Low-Power Wide Area Networks (LPWAN) for Communications of Mobile Sensor Data

Sebastian Barillaro[*,†]
Engineering Laboratory
National Institute of Standards and Technology
Gaithersburg MD USA
sebastian.barillaro@nist.gov
barillaro@inti.gob.ar

Sokwoo Rhee[†]
Engineering Laboratory
National Institute of Standards and Technology
Gaithersburg MD USA
sokwoo.rhee@nist.gov

Gustavo Escudero[*]
Departamento de validación de dispositivos y sistemas electrónicos
Instituto Nacional de Tecnología Industrial
Buenos Aires, Argentina
gescudero@inti.gob.ar

Raghu Kacker[††]
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg MD USA
raghu.kacker@gmail.com

Lee Badger[††]
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg MD USA
lee.badger@nist.gov

D. Rick Kuhn[††]
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg MD USA
d.kuhn@nist.gov

ABSTRACT

There are multiple options for communication of data to and from mobile sensors. For tracking systems, Global Navigation Satellite System (GNSS) is often used for localization and mobile-phone technologies are used for transmission of data. Low-power wide area networks (LPWAN) is a newer option for sensor networks including mobile sensors.

We developed a tracking system use case application using LPWAN as communication channel for mobile sensor data. The choice of LPWAN has pros and cons. In this paper, we discuss the differences between LPWAN and other technologies as communication channel for sensor networks. We describe the LPWAN test setup and analyze its characteristics including transmission frequency, coverage, latency and communication range.

* Department of electronic devices and systems validation, National Institute of Industrial Technology, Buenos Aires, Argentina
† Smart Grid and Cyber-Physical Systems Program Office, Engineering Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce
†† Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce

SCC '19, September 10–12, 2019, Portland, OR, USA

ACM 978-1-4503-6978-7/19/09 $15.00
https://doi.org/10.1145/3357492.3358629

CCS CONCEPTS

Network performance analysis, Network components, Embedded and cyber-physical systems, Sensor networks

KEYWORDS

IoT, Internet of Things, LPWAN, Tracker System, LoRa, LoRaWAN, Sensor Network

ACM Reference format:

Sebastian Barillaro, Sokwoo Rhee, Gustavo Escudero, Raghu Kacker, Mark Lee Badger, D. Rick Kuhn. 2019. Low-Power Wide Area Networks (LPWAN) for Communications of Mobile Sensor Data. In *Proceedings of the 2nd ACM/EIGSCC Symposium On Smart Cities and Communities (SCC 2019). ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/1234567890*

1 Introduction

The emergence of low power wireless technologies has catalyzed broad adoption of Internet of Things (IoT) applications over the past several years. A typical IoT implementation includes a number of components and building blocks; one of the fundamental building blocks of IoT implementation is the communication and networking layer. Due to diverse requirements unique to each IoT application, a number of different technologies are being developed and adopted for communication and networking.

For the applications involving wireless sensors and actuators, the selection of wireless communication technology becomes a critical task. There are a number of fundamental characteristics to be considered when designing a wireless communication technology for an IoT application, and it should be chosen based on a careful analysis of the application requirements. Most of the wireless communication technologies will come with some type

of tradeoff among different characteristics such as data rate, power consumption, communication distance, latency, cost, reliability, robustness, and security. For example, a technology with higher data rate may need to consume more power. Another technology capable of both high data rate and low power may not be able to communicate in a long range. Because of these tradeoffs, a number of wireless technologies such as WiFi, Bluetooth, and Zigbee are discretely used in various IoT applications depending on their requirements.

Low power wide area network (LPWAN) is a wireless communication technology specifically designed to focus on low power and long-range communication. LPWAN is a promising technology with a great potential to be adopted in a number of smart city applications including metering, localization, transportation, and flood monitoring. However, it is important to understand the practical limitation of its characteristics before designing it in an application. To analyze its characteristics, a LPWAN test network was implemented in the main campus of the National Institute of Standards and Technology (NIST) in Gaithersburg, Maryland, USA, with coverage extended to its vicinity area. The test setup was developed to focus on localizations and tracking application. In this paper, the setup of the test network is described, and the test results are presented.

2 LPWAN General Characteristics

LPWAN is not a single technology. It is a set of several technology options with the shared goal of fulfilling specific sensor network requirements. Commercially known as 0G [1], there are plenty of options to choose from. Although these technologies are always prioritized on wider area coverage and minimal energy consumption over data rate, it is possible to apply them to a variety of uses cases which require different degrees of data rate, communication periodicity, latency, distance, etc. Since these technologies are optimized for energy consumption, some of them cannot handle Internet Protocol (IP) Headers, hence are not IP-compliant.

