Which wireless network for the Smart City & Smart Building?

By Pascal DARAGON

1 INTRODUCTION

In this publication, we will examine the various solutions for ensuring successful connectivity in these particular contexts, bearing in mind that some arguments will be equally relevant to other contexts such as utilities, agriculture, and industry, as well as perimeter surveillance applications for security and defense.

We will first outline the limitations of LPWAN solutions, which currently represent the largest market share, to deduce the necessary corrections and what the "ideal" network should be, and then explore the world of "Mesh" networks, which, in our opinion, constitute the best answer to the problems exposed.

Finally, we will explain what makes **ORAMA-Net**, our **LoRa™ Multi-Hop** connectivity solution for IoT, an optimal response, both technically and operationally.

2 THE LIMITATIONS OF LPWAN NETWORKS

2.1 Public Networks

In radio, the concept of distance does not always align with our geographical understanding of it; an object can be close to a Base Station or Gateway in the Euclidean sense, yet simultaneously inaccessible from a radio perspective due to obstructions in the wave path (e.g., metal walls, building facades, vegetation, etc.). Signal penetration at certain sites can quickly become a major challenge for public LPWAN networks (LTE-M, NB-IoT, Sigfox, LoRaWAN) because the placement of Base Stations or Gateways is driven by the objective of providing global coverage for the widest possible range of users, without considering individual needs. Adding infrastructure to cover a specific site is neither technically feasible nor economically viable.

2.2 Private Networks

LPWAN deployments in private networks theoretically allow antennas to be located as close as possible to the site to be covered, but this remains a complex process, sometimes requiring multiple antennas to ensure good coverage. Multiple antennas necessitate the implementation of a network server (NS) to coordinate everything, and technical feasibility and economic viability still remain challenges, albeit to a lesser extent. This is largely why this type of deployment remains relatively uncommon today.

2.3 Remote Control

The IoT is not just about sensor data collection (i.e., upstream data stream), but also about the ability to remotely control or command an actuator (i.e., downstream data stream), and to do so quickly and deterministically while minimizing energy consumption. LPWAN solutions, whether public or private, cannot achieve this because the device must first send a wake-up message to notify the network server (NS) that it is available to receive a return message. Under these conditions, reducing the latency increases the device's wake-up frequency and therefore its energy consumption; reducing the wake-up frequency increases this latency and thus the possibility of contacting the device at any time. Another drawback of this type of protocol is the significant probability that the wake-up message will not be received, and in that case, the instruction cannot be sent as intended.

3 WHAT "IDEAL" NETWORK?

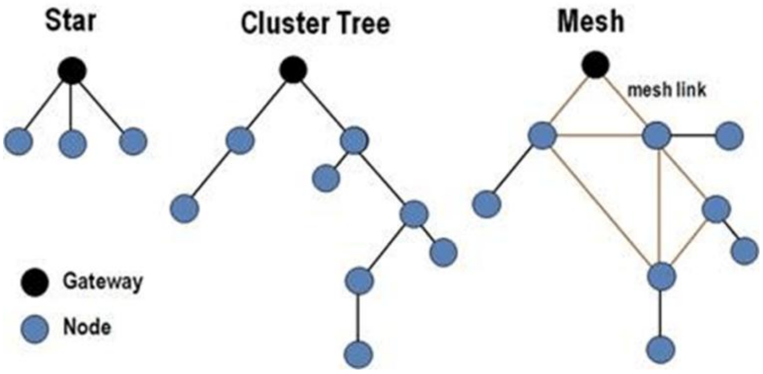
The ideal solution for Smart Cities and Smart Buildings (and by extension, industry) appears to be a system with the following characteristics:

1. Good signal penetration over obstacles that cause significant attenuation between the device and the base station antenna,
2. Good immunity to radio interference within the operating band, particularly in industrial or densely populated urban areas,
3. Only one base station antenna or gateway to install on-site, with no particular constraints on connection to the electrical grid or on people's exposure to electromagnetic radiation,
4. No core network and a direct connection from the gateway to the application server, or even to the supervisory control and data acquisition (SCADA) system for building management systems (BMS),
5. The ability to send a setpoint quickly and reliably, without a pre-programmed wake-up frequency or prior notification to synchronize the device and the application server.

