CSC 4255 –
IoT System Design and Implementation

Network access protocols & IoT placement techniques

Georgios Bouloukakis

Winter 2024 - 2025

Outline

- Connecting Things
  - IoT protocol stack
- Communication & Criteria
- Network access protocols
  - Protocols Utilizing IEEE 802.15.4
  - IoT Access Technologies summary
- IoT Device Placement
  - IoT Placement Taxonomy
  - Static Placement approaches
  - Dynamic Placement approaches
- Conclusion

Connecting Things

- Part 1: Communications Criteria
  - characteristics and attributes to consider when connecting Things
- Part 2” IoT Access Technologies
  - technologies considered when connecting Things

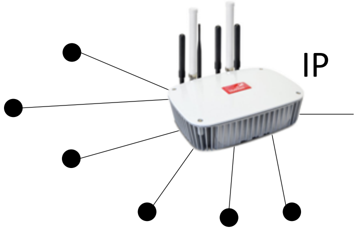
State of the Communication module

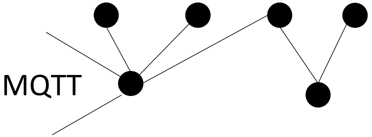
- Radio transceivers can be put in different operational states:
  - Transmit
  - Receive
  - Idle (ready to receive)
    - Parts of the communication module can be switched off saving energy
  - Sleep
    - Needs recovery time and startup time

IoT protocols at multiple layers

Application layer
Middleware/Session layer
Transport Layer
Network layer
Data Link layer (MAC & LLC)
Physical layer

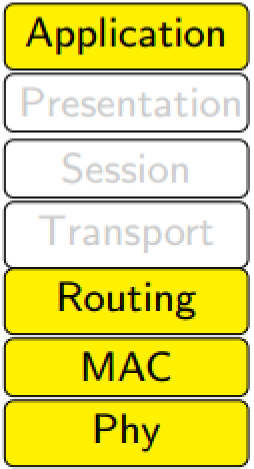
Application layer
Middleware/Session layer
Transport Layer
Network layer
Data Link layer (MAC & LLC)
Physical layer





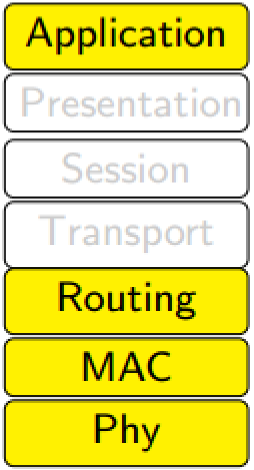
IoT communication protocols

➢ The behavior of a thing is specified by a set of communication protocols, or rules with which the node operate



IoT communication protocols: PHY

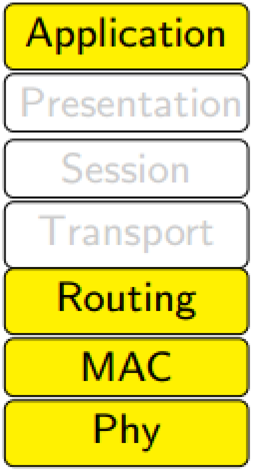
- The behavior of a thing is specified by a set of communication protocols, or rules with which the node operate



- How messages are successfully transmitted and received over the wireless channel?
- Goal: mathematically modelling the probability to successfully receive messages as function of the wireless channel characteristics and available design parameters (e.g., transmit radio power)

IoT communication protocols: MAC

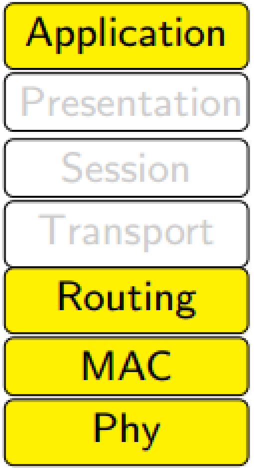
- The behavior of a thing is specified by a set of communication protocols, or rules with which the node operate

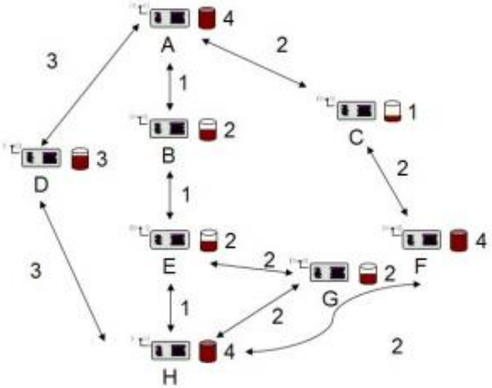


- When a node gets the right to transmit messages?
- What is the mechanism to get such a right?
- Goal: How to model mathematically such a behavior as function of the relevant design parameters (e.g., transmit radio power, time available)?

IoT communication protocols: Routing

➢ The behavior of a thing is specified by a set of communication protocols, or rules with which the node operate





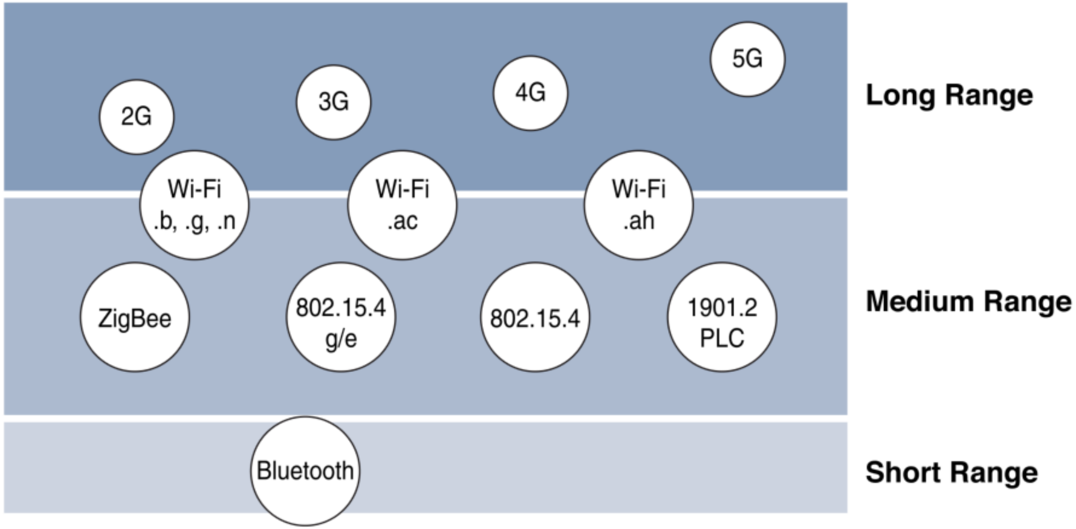
- How to chose a path along the IoT network
- Maximum total available battery capacity
  Path metric: Sum of battery levels □ Example: A-C-F
- Minimum battery cost routing
  Path metric: Sum of reciprocal battery levels □ Example: A-D-H
- Conditional max-min battery capacity routing
- Minimum total transmission power

Communications Criteria

- Wireless communication is prevalent in the world of smart object connectivity
- Wired or Wireless communication via Gateway Interfaces

Communications Criteria – Range

- How far does the signal need to be propagated?
- What will be the area of coverage for a selected wireless technology?
- Should indoor versus outdoor deployments be differentiated?



