Question1: How is the deployment of multiple sensors going to affect the IoT platform?

The platform is equipped with m3 boards which have four types of sensors.

- Ambient sensor light - ISL29020
- Atmospheric pressure and temperature - LPS331AP
- Tri-axis accelerometer / magnetometer - L3G4200D
- Tri-axis gyrometer - LSM303DLHC

These sensors measure environmental variables such as pressure, temperature, light. Since the Saclay site has the layout described in the next figure, it can be deduced that the variables measured by the sensors on different devices should not vary too much each from the others.

Any variations that may occur could be due either to aerators, chillers, air conditioners, radiators, local overheating, or measurement errors. In some cases the sensors can also measure erroneously, or not be calibrated and therefore lead to even large measurement variations. The types of errors coming from sensors are many and they are not the only ones. In other cases there may be network communication errors, leading to missing readings. For example, it can happen that a board disconnects, or rhymes, and consequently the sensors on it will not take readings. or it may happen that the sensors themselves break, or have become obsolete. In all these cases the solution can be the redundancy of the equipment or

temporal redundancy. That is, double the readings or devices.

It was decided to create a mesh network of m3 nodes connected to each other with IEEE 802.15.4 standard, used by the Zigbee communication protocol. Each node uses Public IPv6 (6LoWPAN / RPL) network with M3 nodes in IOT Lab.

Differences between a Wireless Sensor Network (WSN) and Internet of Things

The Internet of Things, commonly abbreviated as IoT, refers to the connection of devices to the Internet.

INTERNET of Things (IoT) is a network of connected objects, each with low storage, limited energy, and processing capabilities. These objects interact in a complex way to enhance reliability, performance, and security of their infrastructure.

In an IoT system, all of the sensors directly send their information to the Internet. For example, a sensor may be used to monitor the temperature of a body of water. In this case, the data will be immediately or periodically sent directly to the

internet, where a server can process the data and it can be interpreted on a front-end interface.

Conversely, in a WSN, there is no direct connection to the Internet. Instead, the various sensors connect to some kind of router or central node. Then route the data from the router or central node to Internet. That being said, an IoT system can utilize a wireless sensor network by communicating with its router to gather data.

You can think of a wireless sensor network (WSN) as more of a group of sensors or "a big sensor" and less like a "competitor" or "rival" to the Internet-of-Things.

In this sense WSN is as a Subset of IoT.
IoT exists at a higher level then WSN. In other words, WSN is often a technology used within an IoT system.
It is important to note that a large collection of sensors, as in a mesh network, can be used to individually gather data and send data through a router to the internet in an IoT system.
It's also important to note that the term "wireless sensor network" is not nearly as encompassing as "the internet of things." WSN consists of a network of only wireless sensors. If the network was to include a wired sensor, it could no longer be labeled

a "wireless sensor network." This is unlike IoT. Essentially any device that connects to the Internet can be considered an IoT device. An "IoT system" can therefore be interpreted as a group of many IoT devices.

We conclude that it is true the following definition of WSN.

Wireless Sensor Network - A collection of wireless sensors that may or may not be connected to the internet.

Experiments to be created in the IOT Lab Testbed

It is going to be created an experiment in IOT Lab testbed with a minimum of 3 nodes to a maximum of 12 nodes, plus an A8 node. One of the M3 nodes will act as a gateway or border router (BR). The other nodes will be simply wireless sensor nodes running an application firmware reading on board sensors .
This will be an M3 simple mesh network with a BR nodes interconnecting the other nodes to the Internet.
The commands to build this M3 network will be reported in the walk-through-guide

IOT-Second-Assignment-2021/Walk-through-guide.pdf at main · robertobruzzese/IOT-Second-Assignment-2021 (github.com)

The global prefix in this mesh network will be successfully propagated by the Border Router , an M3 node.

The border router will route packets between a 6Lo network (PAN) and a 'normal' IPv6 network (i.e. the Internet).

This requires the border router to have two interfaces: A downstream interface to run 6LoWPAN on and an IPv6 uplink.

The IPv6 traffic of the Border Router (BR) to ethernet is then encapsulated on the BR's serial link and routed via a virtual network interface (tap).

To connect to the serial link of the border router and propagate an IPv6 prefix through your network, RIOT provides the ethos_uhcpd tool. It uses the serial interface, ethos (Ethernet Over Serial) and UHCP (micro Host Configuration Protocol). Ethos multiplexes serial data to separate ethernet packets from shell commands. UHCP is in charge of configuring the wireless interface prefix and routes on the Border Router.

We can then interact with the M3 nodes using nc.

