Addressing scalable, optimal and secure communications over LoRa networks: challenges and research directions

Nicola Accettura, Eric Alata, Pascal Berthou, Daniela Dragomirescu, Thierry Monteil

Received xxx; | Revised xxx; | Accepted xxx

DOI: xxx/xxxx

LETTER

Addressing scalable, optimal and secure communications over LoRa networks: challenges and research directions

Nicola Accettura* | Eric Alata | Pascal Berthou | Daniela Dragomirescu | Thierry Monteil

LAAS-CNRS, Université de Toulouse, CNRS, INSA, UPS, Toulouse, France

Correspondence
*Nicola Accettura, 7 Avenue du Colonel Roche, 31400 Toulouse, France. Email: nicola.accettura@laas.fr

Summary

The Internet of Things (IoT) enables large scale deployments of very low power devices connected through wireless lossy links and able to interact with the surrounding environment (sensing and actuation). Two main challenges are then present: make them communicate; handle their energy consumption while respecting some cost constraints. Low Power Wide Area Networks (LPWANs) tackle these challenges by offering long-distance coverage while guaranteeing the use of a very little amount of energy for communications. Among many LPWAN technologies, Long Range (LoRa) networks provide a very promising but incomplete basis for satisfying the needs expressed by the applications running on low power devices. This paper describes the LoRa technology from the architectural point of view and points out those aspects that permit its seamless integration into the IoT. As major contribution, a focus on the current and future research on LoRa networks is provided by inspecting three facets: scalability, Quality of Service and security.

KEYWORDS:
LoRa, LPWAN, Scalability, QoS, Security

1 | INTRODUCTION

The availability of miniaturized and cheap circuitry is still contributing to the growth of the Internet of Things (IoT). In that, the market of IoT networks has been recently extended with long-range technologies in the form of Low Power Wide Area Networks (LPWANs). Several technologies have been developed, including Long Range (LoRa) networks, SIGFOX, WI-SUN and Narrow Band IoT. In order to set up novel monitoring applications, e.g., targeting optimization of industrial processes[1], low power radiolocation, and geofencing[2], it is mandatory to build interoperable networks, ready to be plugged and played through the Internet. In facts, such technologies are featured by some common aspects including: optimized radio modulation, star topology, tens of bytes long frames, a few frames transmitted mostly uplink per day with very low datarates and variable Maximum Transmission Units (MTUs). Among these technologies, LoRa has triggered a huge research interest given the inherent availability of different communication schemes, each mapping to a trade-off between device energy efficiency and network scalability.

In such a novel technological context, this contribution aims at surveying the recent research performed by the authors on LoRa networks. In doing that, it has been recognized that there are three main facets to be followed in future investigations, as also highlighted in the title of this paper. Indeed, the increasing amount of low power devices connected to the Internet requires communication protocols able to handle scalable deployments. From a Quality of Service (QoS) point of view, the consequent spring of novel applications, each having antagonist resource requirements, gives impulse to an anticipated study of optimal resource sharing mechanisms able to accommodate differentiated traffic patterns. Moreover, such networks will require

robustness through reliable implementation of security aspects. In details, Sec. 2 pictures the LoRa protocol stack with a bottom-up approach, paving the way to a complete communication architecture. Then, to browse the main research challenges in LoRa networks and to promote their seamless integration into the IoT, Sec. 3 addresses the description of the current and future investigations from the point of views of scalability, QoS and security. Eventually, Sec. 4 draws conclusions.

2 | LORA COMMUNICATIONS

Currently, LoRa networks are mainly defined through some specifications released by the LoRa Alliance. At the same time, the Internet Engineering Task Force (IETF) is already working on the definition of primitives that will allow IPv6-enabled LPWANs, including LoRa networks. The layered protocol architecture defined by both the LoRa Alliance and the IETF is a foundation on the top of which a service layer can support interoperable Machine-To-Machine (M2M) communications. This concept is illustrated in Fig. 1 and detailed in the following subsections.