4 IS IT A MESH NETWORK?

The ORAMA-Net protocol fully meets these 5 points, and it is indeed not a star-type LPWAN, but what is commonly called a mesh network; given the number of variants of this type of network, we must refine this overly general notion of "mesh" to divide it into at least 2 distinct categories:

1. **Decentralized or "Off-Grid" versions**, such as goTenna Pro, MeshCore, or Meshtastic, whose primary objective is to ensure information exchange within a community of nodes, without any notion of hierarchy, all possible meshes being used at any given time via a "flooding" type of information propagation, controlled or uncontrolled; this type of network is of little interest for centralized monitoring and proves to be energy inefficient,
2. **Centralized versions, or WSNs** (Wireless Sensor Networks), most often use a tree-like topology characterized by a multi-level structure with a root node at the top, intermediate nodes (branches), and terminal nodes (leaves) at the ends. Depending on the protocols, this tree structure is not fixed and can be reconfigured according to its environment, while maintaining a path back to the root node. For a given traversal, only one mesh is used at a given time T for several possible meshes. This is the category we will focus on for the remainder of the study.



4.1 WSN Networks

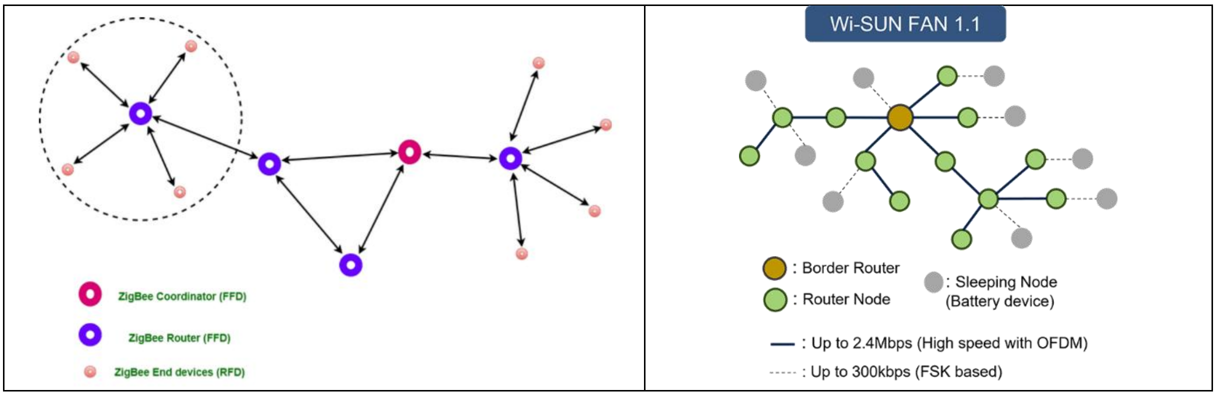
Several protocols of this type exist on the market, and without being exhaustive, we can mention the best known, Zigbee (2.4GHz), Wirepas with several variants (5G or NR+, 2.4GHz, Sub-GHz), more recently the Wi-SUN initiative (Sub-GHz, 2.4GHz), and finally ORAMA-Net (Sub-GHz, 2.4GHz). The term "Sub-GHz" mainly encompasses two relatively close bands:

1. EU863-870 for Europe, between 863MHz and 870MHz,
2. US902-928 for the USA, between 902MHz and 928MHz.

ZigBee and Wi-SUN are both based on the IEEE 802.15.4 public specification, while Wirepas 5G is based on the ETSI NR+ public specification; other Wirepas variants and ORAMA-Net are based on proprietary specifications.

ZigBee and Wi-SUN FAN (Field Area Network) have very similar architectures, inherited from their common foundation; there are 3 categories of nodes according to their hierarchy in the network:

1. The "Coordinator" or "Border Router" node, which manages several PANs (Personal Area Networks) and acts as a gateway to the backend (i.e., the cloud),
2. The "Router" node, which provides uplink and downlink communication within a PAN for a subgroup of nodes for which it acts as a relay; this node can also be a sensor or actuator, but its load capacity generally prevents it from operating on batteries,
3. The "End" or "Sleeping" node, which constitutes the sensor or actuator itself, operates on batteries; it is a terminal node that can only connect to a router node, and therefore cannot serve as a relay for another node.



It should be noted that building a ZigBee or Wi-SUN network requires a particular level of node specialization, which can prove to be a disadvantage in certain situations: instability of the radio link and/or mobility of the object.