6LoWPAN is an acronym of *IPv6 over Low -Power Wireless Personal Area Networks*.[1] 6LoWPAN is the name of a concluded working group in the Internet area of the IETF.[2]

The 6LoWPAN concept originated from the idea that "the Internet Protocol could and should be applied even to the smallest devices,"[3] and that low-power devices with limited processing capabilities should be able to participate in the Internet of Things.[4]

The 6LoWPAN group has defined encapsulation and header compression mechanisms that allow IPv6 packets to be sent and received over IEEE 802.15.4 based networks

After carrying out the propagation of the ipv6 addresses, each node will be reachable on the internet with its global ipv6 address.

Consider the benefits of deploying multiple sensors with overlapping observation areas in terms of data quality, fault tolerance, and energy efficiency.

The benefits from the point of view of data quality, fault tolerance, and energy efficiency of having multiple sensors that have overlapping observation areas will be evaluated from a general and theoretical point of view.

Data Quality

The sensors are the main source of data. *Errors* in sensing measurements can be handled by procedures that are established based on a deep understanding of the characteristics of the sensors. *Missing readings*

may be handled by oversampling, and glitches, like *outliers and noise*, can be masked by averaging.

System dependability

The accuracy of data means its quality. The concept of dependability of a system is strictly related to the data quality.

Dependability can be defined as the ability of a system to avoid service failures that are more frequent or more severe than is acceptable.

The problem becomes critical when dependability is an important application requirement. For instance, in water-related information systems, inaccurate information in aquatic monitoring may lead to false warnings being issued or harmful situations not being detected early enough (e.g., floods or pollution events). As another example, WSNs are deployed in data centers for flexible temperature monitoring and energy-efficient control of air-cooling equipment. Therefore, ensuring the accuracy of collected data is also necessary for effectiveness reasons. In these examples, the operational conditions are typically hard to accurately predict, ensuring that the reliability of operations is often hard or costly, and the consequences of inaccurate sensor data collection can be detrimental.

The root cause of dependability problems concerning the quality of sensor data, that is the several kinds of faults that may affect the system operation, in particular at the sensor and network levels, describing the specific effect on the sensor data and the relevant failure modes-

It is important to know that fault-tolerance strategies based on sensor data fusion procedures, exploiting the availability of redundant measurements or available modeling surrogates, do exist. The collected data should be continuously validated , since sensors require maintenance.

Faults at the sensor level

As far as concerns individual sensor measurements, the possible types of errors observed in measurement values can be classified as follows:

1.Random errors are described by an absence of repeatability in the readings of the sensor, for instance due to measurement noise. These errors tend to happen on a permanent basis, but have a stochastic nature;

2.Systematic errors are described through consistency and repeatability in the temporal domain. There are three types of systematic errors at the sensor level: –

3.Calibration errors result from errors in the calibration [iii]procedure, often in relation to linearization procedures; –

4.Loading errors emerge when the intrusive nature of the sensor modifies the measurand. Along with calibration errors, loading errors are caused by internal processes; –

5.Environmental errors emerge when the sensor experiences the surrounding environment and these influences are not considered. In contrast with the previous two types of errors, environmental errors are due to external factors;

6.Spurious readings are non-systematic reading errors. They occur when some spurious physical occurrence leads to a measurement value that does not reflect the intended reality. For instance, a light intensity measurement in a room can provide the wrong value if obtained precisely when a picture of the room is taken and the camera flash is triggered.

Sensor Redundancy and Sensor Fusion

Redundancy implies that the fault has been understood and detected. Redundancy does not refer solely to having multiple similar components as in our case of multiple and contiguous M3. It is also possible to implement forms of redundancy in the time (e.g., repeating some action multiple times).

Providing the system with redundant components, that means redundant sensors, can compensate existing errors or faults affecting some component. The affected component can be replaced in its tasks by the spare, redundancy component, which will ensure that the system function will continue to be provided.

Sometimes sensor fusion techniques can be applied. While in single-sensor situations, there are models or related information that allow reasoning about an individual sensor's data quality without requiring other sensors' data, in sensor fusion techniques the process of combining sensory data or data derived from disparate sources is adopted such that the resulting information has less uncertainty than would be possible when these sources were used individually.

That means that , in the case of M3 board and sensors, we could correlate temperature with light sensor , in order increase data quality and reliability.

In a multi-sensor situation, the quality of sensor measurements is characterized by using redundant or correlated data obtained from the different sensors. This redundancy allows for data fusion methods to be deployed at the network level, resulting in improved (fused) sensor data, as well as improved data quality characterization.

Fault detection methods

A fault detection method for understanding sensor operation can be based on :

1.Rule-based methods that use expert knowledge about the variables that sensors are measuring to determine thresholds or heuristics with which the sensors must comply.