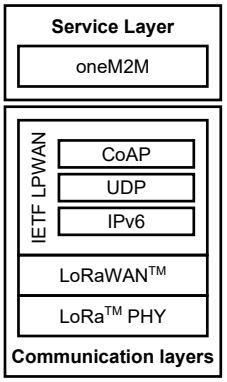

FIGURE 1 Communication architecture for LoRa low power devices.

2.1 | LoRa physical layer

The LoRa physical (PHY) layer makes several datarates available through the use of Chirp Spread Spectrum[3]. It enables robust and effective low power transmissions even in a noisy environment. The LoRa modulation is parameterized by a bandwidth (125 KHz, 250 KHz et 500 KHz), a spreading factor, and a coding rate. Each combination leads to a physical transmission rate (referred to as datarate in LoRa networks) and each device is allowed to choose and potentially adapt its physical transmission rate according to the quality of the wireless links to the gateways. The European 863−870MHz ISM band[4] allows the presence of 7 datarates, sorted from the lowest to the highest and indicated as $DR_0, DR_1, \ldots, DR_6$. Any datarate DR_i has an associated maximum transmission range R_i and a maximum time-on-air τ_i. Decreasing the datarate, both the time-on-air of frames and the transmission range increase[5]. End-devices choose the highest possible datarate, depending on their distance from the gateway. For example, end-devices whose distance from the gateway belongs to $]R_i, R_{i-1}]$ choose DR_i as transmitting datarate. The surface affected by DR_i is then the annulus around the gateway, with the radius of the outer ring being R_{i-1} and the radius of the inner ring being R_i. The area of the annulus increases as decreasing the datarate.

2.2 | LoRaWAN medium access

From an architectural point of view, a Long Range Wide Area Network (LoRaWAN) is handled by a central controller, namely a network *server*. Such a server coordinates several *gateways* by exploiting reliable communications on cabled or wireless technologies. At the same time, very low power constrained *end-devices* can communicate with the gateways over LoRa links. Generally speaking, the LoRaWAN specification[6] defines the Medium Access Control (MAC) layer of LoRa networks.

Whenever an information is available in its output buffer, an end-device immediately turns on its radio to transmit a link-layer frame over one among the available channels. If a duty cycle policy[4] applies, such a transmission is properly delayed to comply with the related limitation. Meanwhile, since gateways stay overhearing on all available channels, such a frame is received by all the gateways falling into the transmission range of the end-device. However, only a portion of such gateways do not observe collisions, thus correctly decoding the frame, extracting the included payload, and forwarding it to the server jointly with the perceived signal strength. Hence, multiple copies of the frame are received by the server, that in turn discards replicas. Then, the server selects the most appropriate gateway that will acknowledge the frame reception. The server piggybacks in the acknowledgment (ACK) the information it may wish to deliver toward the considered end-device. In this sense, the LoRaWAN scheme relies on gateways and server to handle the communication complexity, while easing the related implementation on end-devices. Indeed, the needed circuitry is not complex, thus making LoRaWAN end-devices cheap and easily available.

As a major need for LoRaWAN operators, it is very important to get reliability. This is achieved by properly bounding communication pitfalls, mainly represented by very frequent frame collisions due to the ALOHA-like nature of the access scheme. However, collisions can also be *avoided* through both a proper understanding of communication patterns and a robust design of

network architectures. To offer a trade-off between power-efficiency and the availability of communication resources, there are three modes of operations for end-devices. *Mode A* is the main communication pattern, with bidirectional data exchanges asynchronously and asymmetrically started by end-devices. With *Mode B*, end-devices listen to beacons broadcast by gateways to get synchronization on a common understanding of time. Being synchronized, end-devices can timely open reception windows, to listen to incoming frames from the network. Hence, this mode enables synchronous, bidirectional and symmetric communications. A synchronized access also permits Time Division Multiple Access scheme, which can be exploited either with a Slotted ALOHA access or with collision-free resource scheduling. Although some energy is wasted for synchronization purposes, the network capacity is increased, with time-critical applications benefiting from such a scheme. Finally, with *Mode C*, any communication exchange is bidirectional and asynchronously started by either an end-device or a gateway with a symmetric pattern. This is achieved by having all LoRaWAN devices continuously overhearing on the radio when they have nothing to transmit. This mode of operation fits actuators, or mains-powered end-devices that could perform relaying.

