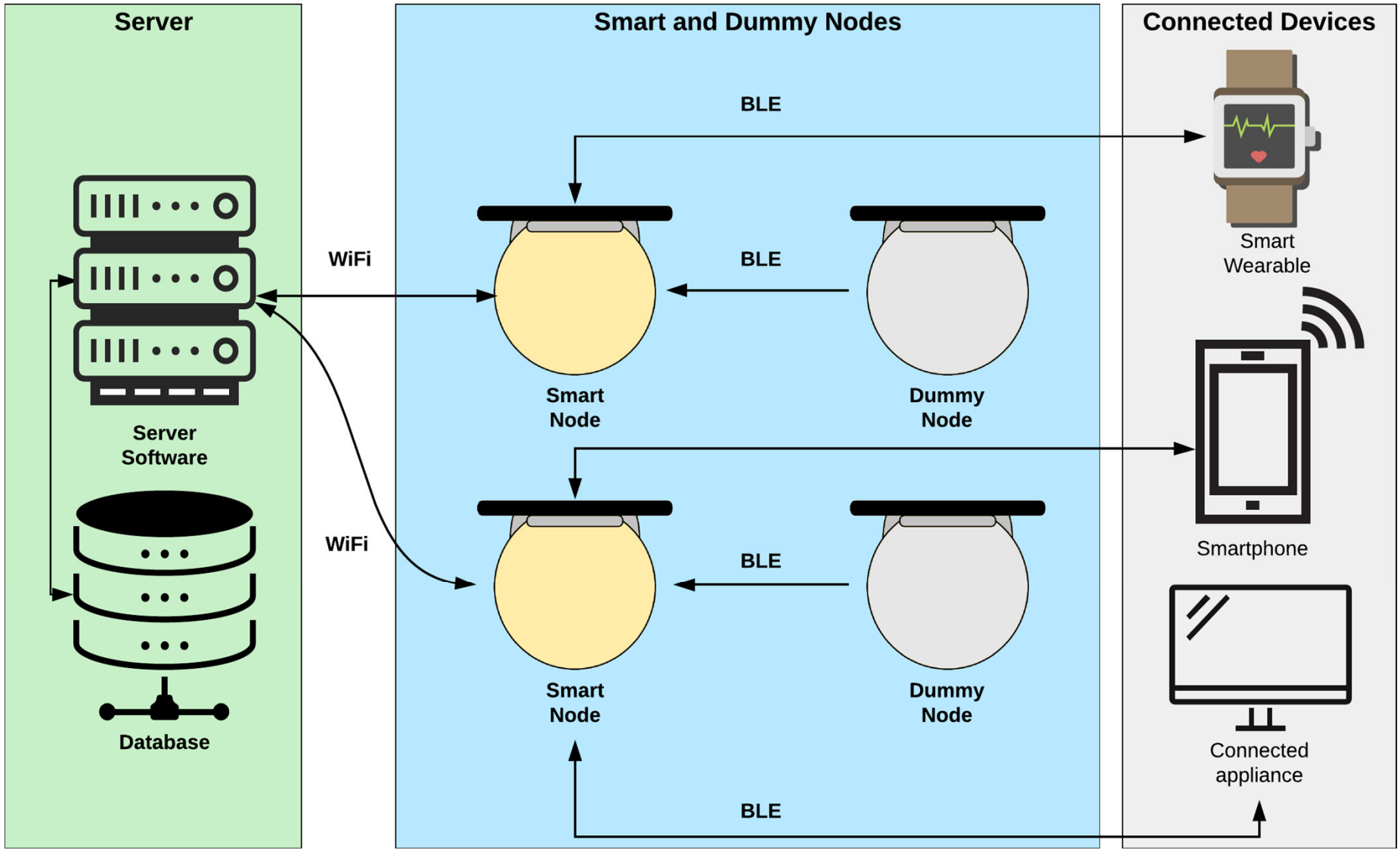
Reports


Monitored Conditions
Temperature
Humidity
Presence
Ambient Light
Smoke
Noise
CO
CO2
Air Quality
Report type
Today
Last week
Last month
Find
Temperature Chart for the last month
6/5/18
Avg: 71°
Range: 61° - 81°
Degrees (Celsius)
90°
85°
80°
75°
70°
65°
60°
55°
50°
45°
40°
35°
30°
25°
20°
15°
10°
5°
0°
5/20/18
5/23/18
5/26/18
5/29/18
6/1/18
6/4/18
6/5/18
6/7/18
6/10/18
6/13/18
6/16/18
6/19/18