2.Estimation methods that define a “normal” behavior by considering spatial and temporal correlations from sensor data. A sensor reading can be matched alongside its forecasted value to assess its validity.

3.Learning-based methods that define models for correct and faulty sensor measurements, using collected data for building the models.

4.Fuzzy logic rules to obtain a qualitative sense of a sensor's validity based on its own historical behavior represented by a confidence measure.

Sensor Failure Modes

The main sensor failures modes, are the following :

1.Constant or offset failure mode: The observations continuously deviate from the expected value by a constant offset.

2.Continuous varying or drifting failure mode: The deviation between the observations and the expected value is continuously changing according to some continuous time-dependent function (linear or non-linear).

3.Crash or jammed failure mode: The sensor stops providing any readings on its interface or gets jammed and stuck in some incorrect value.

4.Trimming failure mode: The observations are correct for values within some interval, but are modified for values outside that interval. Beyond the interval, the observation can be trimmed at the

interval boundary or may vary proportionally with the expected value.

5.Outliers failure mode: The observations occasionally deviate from the expected value, at random points in the time domain;

6.Noise failure mode: The observations deviate from the expected value stochastically in the value domain and permanently in the temporal domain-

Faults at the network level

When connecting individual sensor nodes in a wireless sensor network, additional faults affecting sensor data can be introduced by the network. The main kinds of network faults that may affect the quality of sensor data in order to achieve a reliable network operation, specifically considering faults in the time domain and faults in the value domain. In the time domain, a crash, omission or delay faults could occur.

1.Crash faults (for instance of the radio subsystem in a sensor node) lead to data absence and can only be mitigated with redundancy (e.g., a dual-radio system).

2.Omissions correspond to missing sensor readings due to lost messages. They can be prevented by enforcing communication reliability, for instance based on message retransmission. However, reliable

communication protocols are not very common in WSNs due to the additional resources (namely energy) they require. Therefore, omissions do happen in sensor networks and for the most part emerge because of sensor failures and packet losses.

Heavy packet loss and asymmetric links occur frequently in WSNs [32,33], for instance due to signal strength fading and intermittent or continuous environmental interference (e.g., wind or rain).

3.Attacks that may significantly affect the quality of sensor data, among other consequences for the application. In critical applications, it is important to deploy security techniques to avoid attacks or to mitigate their effects.

However, communication protocols typically incorporate data integrity verification mechanisms that allow the detection of corrupted messages, discarding those messages and hence transforming value faults into omission faults. Therefore, the only chance that received data do not correspond to what has been sent is when some part of the communication stack in the sending or receiving node (or both) is affected by an accidental fault not covered by the integrity verification mechanisms or when it has been intentionally corrupted

The data processing level

Finally, in order to centrally analyze all of the sensing information, a third layer appears in the system. In the data processing layer, it is possible to infer the quality of the gathered information, through fusion processes of redundant and related measurements, by multi-sensor fusion methods, or by expert-knowledge of the system model. In fact, this is where we can ultimately handle both sensor and network-level problems and apply some mitigation techniques.

Energy Efficiency

Obviously the more the redundancy, the more will be the energy consumption , since there will be multiple sensor measurements, multiple data processing, multiple transmissions.

Especially for large-scale deployment since sensors nearby the gateway more often consume energy and deplete earlier, or may face temporal death and disconnect from the network, which makes the lifetime of the whole network short.

Energy Consumption Constraint: The IoT energy consumption model depends on expenditure in transmit and acquisition, while processing and

sensing expenditures are less than data transmission/receiption. Selecting the subsequent hop is achieved via exploiting the nearest neighbor, and therefore each sensor has a transmission range to communicate with neighbors.

Identify the technical limitations of a multi-hop wireless network in terms of throughput, end-to-end delay and security.

In the kind of mesh network we are being setting up , in order to maintain the connectivity, the sensor nodes should be appropriately deployed. We can arrange a deployment by selecting the nodes of our topology. The cost of transmitting a message among sensors is independent of the number of receiving sensors, however, it depends on a function of their maximum distance for sending a message from sensors. Therefore, in the case of multi-hop networking, then it is possible to maintain connectivity without every sensor transmitting at maximum power. This allows us to seek optimal power range assignment for connectivity and other related network issues.

The capacity of a network is an important parameter for evaluating the performance of both an electronic device and a telecommunications system; in the latter

case, the transmission capacity is simply the maximum transmission speed of the line. For a better evaluation of the capacity of a network, reference is made to the **throughput**, i.e. the amount of information conveyed on a channel at a given time, which is always less than or equal to the maximum capacity and depends exclusively on how much information is introduced on the channel during the transmission; the throughput is therefore a specification of the transmission that relates to the maximum capacity of the network, which instead is fixed, constant.