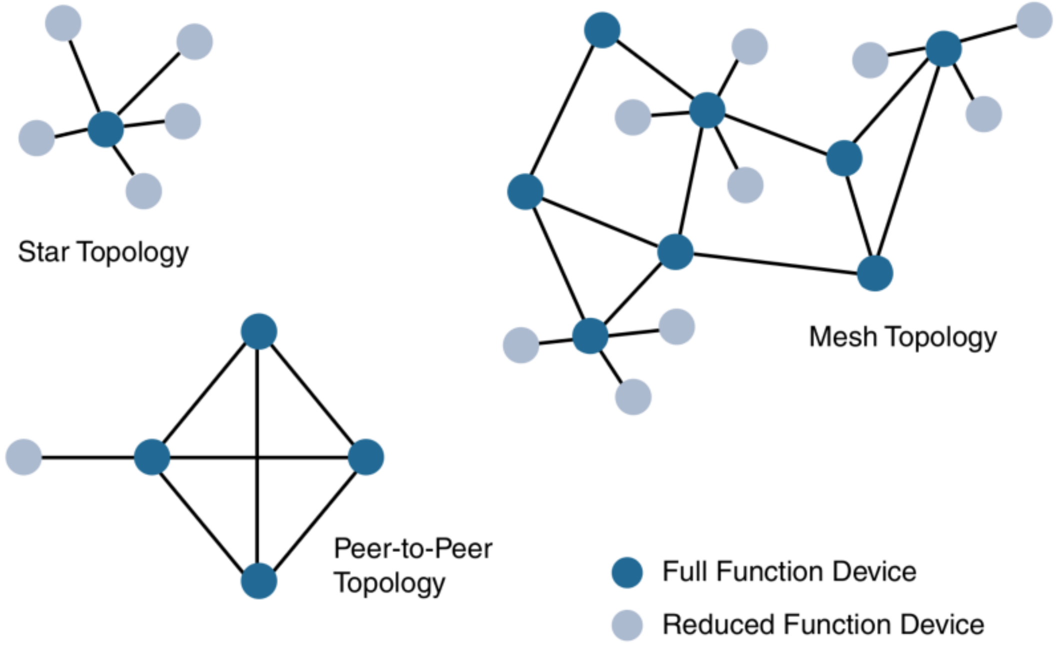
Communications Criteria – Frequency Bands

- Radio spectrum regulated by organizations such as the International Telecommunication Union (ITU), Federal Communications Commission (FCC), etc.
  - E.g., portions of the spectrum are allocated to types of telecommunications such as radio, television, military, etc.
- IoT access: licensed bands
  - Licensed spectrum is generally applicable to IoT long-range access
  - Complex deployments involving large number of Things
  - Exclusivity of the frequency usage, higher quality of service
  - Examples: cellular, WiMAX, and Narrowband IoT (NB-IoT), etc.
- IoT access: unlicensed bands
  - For industrial, scientific, and medical (ISM) portions of the radio bands
  - No guarantees or protections are offered in the ISM bands, simpler to deploy
  - Examples: 2.4 GHz by IEEE 802.11b/g/n Wi-Fi, IEEE 802.15.1 Bluetooth, etc.

Communications Criteria – Power Consumption

- Powered things vs. battery-powered things
- Powered things:
  - direct connection to a power source
  - communications not limited by power consumption
  - deployment limited by the availability of a power source
- Battery-powered things:
  - flexibility to IoT devices
  - classified by the required lifetimes of their batteries (water or gas meters, parking sensors)
  - IoT wireless access technologies must address the needs of low power consumption
- Low-Power Wide-Area (LPWA) -- evolution of a new wireless environment
  - possible to run any wireless technology on batteries

Communications Criteria – Topology (1)



Communications Criteria – Topology (2)

- 3 main topology schemes are dominant: star, mesh, and peer-to-peer
- Start topology:
  - long-range and short-range technologies
  - cellular, LPWA, and Bluetooth networks
  - utilize a single central base station for communications with things
- Peer-to-peer topologies:
  - allow any device to communicate with any other device if in range
  - rely on multiple full-function devices
  - enable more complex formations, such as a mesh networking topology
- Mesh topology:
  - helps cope with low transmit power
  - reach a greater overall distance, and coverage
  - requires a properly optimized implementation for battery-powered nodes

Communications Criteria – Constrained Devices

- Constrained things have limited resources
- Some classes of things do not implement an IP stack
- Classes of Constrained Nodes, as Defined by RFC 7228:
  - **Class 0**: severely constrained, < 10 KB mem, < 100 KB Flash, typically battery powered, no IP stack, no security mechanisms, unlicensed LPWA, e.g., sensors sends 1 byte
  - **Class 1**: ~ 10 KB mem, ~ 100 KB Flash, no complete IP stack implementation, implement an optimized stack (e.g., for CoAP), no need for gateway, support for security
  - **Class 2**: running full implementations of IP stack, > 50 KB mem, > 250 KB Flash

Communications Criteria – Constrained-Node Networks

- IoT access technologies suited to connect constrained nodes
  - E.g,: IEEE 802.15.4-g RF, IEEE 1901.2a PLC, LPWA, and IEEE 802.11ah
  - often referred to as low-power and lossy networks (LLNs)
- Data Rate and Throughput
  - range from 100 bps with protocols such as Sigfox to tens of megabits per second with technologies such as LTE and IEEE 802.11ac. (Sigfox, LTE, and IEEE 802.11ac
  - actual throughput is less—sometimes much less—than the data rate
  - bandwidth requirements, capacity planning rules, expected real throughput, etc.,: important for proper network design and successful production deployment
- Latency and Determinism
  - latency expectations of IoT applications should be known when selecting an access technology
  - May range from a few milliseconds to seconds

IoT Access Technologies

- For each IoT access technology:
  - Standardization and alliances: bodies that maintain the protocols
  - Physical layer: wired or wireless methods and relevant frequencies
  - MAC layer: bridges the physical layer with data link control
  - Topology: topologies supported by the technology
  - Security: security aspects of the technology
  - Competitive technologies: other technologies that are similar

Datalink-layer

IoT protocol stack

Session		MQTT, MQTT-SN, DDS, XMPP, CoAP, etc.
Network	Encapsulation	6LowPAN, 6TiSCH,6Lo, Thread, etc.
	Routing	RPL, CORPL, CARP, etc.
Datalink		WiFi, Bluetooth Low Energy, Z-Wave, ZigBee, DECT/ULE, 3G/LTE, NFC, Weightless, HomePlugGP, 802.11ah, 802.15.4e, WirelessHART, DASH7, ANT+, LTE-A, LoRaWAN, etc.

