Why we use LoRaWAN® connectivity in our solutions

LoRaWAN (Long Range Wide Area Network) is a low-power, long-range wireless communication protocol designed specifically for IoT (Internet of Things) and connected objects. It offers several benefits over traditional WiFi and cellular networks when it comes to IoT applications. Some of these benefits include:

1. **Long-range connectivity**: LoRaWAN can give connectivity through walls and floors by using different radio frequencies and modulation techniques (see FAQ for more details). This makes it ideal for connecting devices that are spread out over a large area or located in remote locations where Wi-Fi or cellular signals are weak or unavailable.

2. **Low power consumption**: LoRaWAN devices consume very little power compared to Wi-Fi or cellular devices, allowing them to run on batteries for years without needing replacement. This makes them ideal for IoT applications where devices need to operate independently and with minimal maintenance.

3. **Cost-effectiveness**: LoRaWAN networks can support a large number of devices at a lower cost compared to cellular and Wi-Fi networks. This is due to its simpler infrastructure and lower licensing fees for the radio spectrum. Additionally, the low power consumption of LoRaWAN devices results in lower operational costs.

4. **Scalability**: LoRaWAN is designed to support a large number of devices, making it highly scalable for IoT deployments. Its network architecture allows for easy addition or removal of devices without impacting the overall performance.

5. **Security**: LoRaWAN includes built-in security features, such as end-to-end encryption, mutual authentication between devices and network servers, and unique network keys for each device as well as no personal data being transmitted over the air. This ensures data privacy and secure communication between connected objects.

6. **Network penetration**: LoRaWAN signals can penetrate through obstacles such as walls and buildings, allowing for better coverage in urban environments and indoor spaces compared to Wi-Fi and cellular signals.

7. **Adaptive data rates**: LoRaWAN supports adaptive data rates, which means that the devices can adjust their data transmission rates based on their distance from the gateway and network conditions. This helps optimize power consumption and enhance network performance.

8. **Simple to deploy**: Installing LoRaWAN in a building does not require the service provider installing the solution to ask for Internet access such as Wi-Fi or Ethernet from the building user or owner. The whole solution is completely separate from the

client's own IT networks, so it does not pose any risks to the client and is therefore easier to get installed. All that is needed is a standard power plug for the gateway.

FAQ's about LoRaWAN

Q: How does LoRaWAN work through walls and floors better than WiFi?

LoRaWAN and Wi-Fi use different radio frequencies and modulation techniques, which impact their ability to penetrate walls and floors. Here are the main reasons why LoRaWAN has better penetration capabilities compared to Wi-Fi:

1. **Lower frequency**: LoRaWAN operates in the sub-GHz frequency bands (such as 868 MHz in Europe and 915 MHz in North America), while Wi-Fi typically operates in the 2.4 GHz and 5 GHz frequency bands. Lower frequencies have longer wavelengths, which allows them to penetrate solid objects more effectively than higher frequencies. As a result, LoRaWAN signals can pass through walls and floors more easily compared to Wi-Fi signals.

2. **Modulation technique**: LoRaWAN uses a modulation technique called Chirp Spread Spectrum (CSS), which is known for its resilience to interference and ability to maintain a strong signal in challenging environments. Wi-Fi, on the other hand, uses Orthogonal Frequency-Division Multiplexing (OFDM) modulation. CSS is more resistant to signal degradation caused by obstacles like walls and floors, making it better suited for penetrating these barriers.

3. **Lower data rates**: LoRaWAN is designed for low data rate applications, which means it transmits less information per second compared to Wi-Fi. The lower data rate allows LoRaWAN signals to be more robust and less susceptible to interference and signal degradation caused by physical barriers like walls and floors.

4. **Higher receiver sensitivity**: LoRaWAN gateways typically have a higher receiver sensitivity compared to Wi-Fi access points. This means they can detect and decode weaker signals even in the presence of noise or interference. The increased sensitivity allows LoRaWAN signals to be picked up despite being weakened by walls and floors.

Q: Is LoRaWAN secure?

LoRaWAN has built-in security features, and cellular networks also have their own security mechanisms. Microshare combines both for a robust and secure communication system for IoT applications. Devices such as sensors communicate

over LoRaWAN to gateways which in turn use cellular connectivity to send data to the Microshare cloud. All of these transmissions use highly secure wireless communications. Here are the security features of both protocols:

LoRaWAN security features:

1. End-to-end encryption: LoRaWAN ensures that the data transmitted between the end devices (such as sensors) and the network servers is encrypted using Advanced Encryption Standard (AES) with a 128-bit key. This provides confidentiality and protects the data from eavesdropping during transmission.

2. Unique keys: LoRaWAN uses unique network session keys (NwkSKey) and application session keys (AppSKey) for each device, ensuring that the data of each device remains secure even if another device's keys are compromised.

3. Mutual authentication: LoRaWAN devices and network servers use a process called "Join Procedure" to mutually authenticate each other before exchanging data. This ensures that only authorized devices can connect to the network.

Cellular backhaul security features:

1. Encryption: Cellular networks use encryption algorithms to protect data transmitted over the air interface between the devices and the base stations. For example, 4G LTE networks use the AES encryption algorithm with a 128-bit key, while 3G networks use the KASUMI block cipher.

2. Authentication and integrity protection: Cellular networks use a combination of a unique authentication key and a challenge-response mechanism to authenticate devices and protect the integrity of the data being transmitted.

3. Secure transport: When data is transmitted from the LoRaWAN gateway to the network server over a cellular backhaul, it can be secured using secure transport protocols like HTTPS, TLS, or VPNs, which encrypt and authenticate the data as it travels over the cellular network.

Q: What range can LoRaWAN cover inside of buildings?

The real-world range for LoRaWAN in deep indoor applications can vary significantly depending on the specific environment, building materials, and network deployment. While LoRaWAN has better penetration capabilities compared to other wireless technologies like Wi-Fi, deep indoor applications still present challenges due to signal attenuation caused by walls, floors, and other obstacles.

In general, LoRaWAN in outdoor settings can achieve a range of up to 2-5 kilometres (1-3 miles) in urban environments, and up to 15 kilometres (9 miles) in rural areas. However, for deep indoor applications, the range is significantly reduced. You can expect a range of 50-300 meters (164-984 feet) in deep indoor environments, but this is highly dependent on factors such as:

1. **Building materials**: Some materials, like concrete, brick, and metal, can significantly attenuate the LoRaWAN signal. The more walls and floors the signal has to penetrate, the shorter the range will be.

2. **Signal interference**: Electrical equipment, other wireless devices, and even the building's infrastructure can cause interference, which can impact the range and performance of LoRaWAN devices.

3. **Network deployment**: The placement of LoRaWAN gateways and the density of the network can impact the range and performance in deep indoor applications. Installing multiple gateways or using signal repeaters can help improve coverage in challenging environments.

4. **Multipath propagation**: In indoor environments, radio signals can bounce off walls and other surfaces, causing multiple signal paths to reach the receiver. This can result in signal fading or constructive interference, which can impact the range.

In summary, while LoRaWAN has better penetration capabilities compared to other wireless technologies, the range in deep indoor applications can be significantly reduced due to various factors. To achieve the best possible range in such environments, it's essential to carefully plan the network deployment, consider building materials and install gateways in locations where they can reach the maximum number of sensors. A typical store will only need one gateway to cover the whole store whereas a hospital or an airport will need several, potentially dozens of gateways due to the amount of interference or the scale of the site.