As far as concerns **end-to-end delay** Constraint it is accounted for by finding the optimal number of hops in a path which might lead to different delay guarantees in the network. This delay might be classified into several types as queuing, propagation, processing, transmission, retransmission, and idle. The delay will be increasingly proportional to the number of hops- and will result by the product of the number of hops by the sum of all the componens of the single delay (Dqueu + Dprop + Dproc + Dtrans + Dretrans + Didle).

Besides energy is correlated with delay. For example, a smart meter requires a higher energy efficiency but has a low requirement for delay. Meanwhile, a

vehicular network is rather delay sensitive. Therefore, it is essential to understand the mechanism of controlling the neighboring set of sensors in different network technologies by adjusting the transmission range and/or selecting appropriate sensors to carry out a specific task

As far as concern **security** the multihop topology is a target of many possible attacks, since it is using the RPL protocol (see Figure x).

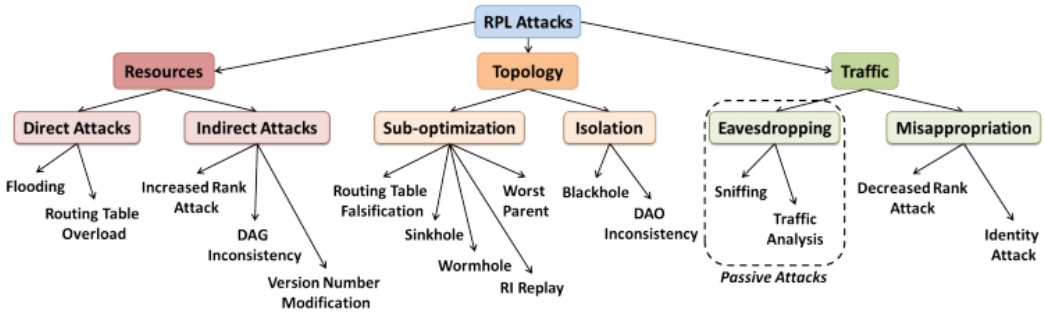


Figure 3.1: Taxonomy of attacks against RPL networks.

As it can be seen from the Figure above, there exist a plethora of attack to this kind of mesh networks.

Just to consider one of them, the traffic type of attack, or eavesdropping , which is passive type in nature.

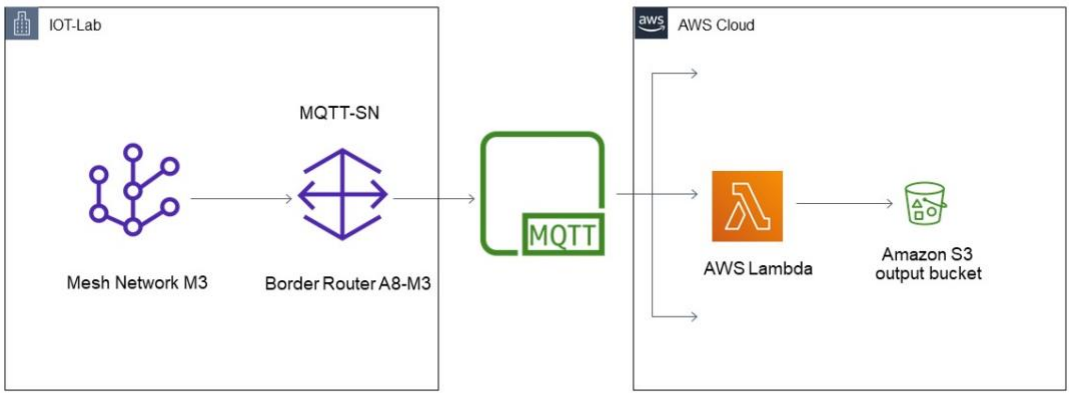
A sniffing attack consists in listening to the packets transmitted over the network. This attack is very common in wired and wireless networks and compromises the confidentiality of communications. An attacker can perform this attack using a compromised device or directly capture the packets from the shared medium in case of wireless networks. The information obtained from the sniffed packets may include partial topology, routing information and data content. In RPL networks, if an attacker sniffs control messages, it can access information regarding the DODAG configuration such as DODAG ID, version number, ranks of the nodes located in the neighborhood. By sniffing data packets, the attacks can not only discover packet content but also have a local view of the topology in the eavesdropped area by looking at source/destination addresses. This attack is difficult to be detected due 38 Chapter 3. Taxonomy of Attacks in RPL Networks to its passive nature. The only way to prevent sniffing is encryption of messages when the attacker is external. Even if RFC 6550 mentions encryption of control messages as an option, the technical details are left out from the specification making implementation difficult.