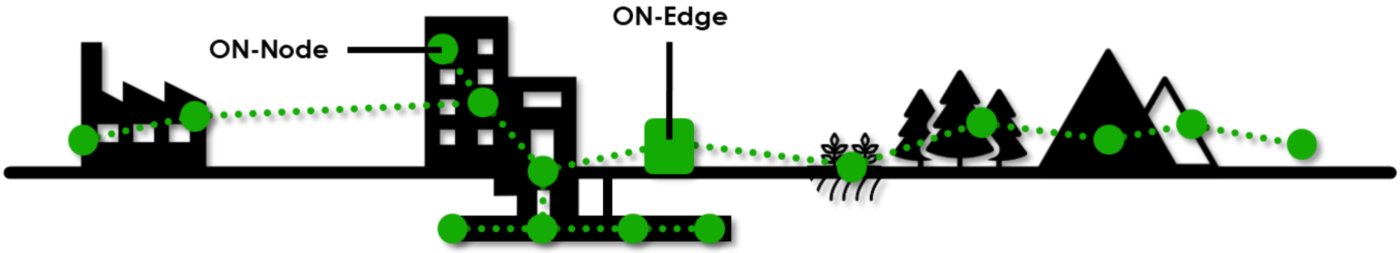
On a more dynamic level, Wirepas and ORAMA-Net present very similar operating models, for which there are only 2 pre-established hierarchical levels:

1. The **"Edge"** or "Sink" node, which manages a cluster of objects and acts as a gateway to the backend,
2. The node **"Node"**, which can connect to the "Edge" directly or via another "Node" which will serve as a relay, this route construction operates dynamically and autonomously for each node, coupled with self-healing capabilities in case of loss of a node on a route.

Both can operate with multiple concurrent edge devices on the same site, and each Peer-to-Peer (P2P) message between nodes is acknowledging and retries are made multiple times in case of transmission failure, enabling a Service Level Agreement (SLA) of 99.9% or higher without end-to-end acknowledgment.

Both also use sophisticated mechanisms to optimally manage the RF spectrum, avoid collisions and comply with applicable radio regulations depending on the deployment regions, from European standards ETSI EN-300-220 for Sub-GHz and EN-300-328 for 2.4GHz, to the American FCC directive part 15.247 for both bands.

For its part, ORAMA-Net uses LBT (Listen Before Talk) or PSA (Polite Spectrum Access) as defined in the ETSI standard, combined with an AFA (Adaptive Frequency Agility) algorithm guaranteeing pseudo-random and equiprobable access to all available channels in the working band, a rule imposed by the FCC directive. Moreover, this combination allows it to circumvent the 1% Duty Cycle constraint that governs the European EU863-870 band.



4.2 ORAMA-NET VERSUS WIREPAS

Since ORAMA-Net is designed for battery-powered devices and can operate for several years without intervention, we will exclude the 5G version of Wirepas from this comparison because we lack precise information on node power consumption. Furthermore, given that the carrier frequency plays a significant role in radio signal range, we can compare the Sub-GHz and 2.4GHz variants available in both solutions without bias.

The differences between Wirepas and ORAMA-Net will mainly lie in two points:

1. The most obvious difference lies in the choice of **physical layer**: Wirepas uses waveforms (or modulation) similar to those of Bluetooth for the Sub-GHz & 2.4GHz versions; for its part, ORAMA-Net relies on the CSS (Chirp Spread Spectrum) modulation of LoRa™ radio in Sub-GHz & 2.4GHz, known for its low power consumption, multi-kilometer range, and high immunity to interference,
2. The less obvious (but no less important) aspect focuses on **network construction**. The Wirepas node operates in "Discovery" mode, meaning it begins by sending a discovery message to its neighbors and waits for one or more responses that will determine its subsequent actions. An ORAMA-Net node is less "talkative" and initially listens periodically for a beacon emitted by the "Edge" and re-separated by intermediate nodes, much like a ripple on the surface of water. The benefit of this approach compared to "Discovery" mode is that ORAMA-Net nodes remain silent outside of any coverage area. The number of concentric circles is limited in practice to 9 ranks or hops to restrict network size and latency (standard configuration, although this number can be adjusted between 5 and 15 hops for specific uses).

The choices in point #2 stem from point #1, which determines the available bandwidth based on the modulations used. While Wirepas offers raw throughput ranging from 250 Kbps to 1 Mbps, ORAMA-Net can only rely on throughput ranging from 5 Kbps to 20 Kbps—up to 50 times less! Consequently, ORAMA-Net is designed to operate with minimal signaling, freeing up bandwidth for application messaging, and a finite number of hops from the edge to limit the population in a cluster. This limit remains high, however, since the model is designed to support up to 65,000 nodes per cluster.

What might seem like a drawback becomes an advantage when considering receiver sensitivity, that is, its ability to accurately receive a very weak radio signal, even below the noise floor. In this respect, CSS LoRa™ modulation is incomparably superior to the (G)FSK modulation used by Bluetooth. Where the sensitivity of a Wirepas receiver will be at best -100dBm, that of an ORAMA-Net receiver will reach -120dBm in DR6 (SF7/250KHz in Sub-GHz). It's important to understand that a gain of -6dBm doubles the communication distance between a fixed-power transmitter and a receiver, meaning that in the same environment, the potential communication distance between two ORAMA-Net nodes is **at least eight times greater** than that between two Wirepas nodes!