2.3 | Internet-connected LoRa networks

Given the inherent capability of addressing up to $\sim 3.4 \cdot 10^{38}$ entities, IPv6 is the key enabler protocol of IoT-aided automated houses, buildings, factories, and cities. However, wireless low power networks use data-link frames whose maximum length is not enough to contain a 1280-bytes long IPv6 MTU. On this regard, within the Internet Engineering Task Force (IETF) standardization body, the "IPv6 over Low power WPAN" (6LoWPAN) working group (WG) first and the "IPv6 over Networks of Resource-constrained Nodes" (6lo) WG later have already been dealing with the design of compression and fragmentation schemes able to let IPv6 packets fit 127 bytes long IEEE802.15.4 link-layer frames.

Herein, the spring of long range low power networks has triggered a renewed interest into adaptation layers similar to 6LoWPAN and able to guarantee RESTful CoAP-enabled communications and IPv6 connectivity [7]. Indeed, the wireless communication of such networks, by involving sporadic transmissions of very small frames at low datarates, puts an additional design constraints on IPv6 compression and fragmentation schemes. To this aim, the "IPv6 over Low Power Wide-Area Networks" (lpwan) IETF WG has been created within the IETF to target IPv6 connectivity on the top of some LPWAN technologies. In details, an informational document has been produced to describe the common characteristics and the actual needs of LPWAN technologies supporting IPv6. In addition, a specification has been being elaborated to enable the compression and fragmentation of CoAP messages encapsulated into IPv6 packet traveling over LPWANs. In details, a Static Context Compression Scheme is adopted to let CoAP/UDP/IPv6 packets be encapsulated in very small link-layer frames. A context defines how the packet header format is built. The context is static because it is pre-installed on end-devices and not learned through packet exchanges, since this in not compatible with LPWAN characteristics (e.g., duty cycle limitations or very sporadic traffic). Such a compression mechanism is independent of the specific LPWAN technology.

2.4 | oneM2M-interoperable LoRa deployments

The characteristics and capacities of LoRa networks address some of the problems that are found in connected object systems such as smart cities and even Industry 4.0. Nevertheless, the manipulation of a single communication protocol in these systems remains marginal. In general, it must be possible to interact with several protocols and be able to deal with the specific features of each of them. The solution was to propose standards for IoT able to take into account this challenge either in a specific field (e.g., in industrial contexts through the Industrial Internet Consortium) or in a multi-domain vision with the oneM2M standard. Indeed, the latter defines a common M2M service platform which can be implemented as an horizontal solution interconnecting all network devices. oneM2M enables multiple communication protocols binding, reuse of existing remote devices management mechanisms, and interworking with existing legacy devices. A specific entity called Interworking Proxy Entity (IPE) allows to connect specific protocols of sensors like those connected on a specific LoRa network. This standard is based on a RESTful approach with open interfaces to enable developing services and applications independently of the underlying network, thus easing the deployment of vertical applications. The oneM2M standard defines: (i) a set of services, i.e., registration, discovery, security, group management, data management, device management, network service exposure, communication, etc.; (ii) a structured data model based on resources; (iii) a standard Application Programming Interface.

It is worth remarking that the oneM2M standard does not define by now how to integrate and take care of specific LoRa features (limited payload sizes, limited bandwidth, energy management, selection of the most fitting LoRaWAN mode).

3 | ISSUES AND CHALLENGES

The presented overview on LoRa networks has been focused on the innovative features that make it the preferred technology supporting very low traffic and reliable monitoring applications. However, there are still some issues that need to be addressed to make LoRa tailored for huge IoT deployments supporting differentiated types of traffic while preserving secure communications.