2.1 LPWAN Options

There are many LPWAN options. The list is broad and its border-line is not clearly defined. It is not the intention of this paper to discuss what is, and what is not an LPWAN option nor make an exhaustive analysis about all of them. However, a non-comprehensive list is given as starting point for readers that would desire to dive deep. This list is divided according to whether a license is required or not to operate in a specific frequency.

2.1.1 Cellular LPWAN Options

- LTE Cat 1
- LTE Cat 0
- EC-GSM-IoT
- LTE Cat M1 (also known as LTE-M)
- LTE Cat M2
- LTE Cat NB1 (also known as NB-IoT)
- LTE Cat NB2

2.1.2 Non-Cellular LPWAN Options

- Sigfox
- IngeNU (formerly RMPA)
- LoRa/LoRaWAN
- LoRa/M.O.S.T.
- LoRa/Symphony Link

Due to NIST's IT security restrictions and policies, four main requirements, among others, were considered when selecting a technology to be tested:

- No proprietary solutions.
- Built-in security in specification.
- Ownership of entire platform.
- No Internet connection required.

All these LPWAN options were analyzed based on available literatures. IngeNU did not meet requirements due to be a proprietary specification. Sigfox, LTE-M, and NB-IoT require Internet connection and cannot be deployed as an isolated network without Internet access. LoRa is a proprietary technology, but LoRaWAN Protocol is an open standard. It does not require Internet connection and its deployment can be done entirely on premises at The NIST Campus as a standalone system. LoRaWAN also has built-in security measures and is broadly adopted. LoRaWAN alternatives (M.O.S.T and Symphony Link) also did not meet requirements due to its nature as a proprietary technology.

After considering all these options, LoRa/LoRaWAN was selected as the LPWAN option to study its characteristics.

2.2 LoRa/LoRaWAN

LoRa (short for Long Range) and LoRaWAN (LoRa Wide Area Network) refer to different meanings and concepts. LoRa is a spread spectrum modulation technique derived from chirp spread spectrum (CSS) technology with an operational frequency in the sub-GHz ISM band. The LoRa-Alliance defines regional specification according to local regulations dictated by local telecommunication authorities. The most widely adopted operating frequencies are the US915 band which includes 64 x 125 kHz width channels and 8 x 500 MHz width channels between 902.3 and 914.9 MHz; and the EU868 band, which includes 8 x 125 kHz channels and one 250 kHz channel between 863 to 870 MHz. Full detailed specification is available on the LoRa-Alliance website [2].

LoRaWAN (formerly known as LoRaMAC) is the specification for Medium Access Control (MAC). The specification [3] is maintained by LoRa-Alliance, a consortium with more than 500 members including companies, research institutions and universities. LoRaWAN is designed to minimize and make efficient use of energy by End-Nodes. It is also designed to communicate bi-directionally, although messages from End-Node to Network (uplink) are prioritized over messages from Network

to End-Nodes (downlink). According to LoRa-Alliance, LoRaWAN supports geo-localization of End-Nodes by the Network Server [4]. However, its feasibility is still being discussed [5].

As shown in Figure 1, there are at least 5 main components in any LoRa/LoRaWAN Topology. They are described in sections 2.2.1 to 2.2.5. Section 2.2.6 describe the dynamic of communications.

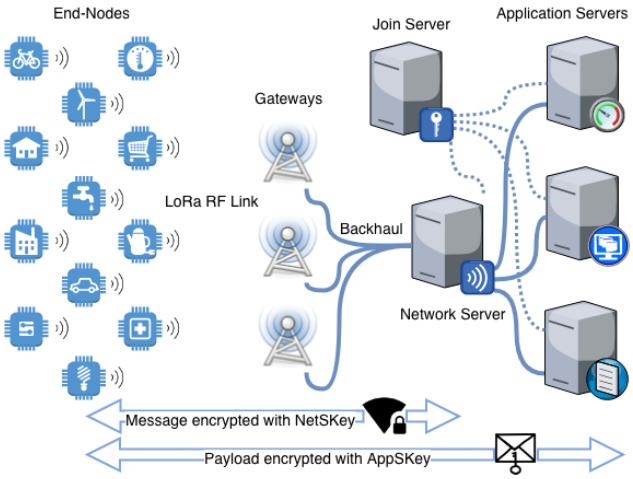

Figure 1: Lora/LoRaWAN Topology

2.2.1 End-node

An End-Node could be any electronic device, which are generally sensors, although they may be actuators as well. An End-Node has a radio module to transmit (up-link) and to receive (down-link) data through LoRa RF Link to/from Cloud. Communication is half-duplex in a specific frequency at a time.