Security
TCG, Oath 2.0, SMACK, ISASecure, ace, DTLS, Dice, etc.

Management
IEEE 1905, IEEE 1451, etc.

- IoT Datalink protocols:
  - includes PHY and MAC layer protocols
  - PHY & MAC combined by most standards

IEEE 802.15.4 (1)

- Most commonly used IoT standard for MAC
- Defines frame format, headers, node communication, etc.
- IEEE 802.15.4e for low-cost and low-data-rate devices
- Easy installation using a compact protocol stack
- Applications: Home and building automation, Automotive networks, etc.
- Criticisms on MAC reliability, unbounded latency, and susceptibility to interference and multipath fading

Protocols Utilizing IEEE 802.15.4

- ZigBee:
  - ZigBee Alliance defines upper-layer components as well as application profiles
  - open global standard to address low-cost, low-power wireless IoT
  - unlicensed bands
- 6LoWPAN :
  - IPv6 adaptation layer by IETF 6LoWPAN
  - header compression and IPv6 enhancements
- ZigBee IP:
  - evolution of the ZigBee protocol stack
  - adopts the 6LoWPAN adaptation layer. IPv6 network layer, and RPL routing protocol
  - improvements to IP security
- WirelessHART :
  - offers a time-synchronized, self-organizing, and self-healing mesh architecture
  - IEEE 802.15.4-2006 over the 2.4 GHz frequency band

ZigBee

- Layer 4 and above (PHY and MAC by 802.15.4)
- Star, peer-to-peer, mesh topologies
- Device object functions: device role, device discovery, network join, and security
- Large range of IoT applications: building automation, home automation, and healthcare

Bluetooth Low Energy (BLE)

- For low data-rate, better power saving, massive number of IoT devices
- BLE’s consumption nearly half of classic Bluetooth device
- Topology: star, mesh, peer-to-peer, peer-to-multipeer
- Range up to 400m
- Large of IoT applications: Healthcare, Activity trackers, audio HS, etc.

Z-Wave

- A master node manages a Zwave network of nodes
- Logical Zwave network has 1 Home ID and multiple (up to 232) nodes
- Node of one network cannot communicate with nodes of other networks
- Devices not in range can communicate via different nodes (healing)
- Topology: peer-to-peer
- Typically for home automation, wearable healthcare

Wireless HART

- HART – Highway Addressable Remote Transducer – to support large number of IoT devices (analog and digital sensors)
- Wireless HART → wireless version of HART; easier to implement; common app-layer; wired HART lacks Network-layer
- Wireless HART:
  - Based on 802.15.4
  - Mesh topology, network graph to handle routing
  - Network manager as supervisor

LoRA

- LoRa and LoRaWAN are different: LoRaWAN protocol for WAN; LoRa technology for WAN → non-cellular modulation tech
- Very small message capacity
- Usually requires its own network gateway

NB-IoT

- For very low data-rate devices to mobile battery-powered networks
- Cellular standard for IoT devices; non IP-based protocol
- Send/receive small amounts of data
- Message-based communication; handle a lot more data than other low power protocols

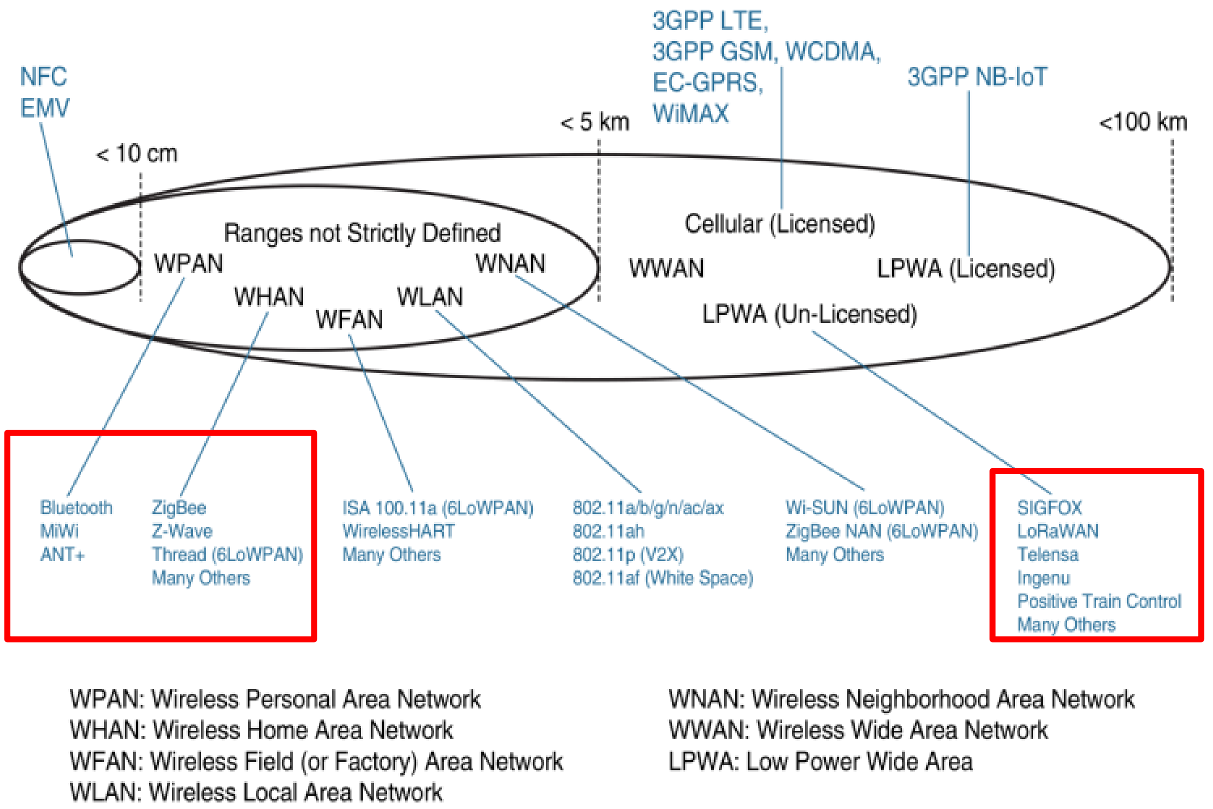
SigFox

- Proprietary low-power WAN network; uplink only
- Works well for low-power devices transmitting infrequently
- Wide coverage
- Poor link budget for downlink
- Supporting mobile is a problem