3.1 | Scalable deployments

LoRa deployments will connect a huge number of end-devices performing sensing operations. Thus, it is mandatory to study the capacity of such technology, in order to understand its scalability. The capacity of LoRaWAN has also been studied for single gateway deployments [8] and city scaled ones [9]. Based on the consideration about datarates and transmission ranges presented above in Sec. 2.1, it comes out that city scaled LoRa deployments should prefer the use of the highest datarate. Indeed, assuming that the end-device density per area stays constant, for a datarate lower than the fastest one, (i) more end-devices contend the access to the radio, and (ii) transmitting the same amount of information takes more time (i.e., longer time-on-air). As a consequence, the collision rate is higher for lower datarates, thus making worth using just the fastest datarate in dense deployments of city scaled scenarios. Remarkably, it has been quickly recognized that the throughput of Pure ALOHA based LoRaWANs had not been investigated yet, to target multi-channel multi-gateway deployments [10]. In such environment, the classical ALOHA probability models do not suffice in picturing the increased capacity due to gateway redundancy. Moreover, some form of low power tracking and geofencing can be enabled through signal multilateration [2]. The system model sprang out from the assumption that gateways are placed according to regular patterns. In addition, the gateway redundancy was achieved by insuring that any end-device falls into the coverage range of at least three gateways. The throughput formulas found in those works [2,10] were designed to reflect the variation in the density of end-devices per unit area. Such probabilistic models were also validated through wide simulation campaigns. The simulation of realistic duty cycle limitations [4] showed also that the throughput trend can slightly differ when each device transmits very frequently, even though such discrepancy can be easily predicted. As matter of facts, such an investigation has been the first milestone in the study of scalable LoRaWANs, with several research directions open ahead.

Benefit of multiple gateways: To increase the number of gateways able to capture frames from end-devices, it is sufficient to reduce the relative distance among them. On this regard, the network capacity must be assessed when varying the ratio between the density of gateways and the density of end-devices.

Impact of ACKs: It has to be understood the trend in the throughput when uplink frame transmissions are confirmed (i.e., ACKs are required to the aim of reliability). Indeed, duty-cycle limitation put constraints also on the downlink transmissions, thus dwarfing the capacity of gateways to acknowledge correct frame receptions.

From LoRaWAN to 5g and beyond: A question to be answered is about which features of LoRaWAN will be imported in the future IoT standard technologies enabled in 5+ generation of cellular systems.

LoRa-equipped low-orbit satellite networks: With the recent availability of low-orbit satellites equipped with LoRa chipsets, there have been some envisaged scenarios [11] where some inaccessible areas could be easily monitored. In that, a thorough investigation should be done to the aim of understanding how many end devices can be managed over very long ranges and how to handle intermittent communications.

3.2 | Quality of Service

LoRaWANs have been evaluated in several research works in terms of coverage, throughput offered to end-devices, network capacity and scalability [12,8,13]. Evaluation results show that LoRaWANs can offer good performances in terms of coverage with limited amount of exchanged traffic [8]. However, the scalability of the network can be limited in terms of exchanged data due to the joint utilization of ALOHA access scheme with duty cycle limitations [2]. In fact, in a dense network of relatively high traffic devices, applications experience high delays and low reliability [13]. In addition, a high amount of confirmed end-device traffic (requesting ACK from the network) leads to severe degradation of network performances [14]. Accordingly, modes B and C (enabling a symmetric communication), may even trigger additional uplink communication by pulling data from the end-devices. Hence, to allow LoRaWAN technology to broaden its scope to applications with strict latency and/or reliability requirements, it is essential to make changes to offer better quality of communications [15]. Several ideas have been pursued to optimize the capacity of the LoRaWAN network and achieve better performances. For example, the use of mode B enables the use of resource

scheduling that can be handled in a centralized way, in order to reduce the collision rate and to provide time determinism. In this sense, the following research lines are envisaged to be addressed to achieve optimal traffic management on LoRa networks.