An End-Node first encrypts the payload (usually sensor data) using Application Session Key (AppSKey). Then, it encrypts the entire message, including headers and the encrypted payload with Network Session Key (NetSKey). After these two encryption processes, the End-Node transmits the message in a LoRa packet.

2.2.2 Gateway

The Gateway is an interface between LoRa End-Nodes and the backhaul network. A LoRa interface radio module in a Gateway is used to communicate with End-Nodes through the LoRa RF Link. The LoRa interface radio module in a Gateway is more complex than its counterpart in an End-Node. It is composed of sophisticated and sensitive integrated chips, combining one or more transceivers with at least one Digital Signal Processor (DSP) capable of receiving radio signals in several channels simultaneously. Gateways are usually equipped with a Global Navigation Satellite System (GNSS) sensor which adds timestamps to the messages received.

Gateways do not interpret messages. They do not have any security key to decrypt messages. They only check packet integrity and forward the messages to the Network Server, which is connected to Gateways through a regular IP Network usually implemented over an Ethernet or cellular link. The process is reversed for messages that go from the Network Server to End-Nodes.

2.2.3 Network Server

The Network Server is the manager of network. There is only one Network Server per LoRa Network. It registers End-Nodes, Gateways, and Application Servers. The Network Server receives LoRa frames wrapped in IP packets from gateways, and sort out and discard possible duplicate messages that may be received by more than one gateway connected to the same network. It decrypts LoRa frame using NetSKey and passes the encrypted payload to the respective Application Server. When the network traffic flows in the other direction, the Network Server encrypts messages, including headers and payloads (which are already encrypted with AppSKey, by Application Servers) using NetSKey and assigns them to a gateway to be forwarded to an End-Node. Because AppSKey and NetSKey are different, the Network Server does not have access to the encrypted payloads.

2.2.4 Application Server

Application Servers (there may be more than one per network) are the final destination of encrypted payloads from End-Nodes in the LoRa system. It is worth noting that the payload transmitted and received by the LoRa system may continue its way through the cloud to a final destination where it becomes useful, such as a database or dashboard. However, that part of the IoT System is out of scope of the LoRa/LoRaWAN architecture although it can be conceptually aggregated in an Application Server. Application Servers have the AppSKey to decrypt payloads.

2.2.5 Join Server

Join Server plays a role at the beginning of communications which handles Join-Request from End-Nodes during activation stage. Join Server was added in LoRaWAN Specification [3] v1.1 to support the segregation of key management. A deep analysis of the modifications made in v1.1 can be found in [6].

There might be more components. For example, LoRaWAN v1.1 includes Home Server, Forwarding Server and Serving Server to support Roaming between networks [7].

2.2.6 Protocol Operation

LoRa/LoRaWAN protocol operation may be divide in 2 stages: Activation and Communication. Activation is a process to authorize a device to communicate in the network. A successful activation will result in a valid session. Communication occurs while the session remains valid.

2.2.6.1 Activation Stage

The goal of activation stage is to have End-Nodes and Servers (both Network and Application) agree on Session Keys. This goal can be achieved through two different methods: Activation by Personalization (ABP) or Over the Air Activation (OTAA).

In OTAA method, the End-Node and Network Server exchange a series of random numbers signed and encrypted with pre-shared keys, i.e., Network Key (NetKey) and Application Key (AppKey). After a successful handshake, both sides derive identical Session keys that will be used in Communication Stage. Session keys derived are known as Network Session Key (NetSKey) and Application Session Key (AppSKey).

In the ABP method, derived Session Keys (NetSKey and AppSKey) are pre-implanted in both sides before deploying End-Nodes. There is no handshake to derive Sessions Keys. When using the ABP method, it is unlikely that Session keys will ever change, making the sessions valid for unlimited time. Although implementation is easier, ABP method is considered less secure.