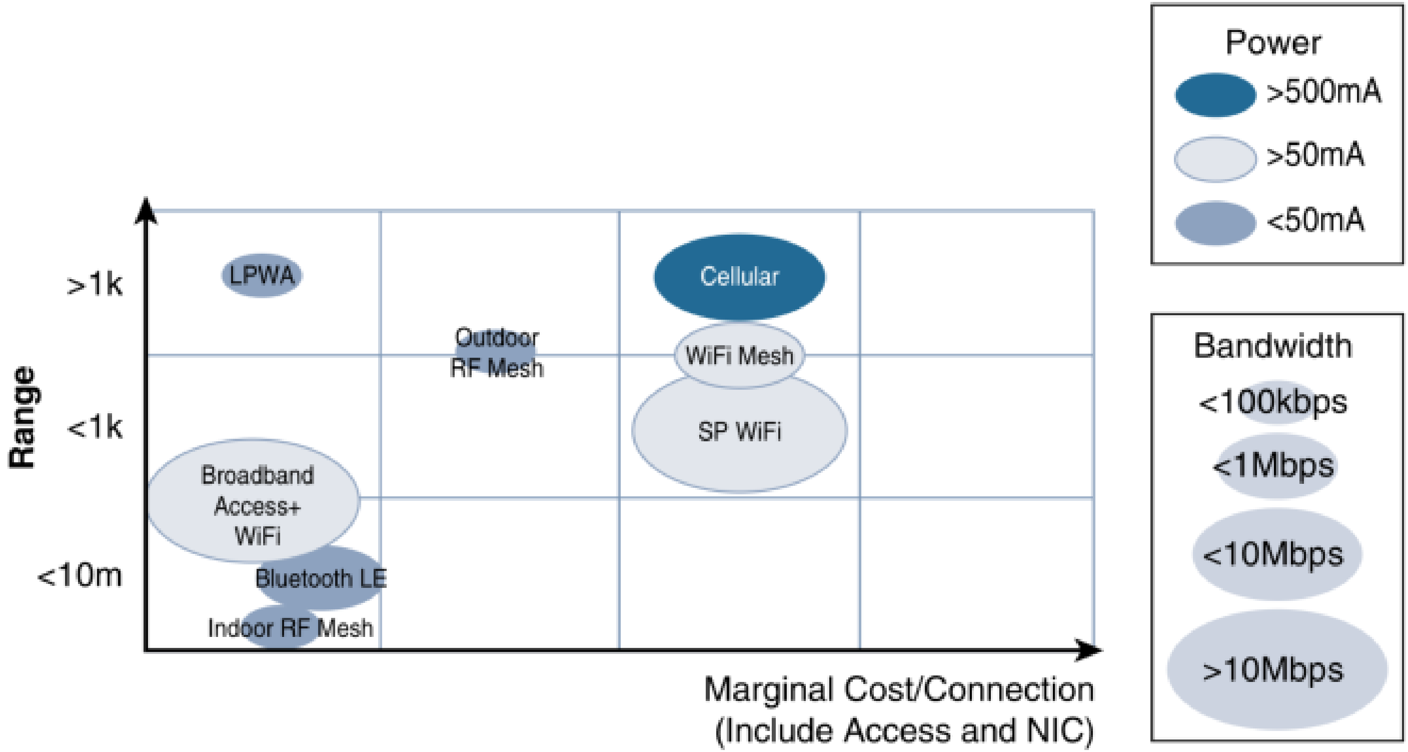
IoT Access Technologies summary

Technology	Frequency	Data Rate	Range	Power Usage	Cost
2G / 3G	Cellular Band	384 Kbps / 10 Mbps	Several Km	High	High
BLE	2.4 GHz	1,2,3 Mbps	1, 10, 100 m	Low	Low
802.15.4	Sub GHz, 2.4 GHz	40, 250 Kbps	1—75 m	Low	Low
LoRa	Sub GHz	< 50 Kbps	1.5 – 4.5 Km	Low	Medium
NB-IoT	Cellular Band	0.1 – 1 Mbps	Several Km	Medium	High
SigFox	Sub GHz	< 1 Kbps	Several Km	Low	Medium
WiFi	Sub GHz, 2.4 GHz, 5 GHz	0.1 – 54 Mbps	< 100 m	Medium	Low
WirelessHART	2.4 GHz	250 Kbps	~ 100 m	Medium	Medium
Zigbee	2.4 GHz	250 Kbps	~ 100 m	Low	Medium
Z-Wave	Sub GHz	40 Kbps	~ 30 m	Low	Medium
5G	30 GHz	10 Gbps	400 m	High	Hogh

Network access protocols - summary



Network access protocols - summary



Exercise: Choosing the Right Protocol

- **Objective:** Recommend the best network access protocol for different IoT use cases.

Instructions:

1. In pairs or small groups, review the scenarios below.
2. For each scenario, choose the most suitable protocol (WiFi, Zigbee, Bluetooth, LoRaWAN, Cellular) based on:
   I. Range
   II. Power Consumption
   III. Data Rate

- **Scenarios:**

1. *Smart Home Lighting: Remote-controlled light bulbs.*
2. *Farm Sensors: Soil moisture sensors across a large field.*
3. *Fitness Tracker*: Wristband syncing data to a phone.
4. *City Parking Sensors*: Notify drivers of available spots.