Scheduling LoRaWAN access: The LoRaWAN performance shift when employing mode B has to be thoroughly investigated. On this regard, scheduling algorithms for LoRaWANs have to be properly designed to account for multi-gateway deployments.

Coexistence of mode A and B: Mode A and B can coexist on the same deployments. It is of utmost importance finding a threshold mechanism able to let end-devices switch among the two modes of operation depending on the traffic conditions.

Defining new LoRaWAN modes: End-devices with higher requirements in terms of data exchange will need to use other communication patterns, possibly half-way in the middle between mode B and mode C. Specific channels can be assigned to devices operating with such mode. The channel access has to be designed to respect duty cycle limitation, while spreading the end-device transmissions over the time based on pseudo-random calculations and soft synchronization tools.

Listen Before Talk (LBT): Such a channel access should be investigated as replacement for the current policy used for attaining the management of the duty cycle limitation.

LoRaWAN gateways connected through geostationary satellite links: Satellite links represent a backup solution in case of malfunctioning of backbone infrastructure among gateways. They can also be used to replace cable links onto inaccessible areas. The performance evaluation of such networks is indeed finalized to combine resource scheduling in beacon-enabled LoRaWANs with the communication scheduling on geostationary satellite infrastructures.

3.3 | Security

LoRa provides confidentiality with encryption based on multiple keys. A good level of confidentiality is achieved if keys are different among LoRa devices of the same type and if the AES implementation works properly. However, in a critical context, integrity and availability are also important properties to be addressed on LoRa devices[16]. Even though the LoRaWAN MAC layer is publicly available, the LoRa PHY is not completely open, with the only documents available being a patent and a specification[3]. It is important to assess the security of the LoRa physical layer.

The protocol has been assessed in several studies. A work by Aras et al.[17] proposed to selectively jam one device while leaving other devices unaffected. This weakness impacts availability. Two other vulnerabilities were found[18]. The first one is related to the attacker's ability to open a device to retrieve the keys. The second one is linked to the reply of an already transmitted message. The reverse engineering of the LoRa PHY[19] has been done using an Universal Software Radio Peripheral (USRP) and GNU-radio software. This reverse engineering led to the implementation of LoRa modulation/demodulation as a GNU-radio block. This result allows to retrieve the content of messages that respects the format described in the MAC specification[6], and to confirm the previous vulnerabilities. Based on these studies, two future directions have been identified.

End-to-end security: To deal with the identified security issues, devices should be designed with end-to-end security, from the PHY to the application layer. In particular, a poor reception quality must cause a software exception. Nevertheless, this strategy must be implemented with care, otherwise, an excess of corrupted messages may overwhelm the software with exceptions.

Identification of the emitter: Investigating the behavior of chips may be used to establish a "behavioral" signature and to identify the emitter. This solution is based on the assumption that a chip and its behavior cannot be cloned.

4 | CONCLUSIONS

LoRa networks will play a great role in shaping the access infrastructure for the Internet of Things. Belonging to the wider class of LPWANs, they will ease the connection of billions of low power devices to the Internet, thus increasing the M2M traffic offered for novel IoT applications. However, there is still some ongoing debate on the real scope of such networks. Investigating the scalability is then necessary for an anticipated management of large LoRa network sizes. At the same time, different applications will need different treatments, calling for built-in mechanisms, like resource scheduling, able to insure an acceptable level of QoS. Also a thorough investigation on the security of such network is needed, given the sensitive data generated and relayed over these networks. This contribution has detailed these open issues and future research directions, by fitting them to an interoperable communication stack ready to be plugged and played through the IoT. As additional outcome, the paper has also given some pitch on future integration of LoRa networks coordinated by satellite links, for a totally reliable network infrastructure.

