LoRa: An Excellent Long-Range Wireless Technology

Considerations for Implementation in Building Automation and Control Applications

Graham Martin, Chairman & CEO EnOcean Alliance

LoRa basically stands for Long Range radio - and that's exactly what it is. With a signal range of up to 10+ km, there is an abundant variety of applications for which this technology is well suited. For example, it's perfect for sending a meter reading signal from a smart meter to a central collection point a few kilometres away, once or twice a day (1). Other ideal applications include transmitting data on outdoor air quality, water levels in rivers and reservoirs, rainfall data or parking space availability. In the words of the LoRa Alliance, this proprietary wireless technology (exclusively owned and all chips supplied by Semtech Corporation, USA) - together with its wide-area network protocol, LoRaWAN LoRa : *"provides low power, long range connectivity within large-scale commercial implementations"* (2). Most applications feature a low sensor density and building-to-building outdoor communication in peripheral urban and rural areas (LoRa Alliance mission statement: "for large public networks").

This begs a question: how suitable is a slow-transmitting Long Range radio for home and building automation applications? A LoRaWAN signal that travels 10km is seconds long and very energy-hungry. Even using shorter range versions of LoRa, this seems like overkill for many typical building automation applications. Here we would like to investigate some of the considerations to be taken into account before implementing a LoRa solution in such applications.

LoRa's claim to suitability in a building automation context stems mainly from the assumption that there is no need to install an extensive infrastructure of gateways or receivers in a large building when a signal can travel from the basement to the 25th floor. However, these long and energy-hungry signals are less than ideal for many building automation and control applications. In many cases the resulting latency is not only a user issue, but also falls outside national specifications, e.g. the time required for switching a light on/off. More importantly, the long range and signal length characteristics of LoRa raise issues about security, duty cycle and interference or collisions. If all signals from the building can travel hundreds of meters or even a few kilometers, anyone within this radius could pick up and ultimately hack this signal / system. And when there are too many signals within this radius, the potential for interference, collisions and significant loss of signals threatens to cause network failure.

Spreading Factors

To enable optimization of different applications and their requirements, LoRa offers different configurations for transmitting data. It can differentiate between several spreading factors (SF). They basically change data rate in the spectrum between SF7 and SF12 and directly influence range, energy consumption, data package size and latency times. Long-range applications are typically taken care of by higher SF configurations (e.g. SF12) - less suitable for most building automation applications. Such applications are typically taken care of by lower SF configurations (e.g. SF7, 8 or 9).

The highest range (i.e. >10 km typically attained @ SF12) calls for a data burst lasting approx. 1.5 seconds - bringing the greatest risk of interference, collisions, eavesdropping and latency issues. Typical battery life in building monitoring and control applications would be just a few months, even with a high-cost, high-power battery (3). The shortest free-field range e.g. a few hundred meters (typically attained @ SF 7) calls for a 28 ms (or 56 ms) data burst - with a lower risk of interference, collisions or eavesdropping. High-cost, high-power battery life for typical building automation sensors could be around 4 years at the rate of 1 data burst with 6 Bytes of payload data every 15 minutes (3). In this case, the indoor range of such LoRa sensors is similar to other low-power wireless sensor solutions requiring significantly less energy and air-time, virtually eliminating the theoretical minimized-infrastructure advantage of LoRa (3),(4).

Power Supply Considerations

For LoRa sensors, the most common sources of energy are batteries. They must be sourced, stocked, installed, replaced and disposed of - and constitute an important cost and reliability factor. Moreover, high-capacity battery dimensions can be a limiting factor in device design/cost. Wired power supply can also be used, but obviously eliminates many of the advantages of a wireless communication, reducing placement flexibility, adding to installation time and cost etc.

Therefore, battery lifetime is a key consideration when deciding whether to adopt LoRa technology.

Let's investigate a typical LoRaWAN marketing claim.[(5)] **"**LoRaWAN end devices are optimized to operate in low-power mode and can last up to 10 years on a single coin cell battery".