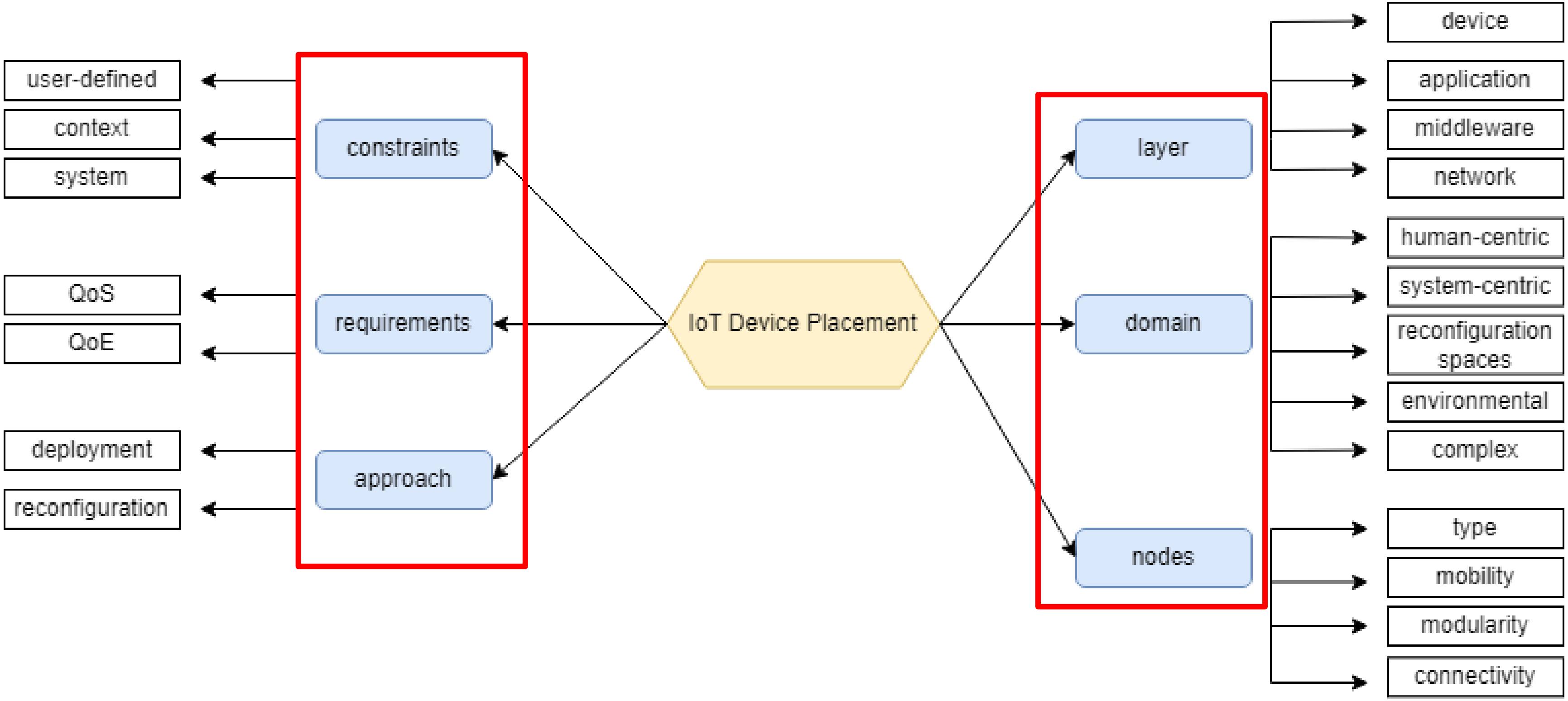
Time: 10 minutes

Tip: Focus on the *input (sensor)*, *output (actuator)*, and *intelligence (smart object)* of the system.

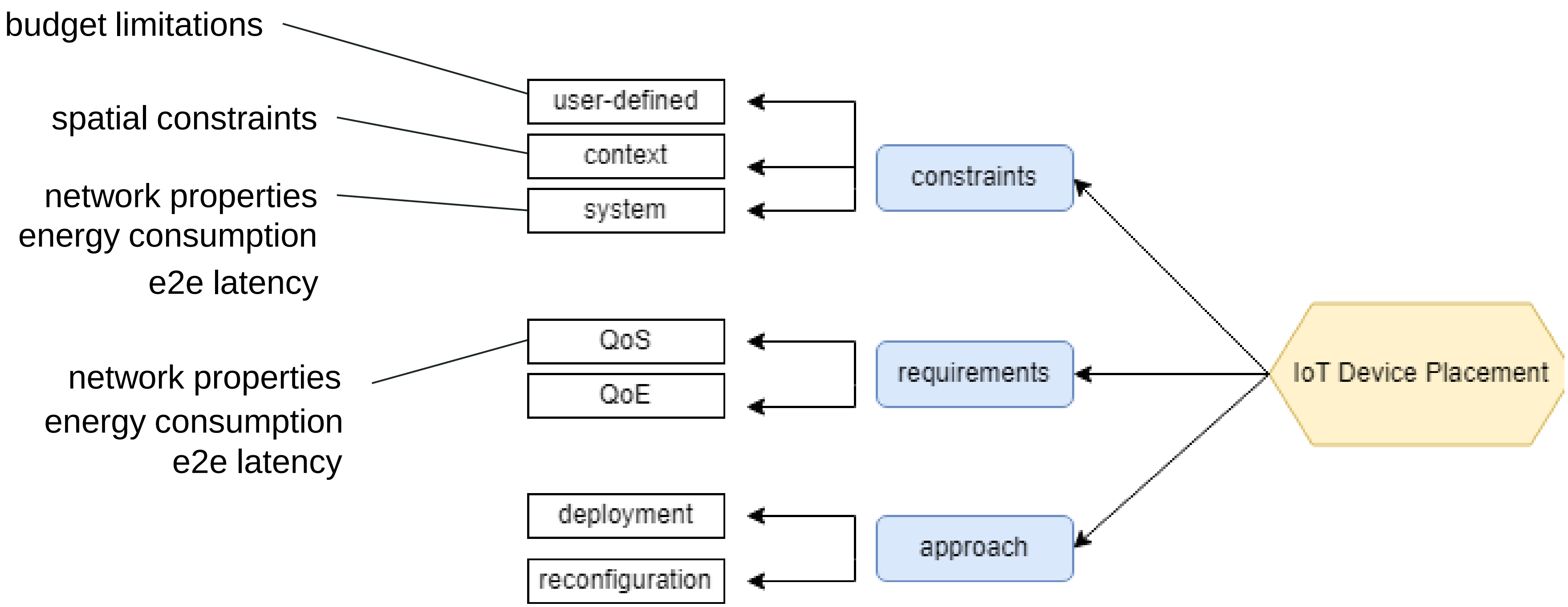
IoT Device Placement

- Placement of IoT devices (sensors and actuators) requires to take into account:
  - IoT device properties: input/output rate, range & direction, latency, sensitivity, and more
  - IoT Access protocol properties: frequency, data rate, range, power usage, cost, and more
  - Application domain (industry, healthcare, agriculture, etc.)
  - Available budget
  - Geospatial characteristics (buildings, open space, etc.)

IoT Placement Taxonomy



IoT Placement Taxonomy – Constraints and reqs.