Reports


Monitored Conditions
Temperature
Humidity
Presence
Ambient Light
Smoke
Noise
CO
CO2
Air Quality
Report type
Today
Last week
Last month
Find
Temperature [°C]
0
10
20
30
40
50
60
70
80
30
Humidity [%]
0
15
30
45
60
75
90
100
55
CO2 [PPM]
0
725
1450
2175
2900
3625
4350
5000
4000
Meter History
Temperature [°C]: 28
Humidity [%]: 55
CO2 [PPM]: 1321
Fri 04:45:58
Fri 05:15:58
Fri 05:45:58
Fri 06:15:58
Fri 06:45:58
Fri 07:15:58
Fri 07:45:58
Fri 08:15:58
Fri 08:45:58

High level Architecture



Outline

- Introduction
- Sensor networks
- iLight
- **Fog computing**
- IoT Security

Fog computing

- "a scenario where a huge number of heterogeneous (wireless and sometimes autonomous) ubiquitous and decentralized devices communicate and potentially cooperate among them and with the network to perform storage and processing tasks without the intervention of third parties.
- These tasks can be for supporting basic network functions or new services and applications that run in a sandboxed environment. Users leasing part of their devices to host these services get incentives for doing so."
- enable computing directly at the edge of the network
- Similar concepts: mobile cloud computing, mobile-edge computing

Beyond cloud computing

- Edge location, location awareness, and low latency.
- Geographical distribution.
- Large-scale sensor networks, smart grid
- Support for mobility
- Real-time interactions
- Heterogeneity
- Interoperability and federation

Use cases

- Augmented Reality (AR) and Real-time video analytics
  - smart city
- Content Delivery and Caching
  - customizable optimization based on client devices and local network conditions
  - save the bandwidth and reduce latency for content delivery
- Mobile Big Data Analytics
  - big data acquisition, aggregation and preprocessing
- Connected Vehicle
- Wireless Sensors and Actuators Networks

Fog computing issues

- Fog networking
  - need flexible and easy to maintain network environments
  - software-dened networking (SDN), network function virtualization (NFV)
  - SDN - each node should be able to act as a router for nearby nodes
  - NFV – network functions – virtual machine instances (gateways, switches, load balancers, firewalls)
- Quality of Service
  - Connectivity
  - Reliability
  - Capacity : network bandwidth, storage capacity
  - Delay

Outline

- Introduction
- Sensor networks
- iLight
- Fog computing
- **IoT Security**

IoT Security Challenges

- Multiple Technologies
  - radio, frequency identification (RFID), wireless sensor networks, cloud computing and virtualization
  - each with its own vulnerabilities
  - entire chain must be secured –weakest link
- Multiple Verticals
  - numerous applications (also called verticals) that span eHealth, industrial, smart home gadgets, smart cities
  - each have different security requirements
- Scalability
  - centralized defensive frameworks cannot be used
  - solutions must scale cost-effectively

Big Data

- need efficient defensive mechanisms that can secure large streams of data.

- Availability
  - network administrators often hesitate to use needed threat response technology functions for fear that such functions will take down critical systems
- Resource limitations
  - resource limited devices can be targeted by denial-of-service (DoS) attacks where the attacker can easily overwhelm the limited resource capabilities of those devices causing a service disruption.
  - mature cryptography techniques are known to be computationally expensive

Remote Locations

- sensors can be installed in unmanned locations that are difficult to reach
- attackers can interfere with these devices without being seen

Mobility

- Smart objects are expected to change their location often in the IoT paradigm

Delay-Sensitive Service

- majority of IoT applications are expected to be delay-sensitive and thus one should protect the different IoT components from any attack that may degrade their service time or may cause a service disruption.