References

1. Thubert P, Pelov A, Krishnan S. Low-Power Wide-Area Networks at the IETF. *IEEE Communications Standards Magazine.* 2017;1(1):76–79.
2. Accettura N, Medjiah S, Prabhu B, Monteil T. Low power radiolocation through long range wide area networks: A performance study. In: Proceedings of IEEE WiMob '17; 2017; Rome, Italy.
3. Semtech . *LoRa™ Modulation Basics, AN1200.22, Revision 2.* 2015.
4. LoRa Alliance Technical Committee. *LoRaWAN™ 1.1 Regional Parameters.* 2017.
5. Petäjäjärvi J, Mikhaylov K, Roivainen A, Hanninen T, Pettissalo M. On the coverage of LPWANs: range evaluation and channel attenuation model for LoRa technology. In: Proceedings of ITST '15; 2015; Copenhagen, Denmark.
6. LoRa Alliance Technical Committee. *LoRaWAN™ 1.1 Specification.* 2017.
7. Al-Kashoash HAA, Kemp AH. Comparison of 6LoWPAN and LPWAN for the Internet of Things. *Australian Journal of Electrical and Electronics Engineering.* 2016;13(4):268–274.
8. Mikhaylov K, Petäjäjärvi J, Haenninen T. Analysis of Capacity and Scalability of the LoRa Low Power Wide Area Network Technology. In: Proceedings of EW '16; 2016; Oulu, Finland.
9. Centenaro M, Vangelista L, Zanella A, Zorzi M. Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios. *IEEE Wireless Communications.* 2016;23(5):60–67.
10. Accettura N, Prabhu B, Monteil T. Simulating scalable Long Range Wide Area Networks for very low power monitoring applications. In: Proceedings of MSSANZ MODSIM '17; 2017; Hobart, Australia.
11. Qu Z, Zhang G, Cao H, Xie J. LEO Satellite Constellation for Internet of Things. *IEEE Access.* 2017;5:18391–18401.
12. Augustin A, Yi J, Clausen T, Townsley WM. A Study of LoRa: Long Range & Low Power Networks for the Internet of Things. *Sensors.* 2016;16(9):1–18.
13. Bor MC, Roedig U, Voigt T, Alonso JM. Do LoRa Low-Power Wide-Area Networks Scale?. In: Proceedings of ACM MSWiM '16; 2016; New York, NY, USA.
14. Pop AI, Raza U, Kulkarni P, Sooriyabandara M. Does Bidirectional Traffic Do More Harm Than Good in LoRaWAN Based LPWA Networks?. In: Proceedings of IEEE GLOBECOM '17; 2017; Singapore.
15. El Fehri C, Kassab M, Abdellatif S, Berthou P, A Belghith. LoRa technology: MAC layer operations and Research issues. In: Proceedings of RAMCOM '18:1–6; 2018; Porto, Portugal.
16. Powell D, Adelsbach A, Cachin C, et al. MAFTIA (Malicious and Accidental-Fault Tolerance for Internet Applications). In: Supplement of the 2001 Int. Conf. on Dependable Systems and Networks; 2001.
17. Aras E, Small N, Ramachandran GS, Delbruel S, Joosen W, Hughes D. Selective Jamming of LoRaWAN using Commodity Hardware. *CoRR.* 2017;abs/1712.02141.
18. Aras E, Ramachandran GS, Lawrence P, Hughes D. Exploring the Security Vulnerabilities of LoRa. In: Proceedings of IEEE CYBCONF '17:1–6; 2017.
19. Récoules Frédéric. Security in the Internet of Things – a LoRa study. Master's thesisInstitut national des sciences appliquées de ToulouseToulouse, France2016. https://hal.laas.fr/hal-01771641v1.

How to cite this article: Accettura N., E. Alata, P. Berthou, D. Dragomirescu, and T. Monteil (XXXX), Addressing scalable, optimal and secure communications over LoRa networks: challenges and research directions, *Internet Technology Letters*, *XXXX;XX:X–X*.