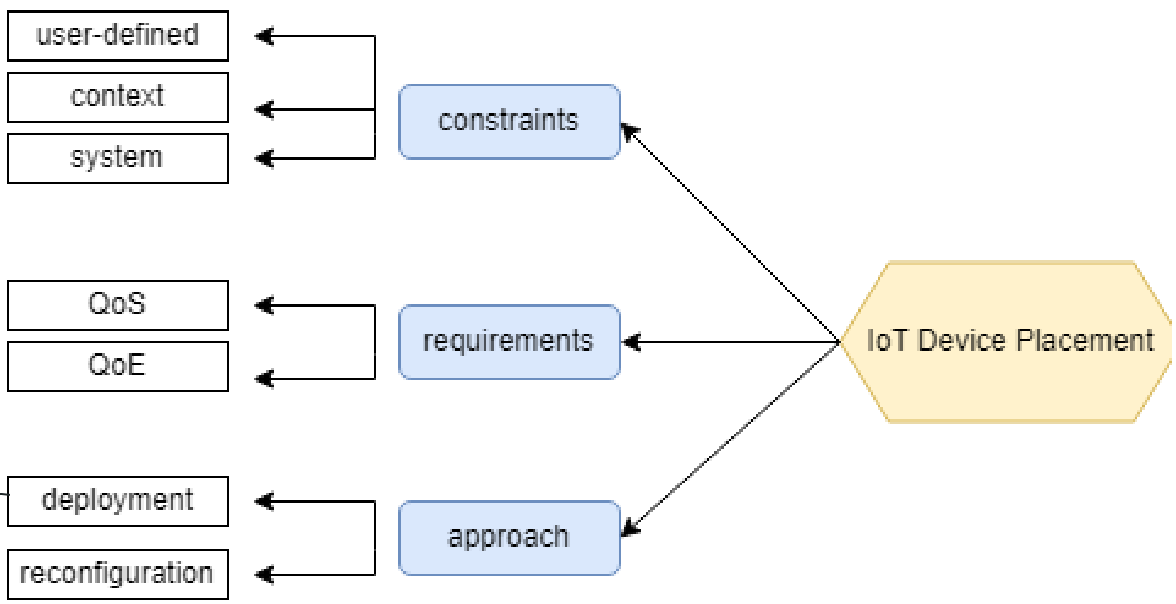


IoT Placement Taxonomy – Algs. placement

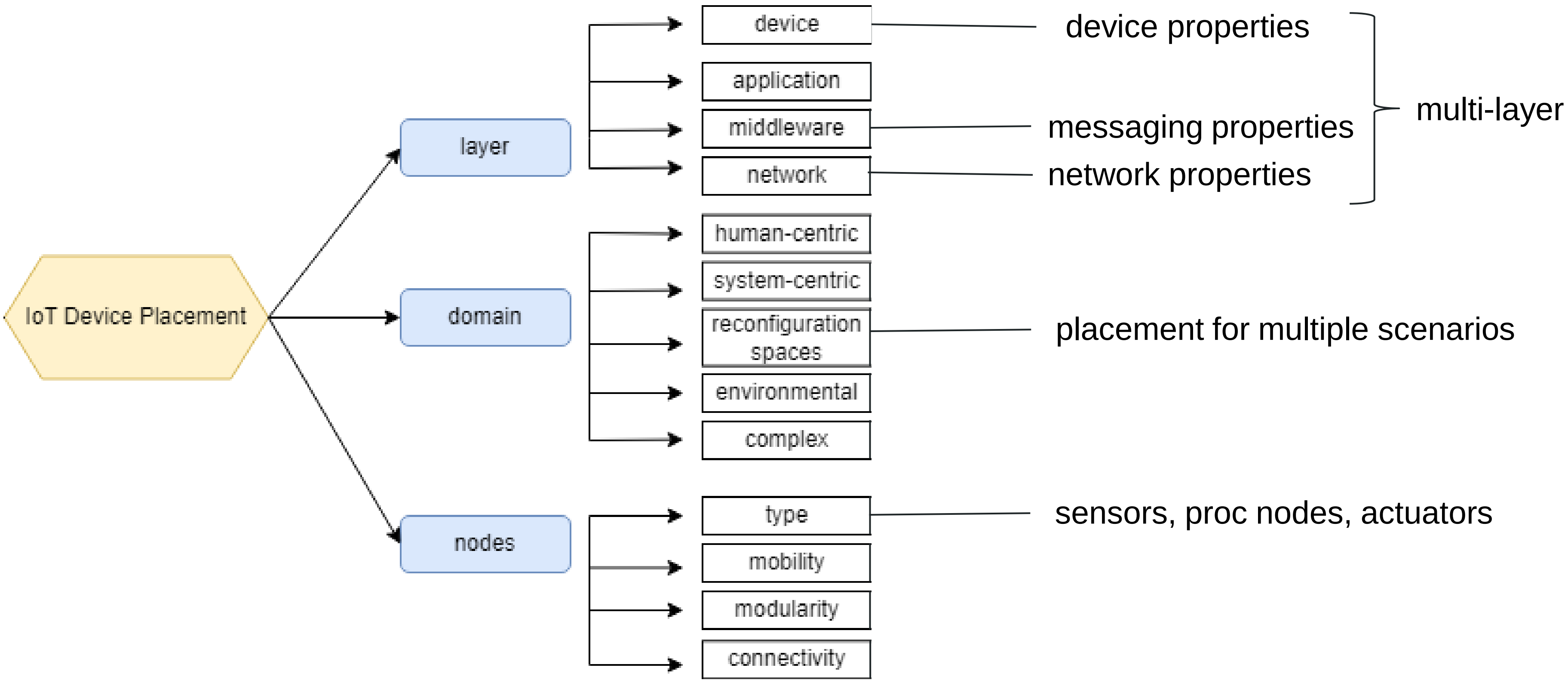
population based algorithm

greedy algorithm

trajectory based



IoT Placement Taxonomy – placement properties

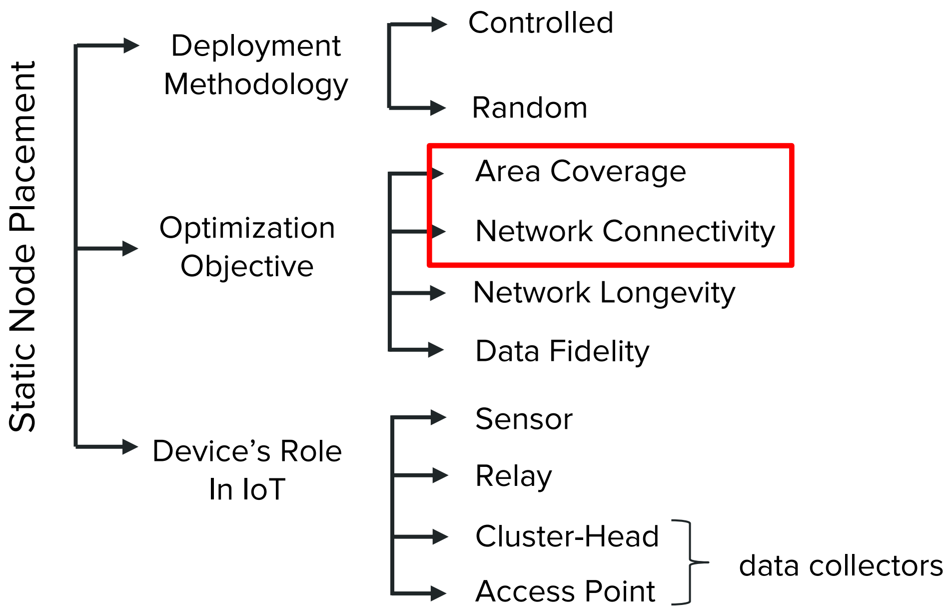


IoT device placement in IoT wireless networks

- Optimal sensor placement has proven to be NP-hard
- Placement categories:
  - Static: optimization is performed at the time of deployment
  - Dynamic: optimization is performed while the IoT network is operational
- Design schemes for placement at various layers:
  - Network-layer: multi-hop route setup, network data aggregation, hierarchical network topology, etc.
  - MAC-layer: collision avoidance, minimizing idle listeners, power control, etc.
  - App-layer: adaptive nodes activation, load balancing, query optimization, etc.

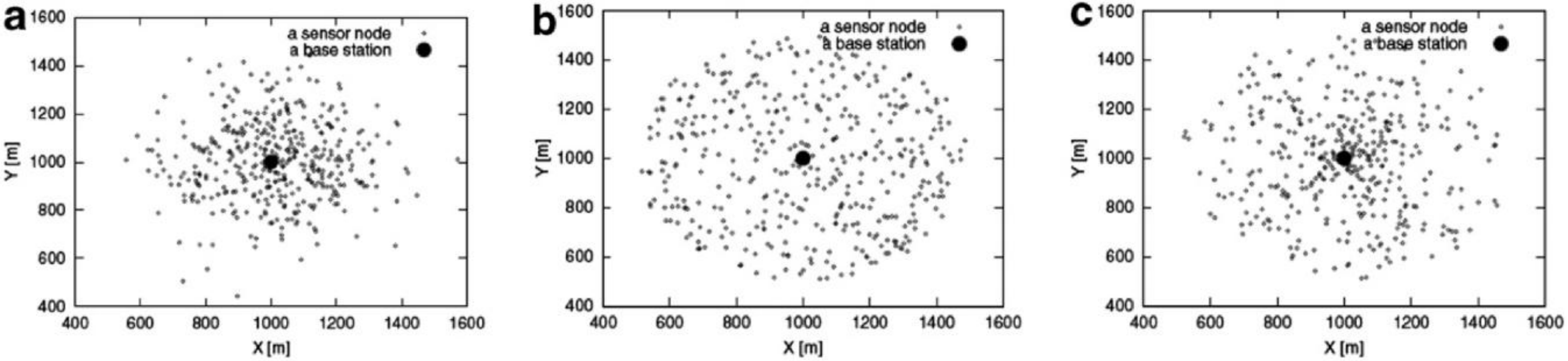
Static Placement approaches