A simple (but realistic) calculation shows that 9 hops in ORAMA-Net are equivalent to 72 hops in Wirepas; or, for the same 9km cluster radius, each ORAMA-Net hop represents 1km, while it represents only 125m in Wirepas. This ratio becomes critical in difficult propagation situations, with high attenuation (e.g., concrete walls) and/or sources of interference along the wave path; the communication distance can drop to 200m for ORAMA-Net, or less than 25m for Wirepas.

The observation is that an ORAMA-Net network offers better "elasticity," providing greater flexibility in the placement of measurement or control points, thus limiting the need to install a large number of relay nodes to maintain a viable route.

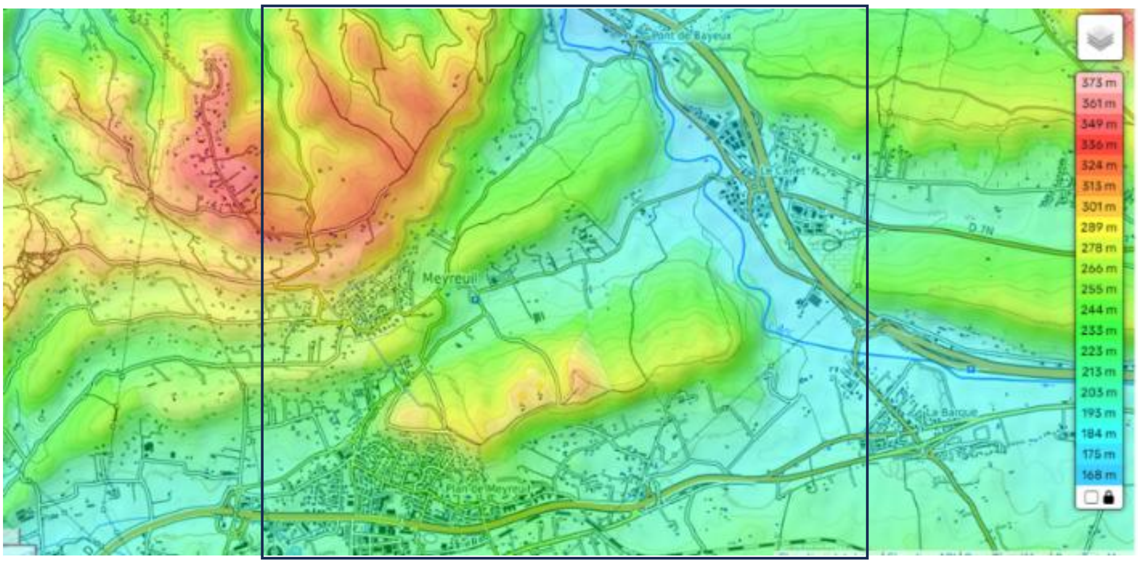
Wirepas claims the ability to network more than 1000 nodes per m3; **in contrast, ORAMA-Net claims an operational network with a density as low as 1 node per km3**.