2.2.6.2 Communication Stage

Once End-Nodes are activated (with ABP or OTAA), they are authorized to communicate with Servers. With few exceptions, communications are initiated by End-Nodes, determined by the class of device. For Class A devices, an End-Node starts communication by transmitting a LoRa Packet. After a successful transmission, the End-Node opens a short receiving window to allow the Network to send a response. If no message is received, a second receiving window, which is longer, is opened. After that, it is up to the End-Node to decide when to re-start Communication Stage. It is assumed that End-Nodes are in sleep mode most of the time, with no way to receive any message from the Network during the sleep. If Network wants to communicate with End-Nodes, it has to wait until End-Nodes decide to start communication again, which may result in undetermined latency for down-link messages. Class B devices vary from Class A devices in that an End-Node opens up receiving windows periodically. Since it is assumed that End-Nodes has no accurate Real Time Clock (RTC) and they sleep during no-transmission, their receiving window timing should be synchronized by beacons sent by Gateways. Class B devices keep a balance between downlink latency and End-node energy consumption. The Class B category of devices was announced at the beginning of LoRaWAN Specification but implemented in version 1.1. Finally, Class C implements an always-open receiving window on End-Nodes. In this manner, latency can be reduced at the expense of End-Node's power consumption.

3 LPWAN Experiments at NIST

The LPWAN technology is designed for extreme efficiency in both distance and power consumption over the data rate. However, the data rate can be improved if the energy source is not limited. An experiment was designed to challenge the coverage and the data rate without restriction of energy source.

NIST has a shuttle service that transports people between the Shady Grove Metro Station and the NIST campus. The Shady Grove Metro Station is located 4.89 km (3.04 mi) *as the crows flies* from the NIST campus, as shown in Figure 2. The shuttle bus travels 10 km (6.2 mi) in 15 minutes each way. Most of the path is on local highways at speeds up to 90 km/h (60 mi/h). As shown in Figure 3 and Figure 4, this shuttle bus was used as a mobile object for the experiment and was equipped with a GSNN sensor. A Gateway and its antenna were installed on the roof of the tallest building (11 stories) on the NIST campus and in the vicinity area. Then, Network and Application server were installed on a laptop. Another computer with a large screen were used to show the location of the shuttle bus.

Figure 2: Simulated aerial view of the NIST Shuttle route area. The high-rise building in the foreground is where the gateway was deployed. In the background, the landmark points where the Shady Grove metro station is.

3.1 NIST LPWAN Facility Infrastructure

NIST LPWAN Facility was deployed using a LoRa/LoRaWAN Infrastructure. This deployment had been made before of LoRaWAN v1.1 specification was released. Thus, no Join-Server was deployed. A detail of infrastructure is described in Figure 3 and following sub-sections.

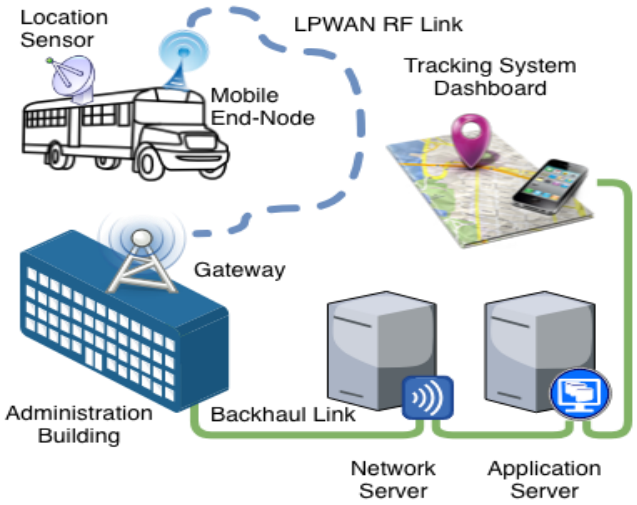

Figure 3: NIST LPWAN Testing Facility Infrastructure

3.1.1 End-Node

Each End-Node was assembled by combining a development module, Pycom FiPy, with an expansion board including a GNSS sensor Pycom PyTrack (see Figure 4). An End-Node was connected to the vehicle power source of the shuttle bus, which eliminated the issue of limitation of power supply. The antenna attached to the End-Node was a 4 dBi water-proof omni-directional antenna with magnetic base and 1.5 m cable passing through the driver's window.

End-Node software was coded in micro-Python. End-Nodes transmit in any of the 64 channels allowed in ISM US-915 specification by default. The End-Nodes were configured to use only the transmission channels covered by The Gateway. Application ID (APPEUI) and Application Key (AppKey) were also set in the End-Node software configuration. After configuration, each End-Node executed a join handshake via Over-The-Air-Authentication (OTAA) until it received a join confirmation. Finally, it ran an infinite-loop where it calculated the GPS coordinates using the GNSS location sensor and transmitted it through LoRa/LoRaWAN.