A study performed by the School of Computer Science & Engineering, Nanyang TU, Singapore [(3)] concluded that sending a 6 Byte payload sensor signal every 15 minutes would result in a battery lifetime of 1.37 years using SF12, and 4.60 years using SF7.

Table 1. LoRa packets energy budget breakdown with PL = 6 Bytes, CR = 4/8, BW = 125kHz, 15 minutes per packet for SF7 & SF12 and battery capacity of 3.7V 2Ah.

States		Time (ms)	Energy (mJ)	Budget (%)
SF7 2dBm	MCU Active	40.50	0.50	0.30
	MCU sleep	899959.50	71.28	43.14
	Radio TX	38.85	4.36	2.64
	Radio Sleep	899961.15	89.10	53.92
		Total	165.24	4.60 years
SF12 20dBm	MCU Active	933.0	12.25	2.22
	MCU sleep	899067.00	71.21	12.87
	Radio TX	926.70	380.73	68.82
	Radio Sleep	899071.30	89.01	16.09
		Total	553.20	1.37 years

Source (3): Known and Unknown Facts of LoRa: Experience from a Large Scale Measurement Study, School of Computer Science and Engineering. Nanyang Technological University Singapore

This study is based on a relatively high-cost, large, high-power battery (3.7V, 2Ah) for home and building automation purposes. Expanding this to cover coin-cell batteries (5) gives the results shown in Table 2. Here we see that a single coin-cell battery-powered LoRa sensor sending a 6-Byte data payload signal every 15 minutes (very typical for a building and home automation sensor application) would last only a few weeks to a few months. In addition, this study notes that the cost of maintaining batteries over a 10- year period would be significant, in many cases exceeding the original cost of the sensor. Battery failure can also cause malfunction of the system. In a commercial environment, when a facility management company is responsible for changing batteries, the costs can increase even more (7). It is therefore common practice to replace batteries in such a scenario every year or in some cases even less, and at significant cost. (8)(9).

Table 2.

	Battery	JST-PHR-2	2 x CR2477	CR 2032
	Price	6,68 €	4,00 €	2,29 €
SF7 2dBm	Time (years)	4,60	1,87	0,41
	Battery change cost	17,52 €	13,50 €	10,94 €
	Battery changes in 10 years	2	6	25
	Battery costs over 10 years	41,72 €	85,00 €	275,67 €
SF12 20dBm	Time (years)	1,37	0,56	0,12
	Battery change cost	17,52 €	16,50 €	45,00 €
	Battery changes in 10 years	9	18	83
	Battery costs over 10 years	164,36 €	301,00 €	3.737,29 €

Assumptions: - Battery change person in-house changing multiple batteries

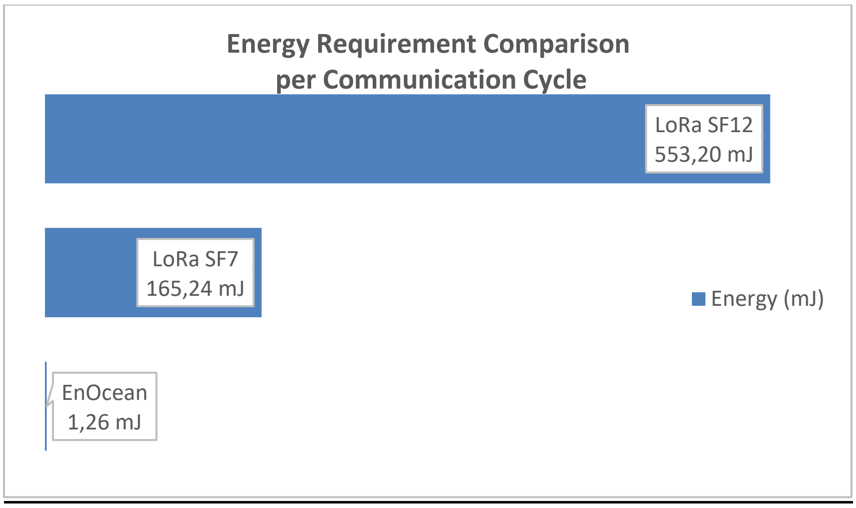
- Battery change time is 10 minutes
- Cost of person is 50 €/h
- Service charge is 50% (battery cost + person cost)