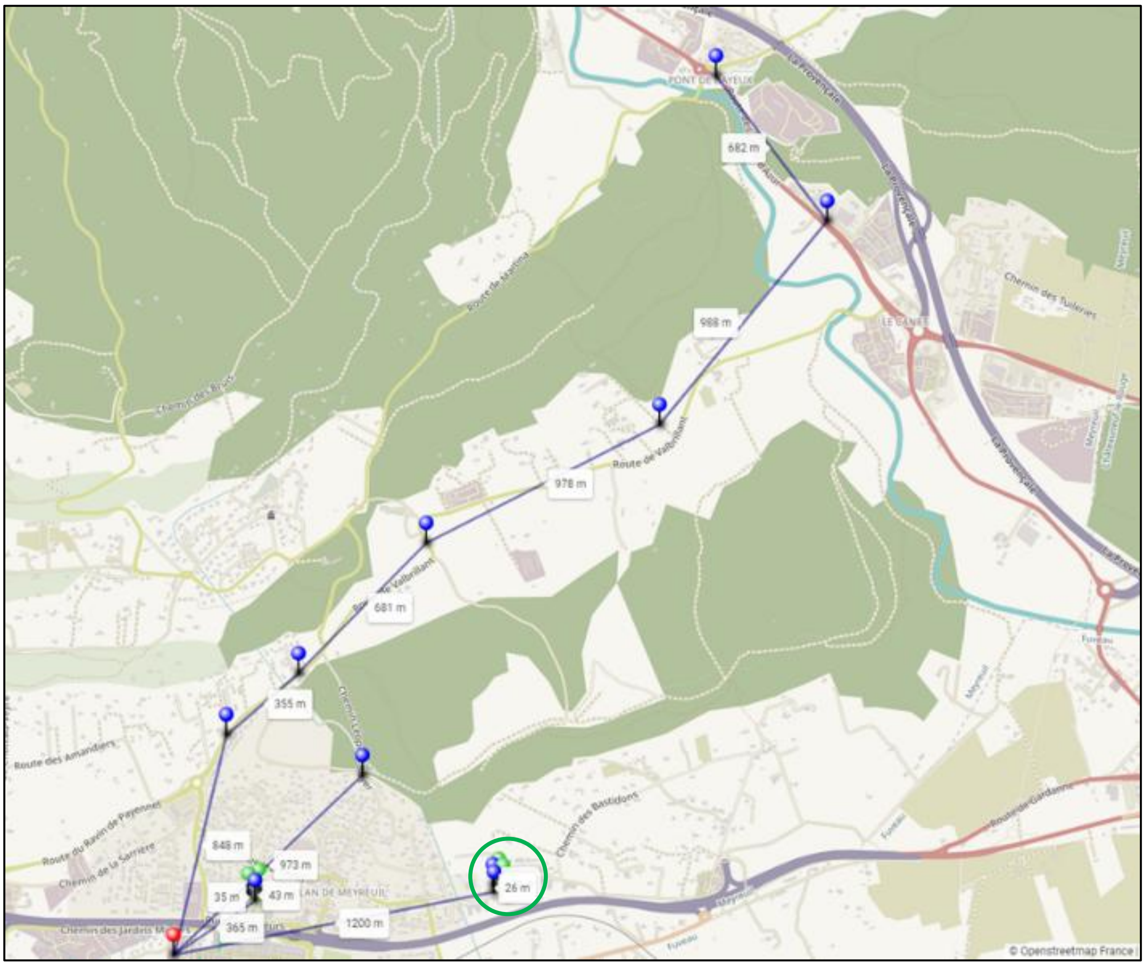
5 ORAMA-NET IN DETAILS

5.1 COVERAGE

The best proof is to see it on the ground; below are two images showing, at the same scale, the deployment of a pilot site with a maximum depth of 6 hops in the municipality of Meyreuil (2500 hectares), which houses our offices:

1. Topographic view showing a mixed environment of urban buildings and forest massifs which constitute multiple barriers to radio signal propagation; the black frame represents the effective deployment area circumscribed within a 5x5km block approximately corresponding to the view shown in (2),
2. OpenStreetMap view, showing the red "Edge" node (i.e., gateway) and the distribution of the blue "Nodes" nodes (i.e., temperature, air quality, and humidity sensors coupled to an actuator controlling a solenoid irrigation valve), and the associated hop distances.





In this complex and expansive environment, hops of close to or greater than 1 km are observed, particularly at 1200 m for the sensor circled in green. It is also interesting to note that the gateway does not need to be located on a high point; its active ON-Edge antenna is placed on the roof of our ground-floor office on a 1.5-meter mast, resulting in a total height of approximately 4 meters above the ground (photo below).

5.2 Consumption

ORAMA-Net is designed for multi-year operation of battery-powered devices; therefore, great care must be taken in the use of onboard energy.

The most important energy consumption factor to consider is not necessarily the energy cost of each message transmitted, as this is a very volatile and application-dependent factor; some use cases will require 2 messages per day while others will require one every 15 minutes, and for sizes ranging from 20 bytes to 200 bytes.

The true benchmark will be the energy expended to maintain the network's operation and the cost of the associated signaling; in this respect, we have two remarkable levers, which are real strengths of the protocol:

1. The **WOR (Wake On Radio)**, an ultra-low power listening and wake-up mechanism that consumes only 25µA.h (standard EU863-870 configuration),
2. The **URS (Ultra Relaxed Synchronization)**, a synchronization process that costs only 15µA.h, at a rate of one beacon every 20 minutes (node equipped with standard quartz).

It is with this **constant budget of 40µA.h** per node that the ORAMA-Net network is built, maintained, and reconfigured as needed (self-healing); this is an important point in that a change in route organization has no impact on this budget.

5.3 Bidirectionality

ORAMA-Net offers the same net upload and download speeds; in standard DR6 configuration (SF7/250KHz), this usable data rate reaches **1.1KByte per second**.

Since the LoRa™ transceivers used cannot transmit and receive at the same time (i.e., half-duplex mode), the arbitration between upstream and downstream streams is performed through a time division mechanism called TDD (Time Division Duplexing).