- Prior to network startup
- Metrics independent of network state:
  - Area coverage
  - Inter-device distance
- Classification based on:



Static Placement: deployment methodology

- Controlled deployment: indoor applications of IoT, 2-D/3-D space setups
- Random deployment (R-random): often the only option, useful during emergency response scenarios, better placement strategy for fault-tolerance

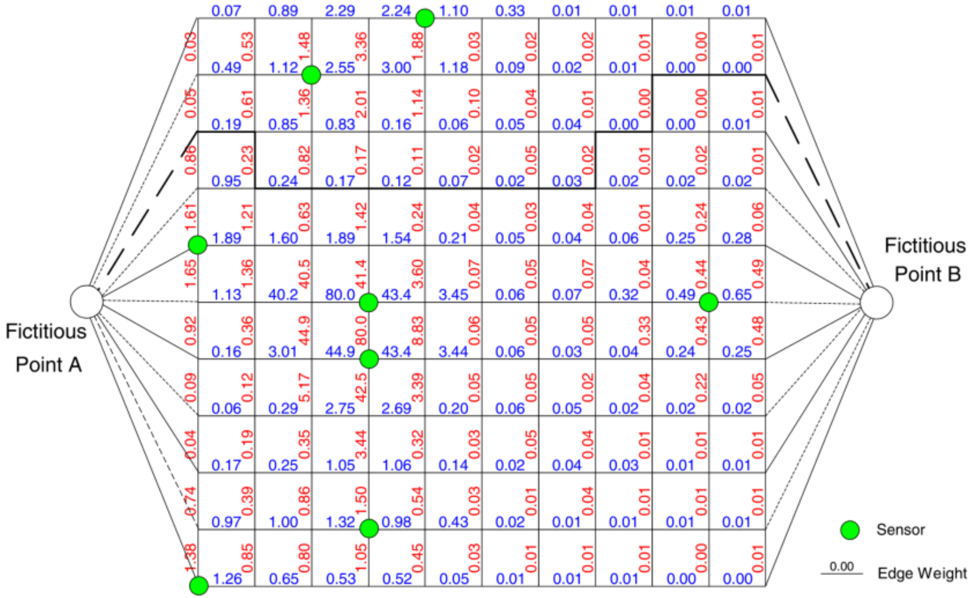


Static Placement: optimization objectives (1)

- Desired goals: increasing coverage, strong network connectivity, extending network lifetime, boosting the data fidelity
- Using: least amount of resources
- **Maximizing area coverage** in an area of interest:

Grid structure:

- Random deployment is assumed
- Least exposure path is identified (Dijkstra's algorithm), probability of detection is calculated
- If probability < threshold, more IoT devices
- Procedure repeated until required coverage is reached