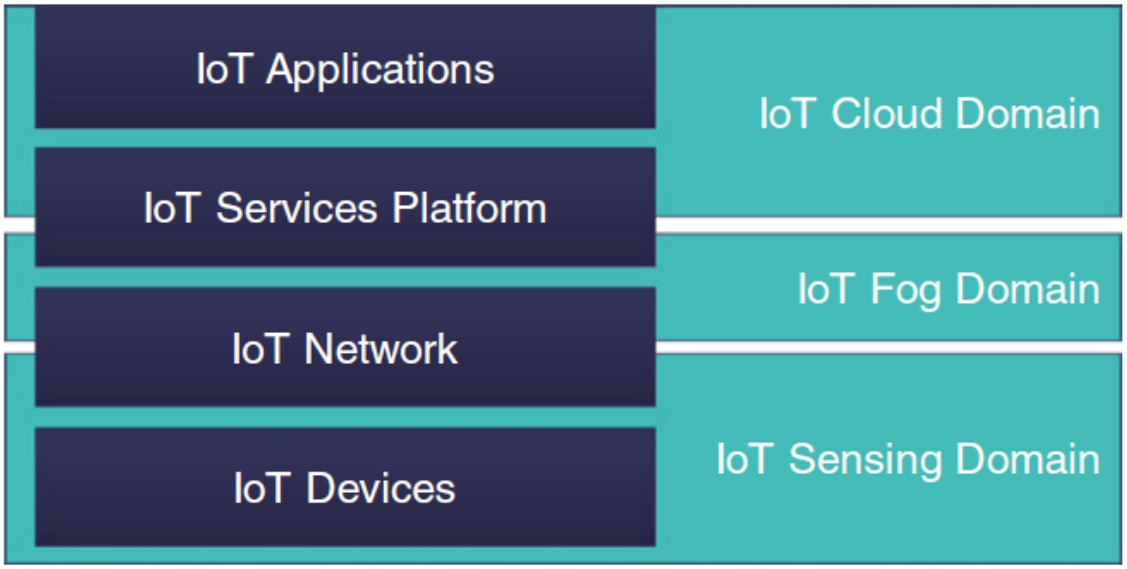
IoT Security Requirements

- Confidentiality
  - exchanged messages can be understood only by the intended entities
- Integrity
  - exchanged messages were not altered/tampered with by a third party
- Authentication
  - entities involved in any operation are indeed who they claim to be
- Availability
  - service is not interrupted
- Authorization
  - entities have the required control permissions to perform the operation they request to perform

IoT Security Requirements

- Freshness
  - data is fresh. Replay attacks target this requirement where an old message is replayed in order to return an entity into an old state.
- Non-repudiation
  - entity cannot deny an action that it has performed
- Forward Secrecy
  - when an object leaves the network, it will not understand the communications that are exchanged after its departure.
- Backward Secrecy
  - any new object that joins the network will not be able to understand the communications that were exchanged prior to joining the network

IoT Three-Domain Architecture



Dabbagh, M. and Rayes, A., 2019. Internet of things security and privacy

IoT Three-Domain Architecture

- IoT Sensing Domain
  - smart objects that have the capability to sense the surrounding environment and report the sensed data to one of the devices in the fog domain. The smart objects in the sensing domain are expected to change their location over time
- Fog Domain
  - fog devices that are located in areas that are highly populated by many smart objects
  - each fog device is allocated a set of smart objects where the allocated objects report their sensed data to the fog device.
  - operations on the collected data including aggregation, preprocessing, and storage.

IoT Three-Domain Architecture

- Fog Domain
  - connected with each other in order to manage the communication among the smart objects and in order to coordinate which fog device will be responsible for handling which object as objects change their location over time
  - connected to one or multiple servers in the cloud domain
- Cloud Domain
  - virtualized servers that host the IoT applications that are responsible for performing the heavy-computational processing operations on the data reported from the fog devices
  - IoT apps -> virtual machines. migration

Cloud Domain Attack

- Hidden-Channel Attacks
  - data leakage across the VMs that reside on the same server based on shared hardware components
  - Step1: Mapping Target VM: locate where target VM resides, can infer location from external IP address.
  - Step2: Malicious VM Placement: use traceroute to check if same server, continue renting until found.
  - Step3: Cross-VM Data Leakage: gain access to cache
- Prevention Hard Isolation
  - separate the cache dedicated for each VM through hardware or software
  - assign only one VM to each server.
  - white list

Cloud Domain Attacks

- Prevention Cache Flushing
  - flushes the shared cache every time the allocation of the cache is switched from a VM to another
- Prevention Noisy Data Access Time
  - adds random noise to the amount of time needed to fetch data, which makes it hard to tell whether or not the data was fetched from the cache or from the memory

Cloud Domain Attacks

- VM Migration Attacks
- Control Plane Attacks
  - target the migration module in the hypervisor.
  - Migration Flooding: moves VMs from hacked server to a victim server that does not have enough resource capacity. DOS.
  - False Resource Advertising:hacked server claims that it has a large resource slack, hacker can attack moved VMs

Cloud Domain Attacks

- Data Plane Attacks
  - target the network links over which the VM is moved from a server to another
  - Sniffing Attack: attacker sniffs the packets that are exchanged between the source and destination and reads the migrated memory pages.
  - Man-In-The-Middle Attack: incoming packets that are destined to the victim get routed to the new physical address where the attacker resides.