In downstream traffic, this principle guarantees a maximum latency of **20 seconds** between the sending of a message by the gateway and its reception by an object located on the last rank of the cluster, i.e. at a distance of 9 hops.

In upstream traffic, the need for determinism is less critical, and the delay between the transmission of a message by an object at the last rank and its reception by the gateway will be **1 minute** for messages tagged as priority (excluding retransmissions following a failure), because this application tag disables the aggregation functionality at the relay nodes; this delay will obviously be shorter for nodes close to the gateway, and a fortiori zero for rank 1 nodes.

For non-priority messages, this delay can reach several minutes depending on the aggregation parameters (timeout, water-level); as a simple example, with a time threshold set at 30 seconds and no other messages sent by the nodes attached to its route, a message from a node of rank 9 will arrive at the gateway within 4 minutes.

5.4 Scalability

In its standard configuration, ORAMA-Net's timing is based on 20-second cycles, totaling 4320 cycles per day, broken down as follows:

- a 2- to 4-second window reserved for the downlink stream,
- a 16- to 18-second window reserved for the uplink stream.

In downstream flow, the daily transfer potential is 4MByte (up to 4 messages of 245 bytes per cycle); each message can be destined either for all nodes of the cluster (i.e., broadcast), or for a particular node (i.e., unicast).

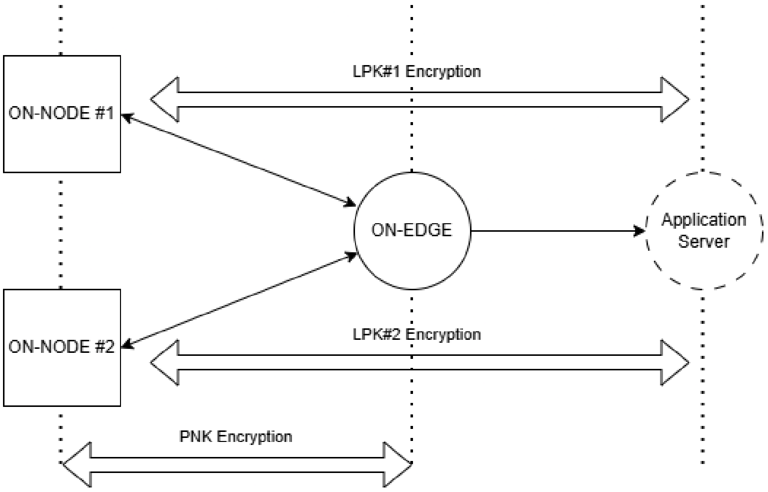
In the upstream flow, all messages are unicast since they are destined for the "Edge"; we will consider a configuration where the transfer load to the gateway is at 20% of its theoretical capacity and with an aggregation rate of 25% at the first-order nodes (i.e., cache purging after 4 messages); for a single message per node of 48 bytes of payload data, the gateway can absorb up to 192K messages per day, which represents:

- One message every 8 hours for a cluster of 64K nodes,
- One message every 2 hours for a cluster of 16K nodes,
- One message every 30 minutes for a cluster of 4K nodes,
- One message every 7 minutes and 30 seconds for a cluster of 1K nodes.

5.5 Security

ORAMA-Net implements a 2-level security scheme:

1. Point-to-point or P2P (Peer-to-Peer) security covers the segment from the node to the gateway; each node, including the edge, encrypts/decrypts and signs/verifies frames based on a **PNK (Private Network Key)** unique to each private network; a node without the correct PNK will not be able to join the cluster and will be rejected by all other nodes,
2. End-to-end (E2E) security covers the segment from the node to the Application Server (AS). This security is optional and can be enabled by the application if the device does not have its own Secure Element (SE) and uses the **License Provisioning Key (LPK)** assigned individually to each node.



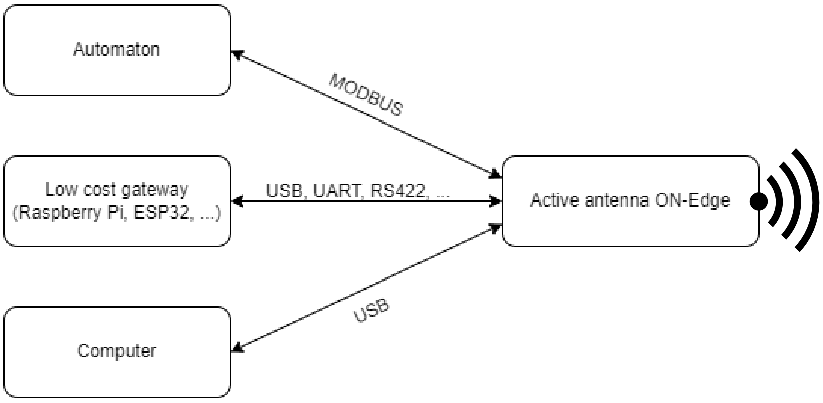
All of these security elements are encapsulated in a single certificate, which is downloaded to the device upon activation of the ORAMA-Net stack.