What are the connected components, the protocols to connect them and the overall IoT architecture?
Provide a **new** network diagram that includes the wireless sensor network and the new network technologies and communication protocols used to interconnect it with the cloud-based elements.

This question is partially answered by the following document:

IOT-Second-Assignment-2021/Technical_Description_Boards.pdf at main · robertobruzzese/IOT-Second-Assignment-2021 (github.com)

As far as concerns the second part of the question the following diagram is the scheme of the overall architecture.



How do you measure the performance of the system?

Measure the performance of the wireless sensor network. Measure the end-to-end latency and throughput. Measure the overall quality of the wireless communication channel.

We have already defined the troughput. The definition of latency is based on ping, defined as the time interval between the time when an input is sent and when the output signal is received. It is the delay in data transmission over a network, that is: the response speed of a system to a pulse. The average time in milliseconds spent processing end to end message transactions over the selected time frame.
We could then measure it as the average response time from terminal nodes M3 to ping border router A3. It is really the BR the bottleneck. And in all the experiments taken in this assignment the BR seem to face well the load of the overall mesh network. This conclusion can be derived also from the distribution of peaks in the maximum number of nodes experiment.

As far as concerns quality , in theory there are many sensors nodes and border router nodes to be

distributed in a the Saclay site area, however, the goal of deploying should be to determine the optimal number of hops between the sensors nodes and the border router nodes while satisfying the quality (QoS) parameters. The model is presented as an optimization problem for quality in terms of energy consumption, delay, and throughput

The quality of service (QoS) or quality of network can be defined in terms of energy consumption, delay, and throughput of the network.

For having a better quality of the network the throughput should be increased , while minimizing the energy consumption and the delay.

In order to be more precise for Iot systems to be successful operations presume the qualities of the 5 experience definition based on energy efficiency, connectivity, throughput, availability, and delay sensitivity.

Since the location of rooms and spaces is not clearly known in the Saclay site, but they are not, it would be interesting to know if the various environments have different climatic conditions, different light exposures and so on. Thus becomes a tool for the investigation of physical environments done remotely just as a WSN

network allows us to know a territory in its environmental variables.

You can also make deductions on the distances between the rooms as we know the range of action of 802.15.4 wireless networks.

We know that in the case of **6LoWPAN** networks, the distance is 10 –100 m.

Energy consumption and duty cycle will be measured in relation to the performance of the wireless network. The negative aspects and limits of multi hop cannot be evaluated in this circumstance since there is single hop. Each M3 node is directly communicating with the BR.

Evaluate the performance of the system as the number of wireless elements increases. How does the physical location of the nodes affect the performance of the wireless network? Examine wireless network topologies of different diameter.

Three different experiments were performed with increasing numbers of nodes involved in the architecture. The first experiment with an application node , a border router and a broker. The second with 5 application nodes , a border router and a broker. And the third experiment with 11 application nodes, a border router and a broker.

M3-type nodes that are connected to the Internet are such due to the proximity of M3 nodes in the Saclay platform topology. In fact, all 12 M3 nodes of Saclay are within a few meters and the test for larger radius cannot take place. . In this case the diameter (the maximum distance between two nodes in the ***network***) of the realized network will be a few centimeters. The traffic will pass through the Border Router which is connected to the Internet thanks to the Ethos serial protocol. The radius of action of 802.15.4 protocol is a few tens of meters, so it is assumed that the Border Router can not be farther than this radius from the application nodes, and in any case in the absence of major disturbances.

Measure the energy consumption and duty cycling of the nodes keeping in mind the overall performance of the wireless sensor network.

The results in terms of performance on consumption are visible on the repository at https://github.com/robertobruzzese/IOT-Second-Assignment-2021/tree/main/Performances .

The performances in terms of consumption does not vary much as we found a constant value for the consumption of the broker and a value of about 20% higher for the border router with a number of ten nodes higher. This factor does not affect much the duty cycle of the border router in the case of 10 nodes, but could be critical in the case of 100 nodes.

Considerations about the location of sensors

Calibration actions are required every time a sensor is deployed in a different environment, as the physical measurement elements must be adjusted or even dedicated to the monitored device or process, providing at the start a reduction of measuring uncertainty and minimal interference with sensor functions. However, periodic calibrations are also needed, since during the operation, we can assist the

change of conditions with respect to those known during the calibration process and to the impact of various external factors that could be absent in the laboratory calibration condition.

---

i