Note - if a Facility Management Service Company sends someone to change one battery, this can cost up to $293 / €275

(Source (7) Xidas_WP.pdf (mouser.com)

In a 2020 study published by Professor Michael Kroedel [(4)] “Smart Building trends - a comparison of wireless standards for automation and control” it is stated that “The most suitable wireless technology can only be identified, case by case, according to the „use cases“. And concludes that LoRa is less suitable for the majority of home and building automation & control systems. Professor Kroedel finds that other low-energy wireless technologies such as EnOcean and Z-Wave, or even BLE and Zigbee, are much better suited to such applications. One reason for this is the high energy and high latency times required by LoRa signals. Armin Pelka [(6)] expanding on the study from Singapore [3] compares the energy requirements for one LoRa communication cycle (at SF12 and SF7) with exactly the same data/communication cycle using the EnOcean Standard, i.e. 6-byte sensor payload data sending every 15 minutes.

Table 3.



Assumptions: 6 Byte Data Payload, 15 Minute Between Transmissions

Sources (3)+(6) Nanyang Technological University, Singapore & Armin Pelka

Duty Cycle Considerations

The Duty Cycle is an important concept in LoRaWAN deployments in order to manage radio frequency usage and prevent interference. Duty Cycle refers to the percentage of time that a device is allowed to transmit on a particular frequency channel within a specific time period e.g. per hour or minimum pause necessary between transmissions of a particular device.

In Europe, for example, the regulatory body ETSI (European Telecommunications Standards Institute) has set limitations on the Duty Cycles to ensure fair and efficient use of the radio spectrum. The Duty Cycle restrictions are designed to prevent any single device or network from monopolizing the available bandwidth, which could lead to interference with or malfunction of other devices or networks.

For the 868 MHz frequency band, which is used in Europe for LoRaWAN and other SRDs, the regulatory limit for a given frequency channel is a 1% Duty Cycle meaning that a device can transmit on that channel for up to 1% of the total time. For example, this means that a device is only allowed a maximum transmission time of 36 seconds per hour or per 1 second transmission time a minimum 100 second pause before another transmission can be performed.

For most home and building automation & control applications using low-power wireless technologies, this is not an issue. Even LoRa using SF7 or SF8 seems uncritical in this aspect. However, using the highest SF's this may become an issue in certain building automation applications [10] as shown in Table 4.

Table 4.

Airtime limitations

Telegram with 8 bytes payload size and 13 bytes overhead size.							
Spreading factor	SF7	SF7	SF8	SF9	SF10	SF11	SF12
Bandwidth [kHz]	250	125	125	125	125	125	125
Airtime [ms]	28,3	56,6	102,9	185,3	370,7	741,4	1482,8
Max. messages per hour	1.272	636	349	194	97	48	24
Min. pause between messages [s]	2,8	5,7	10,3	18,5	37,1	74,1	148,3

Source (10): TTN airtime calculator for LoRaWAN

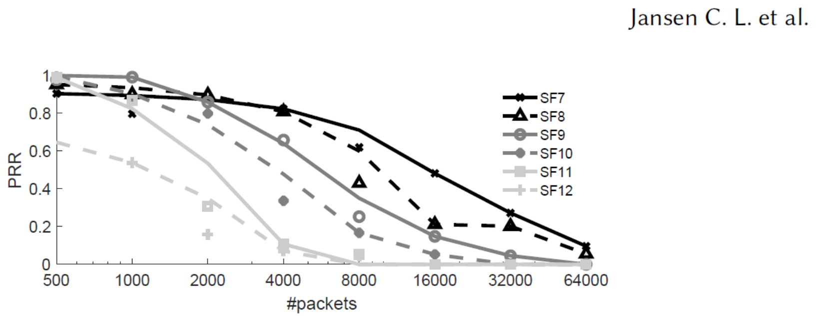
Interference & Collision Considerations

Interference is a significant challenge in LoRaWAN networks, as in any wireless communication system. Interference occurs when unwanted signals or noise disrupt the intended communication between LoRa devices - leading to reduced communication quality, higher error rates and potential loss of data packets. Interference problems in LoRaWAN include:

- Signal Degradation: interference can degrade the quality of the LoRa signal, making it harder for receiving gateways to correctly decode transmitted data. This can result in communication errors and reduced overall network performance.
- Frequency Overlap: LoRaWAN operates in unlicensed frequency bands, which means that multiple devices from various technologies might share the same frequency range. Interference can arise from other wireless devices and networks. This frequency overlap can lead to collisions and reduced range.
- Intermodulation: this occurs when two or more signals interact and generate additional signals at different frequencies causing confusion at the receiving end whilst making it a challenge to distinguish between the intended signal from the unwanted ones.
- Adjacent Channel Interference: devices using neighbouring frequency channels can cause interference if they are transmitting at high power, spilling over into adjacent channels and affecting the desired signal.

Table 5.

Packet Reception Rate Experiment (Source (3))



The experiment in Table 5 shows that, in a LoRa network with each device transmitting every 15 minutes, even with a few hundred nodes the packet reception rate decreases to unacceptable levels.

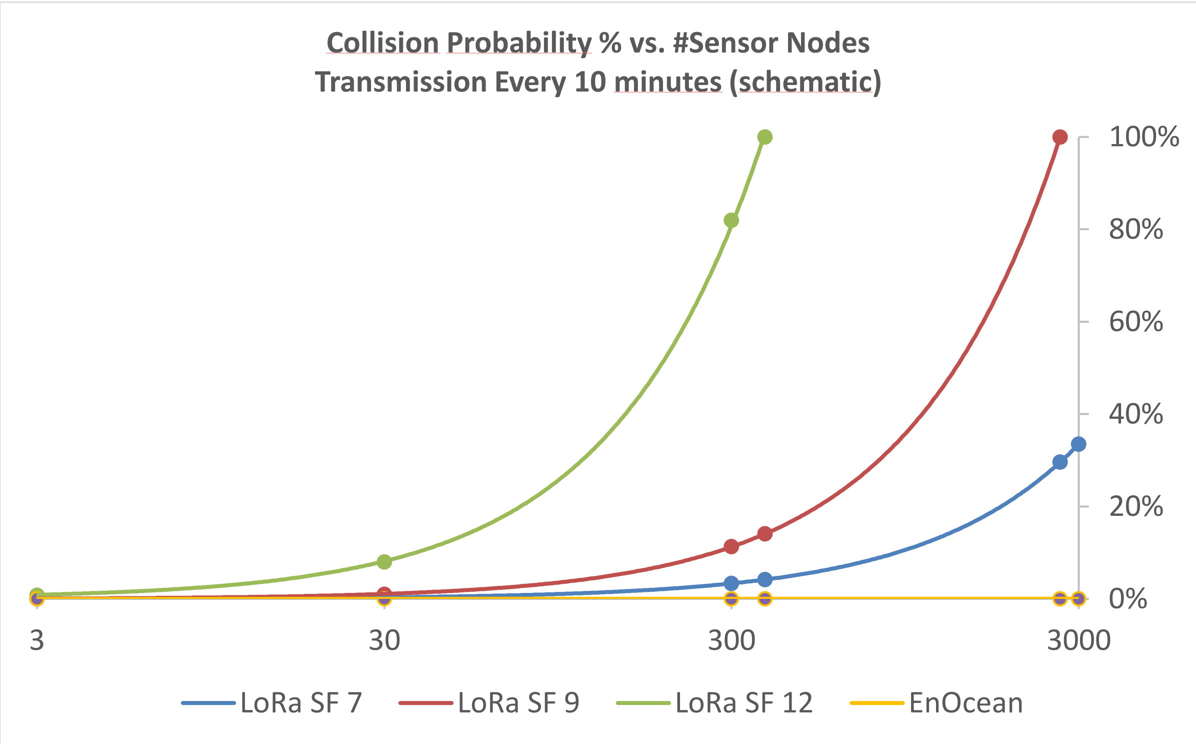
Collisions in LoRaWAN networks occur when two or more devices attempt to transmit data on the same frequency channel at the same time. Such simultaneous transmissions interfere with each other, potentially leading to the loss of the transmitted data packets. Collisions can significantly degrade the network's efficiency and reliability. Collision problems in LoRaWAN include:

- Airtime Utilization: each LoRaWAN device has a limited daily airtime allocation to prevent network congestion and ensure fair access to the shared medium. Collisions result in wasted airtime, reducing the efficiency of the network.
- Data Loss: when two or more devices transmit simultaneously, their signals overlap and become unintelligible to the receiving gateways. As a result, the transmitted data packets are not successfully received - and therefore lost.
- Retransmissions: collisions trigger retransmissions, as devices that experience a collision need to retry transmitting their data. This further consumes airtime and can contribute towards network congestion.
- Network Performance: frequent collisions can lead to a decrease in the overall network performance. Increased retransmissions and airtime wastage can result in longer latency and reduced throughput.
- Spreading Factors and Collisions: devices using different Spreading Factors (SF) have different signal spreads. Devices using lower SFs have wider signals, making them more susceptible to collisions from devices using higher SFs.
- Network Density: in areas with high device density, the likelihood of collisions increases. The probability of collisions also rises when multiple devices are in close proximity and use the same frequency channel.

- Collision Detection: LoRaWAN does not provide built-in collision detection mechanisms due to the modulation's inherent characteristics. Devices rely on acknowledgements and retransmissions to manage collisions.

Table 6 [5][6] illustrates that in a network with 30 nodes at SF12, each sending a signal every 10 minutes, the collision probability is already at a dangerous 8,2% level and the network will break down completely at less than 100 nodes. At SF9 the network will experience this dangerous collision level with around 200 nodes within the network. At SF7 such issues will arise at around 1.000 nodes within the network. In comparison, an EnOcean network (specifically developed for home and building automation & control) can handle a network of 3.000 nodes with less than 0,1% collision probability.

Table 6.



"Foreign network" disturbances

An increase in LoRA popularity inevitably brings the acute, unsolvable problem of data collisions from LoRa networks nearby and further afield - and owned by third parties, whose actions are beyond the control of the individual network operator.

In the study above we see that LoRa network collision levels will reach critical or unacceptable levels with just tens, hundreds or a few thousand nodes depending upon the SF used. In an urban area the LoRa user can take measures to minimize the risk of interference and collisions within his own network, but has absolutely no influence whatsoever on neighbouring networks - which could amount to dozens, hundreds or even thousands of networks featuring tens of thousands of nodes - leading to complete network breakdown. Such problems are exacerbated by LoRa's inherent characteristics and can impact all SF configurations.

Sources:

1. "The Power Struggle for Smart Building Automation Protocols"
by Peter Smith, Head of Sales & Marketing, IAconnects Technology Ltd.
https://www.iaconnects.co.uk

2. http://pages.lora-alliance.org.pages.services/Buildings-Vertical-Market)

3. "Known and Unknown Facts of LoRa: Experiences from a Large Scale Measurement Study"
by School of Computer Science & Engineering, Nanyang Technological University, Singapore
https://dr.ntu.edu.sg/bitstream/10356/142869/2/Known%20and%20unknown%20facts%20of%20LoRa%20experiences%20from%20a%20large-scale%20measurement%20study.pdf

4. "Smart Building trends - a comparison of wireless standards for automation and control"
by Prof. Dr. Michael Krödel, Institut für Gebäudetechnologie

https://www.ashb.com/wp-content/uploads/2020/11/IS-2020-161.pdf

5. LoRaWAN, https://www.thethingsnetwork.org/docs/lorawan/what-is-lorawan/

6. Ingenieurbüro Armin Pelka, https://www.pelka.de

7. Xidas_WP.pdf, www.eu.mouser.com

8. www.tcsecurity.co.uk/index.php/faqs

9. www.abpa.de/media/wartung_jab_18_angebot.pdf

10. TTN airtime calculator for LoRaWAN,
https://www.thethingsnetwork.org/airtime-calculator