ORAMA-Net uses **AEAD (Authenticated Encryption with Additional Data)** cryptography with 256-bit (32-byte) keys, in accordance with **NIST 800-38C** recommendations.

5.6 Simplicity

No specific RF hardware is required for the gateway → an ORAMA-Net device connected via UART, USB, or RS-422 to a PC, industrial PLC, or low-cost gateway board (e.g., Raspberry Pi) is sufficient; only the firmware will be different:

- **ON-Edge** for the object acting as the gateway's active antenna,
- **ON-Node** for the object acting as a sensor or actuator.



ON-Edge manages the entire network, including P2P security:

- It transmits application data received from the cluster nodes to the gateway card after decrypting and verifying it with the PNK network key,
- It receives application data transmitted by the application server from the gateway card, signs and encrypts it with the PNK key before propelling it into the network.

Between the ON-Edge and the gateway card, and even more so between the gateway and the application server, data is always protected, either by E2E software security based on a unique LPK key per node, or by the hardware security of a Secure Element (SE) if the target device has one.

Note : The load on the gateway card is notably low since it operates completely asynchronously with the ORAMA-Net network timing fully managed by ON-Edge; for our demonstration and POC needs, we developed an ON-Spot hardware platform, based on a simple MCU from the ESP32-S3 family, connected to the ON-Edge active antenna via an RS-422 link over standard RJ45-Cat6 Ethernet cable allowing a separation of several hundred meters between the two elements.

The ORAMA-Net principle, whereby a gateway only exchanges messages with objects registered in its cluster, eliminates the need for a core network, such as an additional dedicated network server (NS) positioned between the gateway and the application server (AS). Even when an AS is connected to multiple clusters, an NS is not required for coordination.

Finally, it is not necessary to install the gateway on a high point to cover a large area; as illustrated in section 5.1, the LoRa™ Multi-Hop principle eliminates this terrain constraint.

5.7 Flexibility

ORAMA-Net was designed to address a wide range of IoT use cases, which will therefore include a wide variety of sensors or actuators, the only common point being that they all use LoRa™ radio technology.

In terms of implementation, beyond this requirement, ORAMA-Net does not require any specialization of the device for its execution, nor any hardware changes for existing devices; switching from the LoRaWAN protocol to ORAMA-Net is done through a simple software migration or port. The ON-Edge & ON-Node firmwares are compatible with the latest generations of Semtech SX126x, SX128x, and LR11xx components, and all MCUs based on the ARM® Cortex-M4 architecture (e.g., the STM32L4 family), which is universally adopted by 32-bit microcontroller manufacturers.

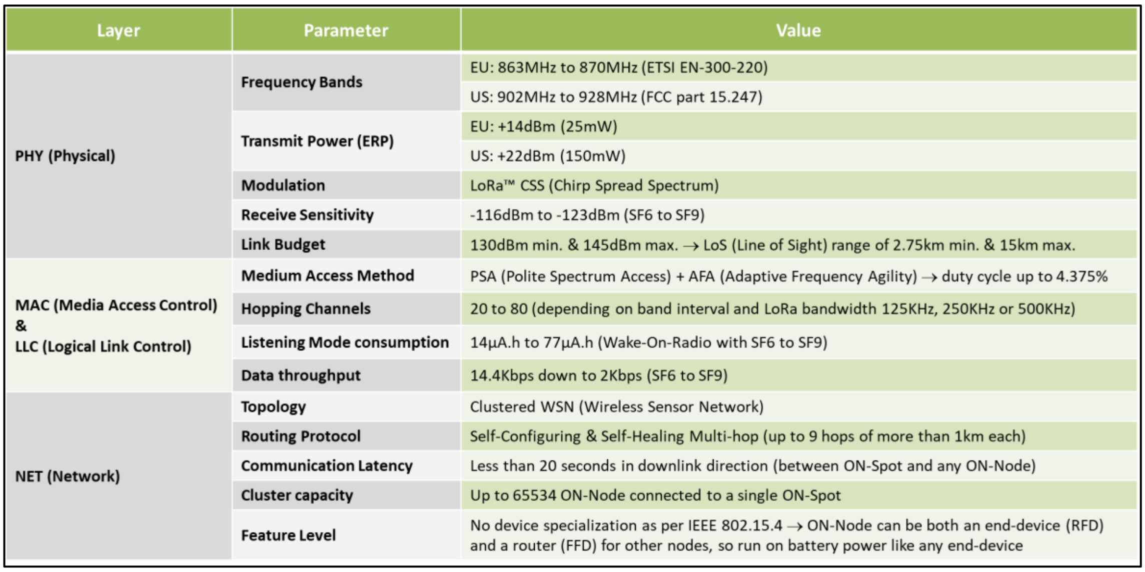
Operationally, as already mentioned in paragraph 4, ORAMA-Net does not use node specialization like protocols derived from the IEEE 802.15.4 standard, and offers greater flexibility in the installation of measurement or control points compared to protocols like Wirepas.