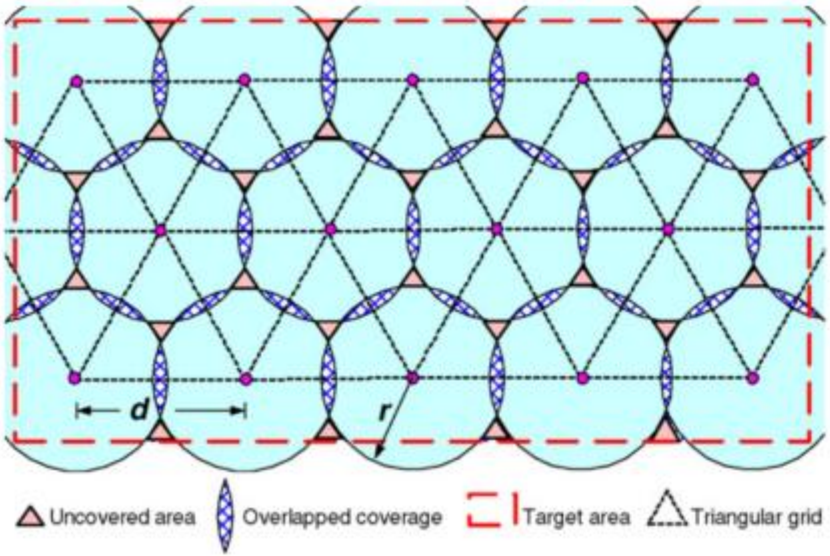


Static Placement: optimization objectives (2)

- Desired goals: increasing coverage, strong network connectivity, extending network lifetime, boosting the data fidelity
- Using: least amount of resources
- **Maximizing area coverage** in an area of interest:

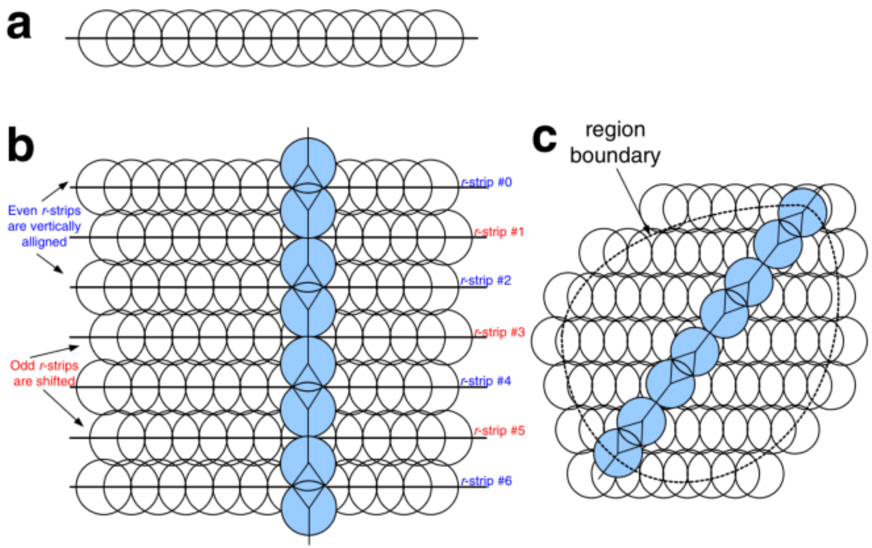
Triangular grid:

- Coverage can be controlled by adjusting the inter-node distance “d”
- 100% coverage is possible if d = $\sqrt{3r}$ where r is the sensing range
- Communication range >> r → connectivity not an issue



Static Placement: optimization objectives (3)

- **Maximizing connectivity**
- If communication range is limited, connectivity becomes an issue
- Connectivity issue can be tackled by using relay devices
- Sensor place for complete coverage and connectivity



r-strip:

- Devices on an r-strip are connected
- The r-strips are aligned for even values of the integer k
- Shifted horizontally r/2 for odd values of k
- **Goal**: fill gaps in coverage with the least overlap among the r-disks that define the boundary of the sensing range
- Shaded disks for connectivity

Dynamic Placement

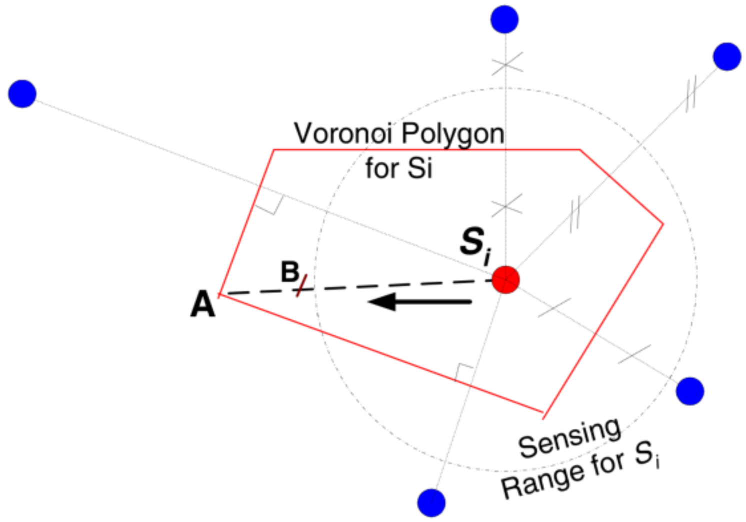
- Traffic patterns can change based on the monitored events
- Load may not be balanced among the IoT devices
- Application-level interest can vary over time
- Available network resources may change as new devices join the network, or as older devices run out of energy
- **Dynamically repositioning devices at runtime (network is operational) is essential to further improve the performance of the network**
- Relocating devices during regular network operation is very challenging. It requires:
  - continual monitoring of the network state
  - analysis of events happening in the vicinity of the device
  - careful handling since it can potentially cause disruption in data delivery
- Schemes for dynamic device positioning can be categorized:
  1. Post-deployment IoT device relocation
  2. On-demand repositioning of IoT devices

Dynamic Placement -- Post-deployment

- At the conclusion of the device deployment phase
- Relocation process should be lightweight and in reasonable time

Voronoi polygon:

- to assess the coverage
- Every IoT device Si forms a Voronoi polygon with respect to the position of its neighboring devices
- The part of the polygon that lies outside the sensing range is not covered by Si
- If there are uncovered areas within the polygon, the sensor should move to cover them
- 3 methods: vector-based (VEC), Voronoi-based (VOR) and Minimax



Conclusion

- Things have communication properties
- Things rely on Network access technologies for operation
- Datalink protocols combine both PHY and MAC protocols and standards
- ZigBee, BLE, WiFi, WirelessHART, Z-Wave, and more, are short-range protocols
- LoRa, NB-IoT, SigFox and more, are long-range protocols
- Network access protocol and sensor characteristics play a crucial role in device placement
- We analyze both static and dynamic approaches for IoT device placement in IoT wireless networks

References

- Main reference for IoT access technologies:

  Al-Fuqaha, Ala, et al. "Internet of things: A survey on enabling technologies, protocols, and applications." IEEE communications surveys & tutorials 17.4 (2015): 2347-2376.

- Main reference for IoT device placement:

  Younis, Mohamed, and Kemal Akkaya. "Strategies and techniques for node placement in wireless sensor networks: A survey." Ad Hoc Networks 6.4 (2008): 621-655.

Thank you

https://gbouloukakis.com/courses/csc4255-w25/