Cloud Domain Attacks

- Theft-of-Service Attack
  - a malicious VM misbehaves in a way that makes the hypervisor assigns to it more resources than the share it is supposed to obtain
- VM Escape Attack
  - If a VM escapes the hypervisor layer and reaches the server's hardware, then the malicious VM can gain root access to the whole server where it resides. This gives the VM full control on all the VMs hosted on the hacked server
- Insider Attacks
  - by administrators

Fog Domain Attacks

- Differences between fog devices and cloud servers
- Location
  - placed close to smart objects – quick response, location awareness
- Mobility
  - VMs on the fog domain migrate to follow the movement of the smart objects
- Lower Computing Capacity

Fog domain security threats

- Authentication and Trust Issues
  - fog devices are expected to be owned by multiple and less-known entities.
- Higher Migration Security Risks
  - migrations from a fog device into another are carried over the Internet.
  - encrypt the migrated VM and to authenticate the VM migration messages that are exchanged among the fog devices
- Higher vulnerability to DoS Attacks
  - due to lower computing capacity
- Container Usage
  - use containers rather than VMs. share OS resources

Sensing Domain Attacks

- Jamming Attack
  - Jamming the Receiver : targets the physical layer in the OSI stack of the receiver. a malicious user (jammer) emits a signal (jamming signal) that interferes with the legitimate signals that are received at the receiver side. interference degrades the quality of the received signal causing many errors.
  - Jamming the Sender: targets the data link layer at the OSI layer of the sending object where the jammer in this attack sends a jamming signal that prevents the neighboring objects from transmitting their packets

Jamming

- Constant Jamming
  - continuously transmits a random jamming signal all the time. Easy to be observed. Requires lots of energy.
- Deceptive Jamming
  - transmit legitimate packets that follow the structure of the MAC protocol rather than sending random bits.
- Reactive Jamming
  - transmits a jamming signal only after it senses that a legitimate signal is being transmitted in the medium
- Random Jamming

Jamming countermeasures

- Frequency Hopping
  - sender and receiver switch from a frequency to another in order to escape from any possible jamming signal.
- Spread Spectrum
  - uses a hopping sequence that converts the narrow band signal into a signal with a very wide band, which makes it harder for malicious users to detect or jam the resulting signal
- Directional Antennas
- Jamming Detection

Vampire Attacks

- a malicious user misbehaves in a way that makes devices consume extra amounts of power so that they run out of battery earlier thereby causing a service disruption
- Denial of Sleep
  - protocols to reduce the power consumption of smart objects by switching them into sleep mode whenever they are not needed.
  - attack which prevents objects from switching to sleep mode by simply sending control signals that change their duty cycles keeping them active for longer durations.
  - mitigate by encrypting control messages for duty-cycle schedule

Vampire Attacks

- Flooding Attack
  - attacker flood the neighboring nodes with dummy packets and request them to deliver those packets to the fog device
  - mitigate by limiting the rate of the packets that each object may generate
- Carrousel Attack
  - adversary specifies routing paths that include loops where the same packet gets routed back and forth among the other objects wasting their power
  - mitigate by checking path

Vampire Attacks

- Stretch Attack
  - attacker can select a next hop that does not have the shortest path to the fog device in order to increase the power consumption of the objects that will be responsible to deliver those packets.
  - mitigate by disabling source routing or checking paths

Sensing Domain Attacks

- Selective-Forwarding Attack
  - when the object can't send its generated packets directly to the fog device but must rely on other objects to deliver those packets. A malicious object in this attack does not forward a portion of the packets that it receives from the neighboring objects.
  - blackhole attack where the attacker drops the entire set of packets
  - mitigate by path redundancy – send to multiple objects.
  - mitigate – discover malicious objects

Sensing Domain Attacks

- Sinkhole Attack
  - malicious object claims that it has the shortest path to the fog device which attracts all neighboring objects

Bibliography

- P. Waher "Learning Internet of Things"
- R. Buyya "Internet of Things. Principles and Paradigms"
- i-Light—Intelligent Luminaire Based Platform for Home Monitoring and Assisted Living. *Electronics*, 2018.
- F. Bonomi, R. Milito, J. Zhu, and S. Addepalli. Fog computing and its role in the internet of things. ACM, 2012.
- Yi, Shanhe, Cheng Li, and Qun Li. "A survey of fog computing: concepts, applications and issues." 2015.
- Bonomi, Flavio, et al. "Fog computing and its role in the internet of things." 2012.
- Olson, Nasrine. "Internet of things-from hype to reality: the road to digitization." 2019.
- Shi, Weisong, et al. "Edge computing: Vision and challenges." 2016

Bibliography

- C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey", IEEE Communications Surveys and Tutorials, vol. 16, no. 1, pp. 414–454, 2014
- Dabbagh, M. and Rayes, A., 2019. Internet of things security and privacy. In Internet of Things from hype to reality (pp. 211-238). Springer, Cham.