Finally, ORAMA-Net is not a fixed protocol and remains intentionally open to adjustments to its operating parameters to optimally meet different use cases:

- First, the SF (Spreading Factor) varies between SF6 and SF9; the lower the SF, the lower the induced consumption and the distance of each hop; the higher the SF, the higher these two metrics will be.
- The maximum number of ranks or hops within a cluster varies between 5 and 15; the lower this number, the lower the network latency, both upstream and downstream; the higher this number, the higher the latency.

- The beaconing rate defines the network's susceptibility to changes in spatial distribution and/or clock drift of the nodes. This parameter can vary from a period of 5 minutes for a scenario with moving nodes (e.g., cattle tracking) or high clock drift, to 80 minutes for a static scenario with very low clock drift (e.g., sensors on TCXOs).

ORAMA-System assists the client in selecting these parameters to evaluate the best settings; the table below summarizes the technical characteristics of the different variants.



Layer	Parameter	Value
PHY (Physical)	Frequency Bands	EU: 863MHz to 870MHz (ETSI EN-300-220) US: 902MHz to 928MHz (FCC part 15.247)
	Transmit Power (ERP)	EU: +14dBm (25mW) US: +22dBm (150mW)
	Modulation	LoRa™ CSS (Chirp Spread Spectrum)
	Receive Sensitivity	-116dBm to -123dBm (SF6 to SF9)
	Link Budget	130dBm min. & 145dBm max. → LoS (Line of Sight) range of 2.75km min. & 15km max.
MAC (Media Access Control) & LLC (Logical Link Control)	Medium Access Method	PSA (Polite Spectrum Access) + AFA (Adaptive Frequency Agility) → duty cycle up to 4.375%
	Hopping Channels	20 to 80 (depending on band interval and LoRa bandwidth 125KHz, 250KHz or 500KHz)
	Listening Mode consumption	14µA.h to 77µA.h (Wake-On-Radio with SF6 to SF9)
	Data throughput	14.4Kbps down to 2Kbps (SF6 to SF9)
NET (Network)	Topology	Clustered WSN (Wireless Sensor Network)
	Routing Protocol	Self-Configuring & Self-Healing Multi-hop (up to 9 hops of more than 1km each)
	Communication Latency	Less than 20 seconds in downlink direction (between ON-Spot and any ON-Node)
	Cluster capacity	Up to 65534 ON-Node connected to a single ON-Spot
	Feature Level	No device specialization as per IEEE 802.15.4 → ON-Node can be both an end-device (RFD) and a router (FFD) for other nodes, so run on battery power like any end-device

Note: This table is given for a fixed number of 9 hops max.; for a maximum number of hops N, the formula for the latency T is as follows:

$$T = (2 * N) + 2$$

We find that 20 seconds is correct for 9 jumps, and this will give 12 seconds for 5 jumps and 32 seconds for 15 jumps.

6 CONCLUSION

We hope this overview has helped you understand why we created ORAMA-Net, with the conviction that this protocol has a rightful place in the landscape of wireless solutions for the IoT market.

We do not claim to solve all wireless connectivity problems; ORAMA-Net is above all a pragmatic response to specific problems posed by Smart-City & Smart-Building use cases, with the tremendous potential offered by LoRa™ radio technology.

ORAMA-Net, presented as a software suite for integration into connected devices, is not aimed at the end users of these devices, but rather at manufacturers of sensors or actuators, integrators, and IoT verticals or **"Solution Makers"**, as we already do with a leading player in the field of solar public lighting.

If you belong to one of these categories and would like to learn more and test ORAMA-Net using our **demo kit**, please contact us by email at contact@orama-system.com

ORAMA-System
Connecting deep all
LoRa
Multi-Hop
A game-changer
for your business
Go deeper, longer,
greener, cheaper,
faster, safer !
Contact us
sales@orama-system.com
www.orama-system.com
POLESCS
SAFE
LoRa Alliance
0x0000000003
IMP18650
0x0000000002