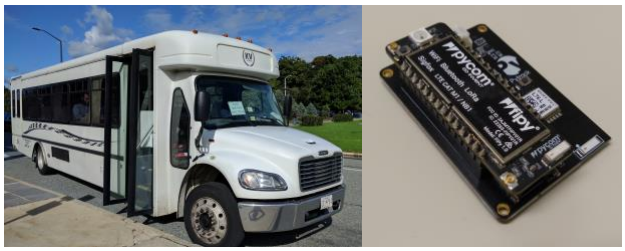

Figure 4: a) NIST Shuttle. b) Pycom FiPy + PyTrack Location Sensor

3.1.2 Gateway

The Gateway was built with a LoRa Gateway Module RisingHF RHF0M301 on top of a Raspberry Pi, as shown in Figure 5.

The LoRa Gateway Module was equipped with SX1301 + 2x SX1257, capable of covering one sub-band (8 + 1 channel) of 8 sub-bands (64 + 8) channels available in the ISM US-915 specification. The same type of antenna was used by both End-Node and Gateway. Packet-forwarder was provided by Gateway manufacturer, based on an implementation by Semtech. Packet-Forwarder was configured to communicate with Network Server. The Packet-forwarder was configured to use the operating frequency (US-915) and sub-band 1: channels 8 to 15 in 903.9 - 905.3 MHz frequency. Raspberry Pi OS (Raspbian) configuration was modified to meet the NIST IT Security policies. After that, the device was approved by NIST IT Security Officer and connected to the NIST-Net LAN Network.

This Gateway was installed inside a weather-proof box on the roof of the Administration Building which is eleven stories tall.

3.1.3 Network Server

The selection process of a Network Server was based on the same criteria as the choice of the LPWAN technology, i.e., no proprietary solutions, built-in security, possibility of ownership of the entire platform, and execution without Internet connection.

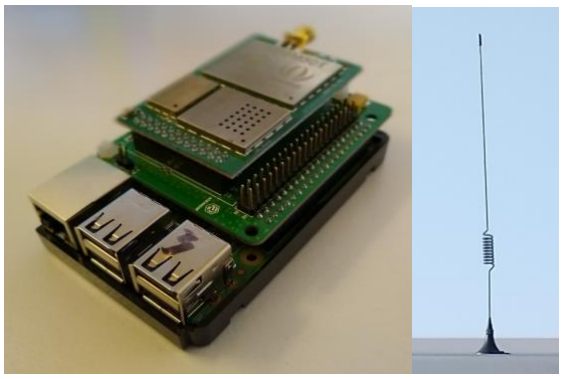

Figure 5: a) Gateway Module. b) Antenna (not in scale)

LoRa Server was selected as Network Server to be consistent with the criteria. LoRa Server software was deployed in a virtualized instance of Linux running on a Macbook Pro laptop.

Some confusion may arise from the nomenclature of LoRa Server components. Two main components in the LoRa Server project named Network Server and Application Server make up what LoRaWAN specification calls Network Server. In order to avoid ambiguity on nomenclature, "LoRaServer-" prefix is added when referring to LoRa Server project components. The functional responsibility of the network-server component (LoRaServer-network-server) is to de-duplicate and process uplink frames received by the gateway(s), to handle the LoRaWAN mac-layer, and to schedule downlink data transmissions [8]. LoRaServer-Application-Server is responsible for the device "inventory" part of a LoRaWAN infrastructure, handling join-requests as well as handling and encryption of application payloads [9].

All the administration and configuration are done via a web interface, as shown in Figure 6. Basic configuration includes: Registration and parametrization of Gateway(s), End-Node(s), and their integration to handle communication with LoRaWAN-Application-Server (the Application Server, according to the LoRaWAN specification nomenclature).

3.1.4 Application Server

The selection process of an Application Server software was based on the same criteria as the Network Server. InfluxDB [10] for data storage, combined with Grafana [11] for data visualization, were deployed in another virtualized instance of Linux, in the same Mac Laptop Host. Most of the InfluxDB configuration was done via the command-line interface except all the Grafana Configuration which was done using a web interface. A Grafana Worldmap Panel [12] was installed to show End-Point location in the map.

3.1.5 Tracking System Dashboard

A computer with a web-browser displayed on a large screen was demonstrated at SIM Week in September 2018 [13].

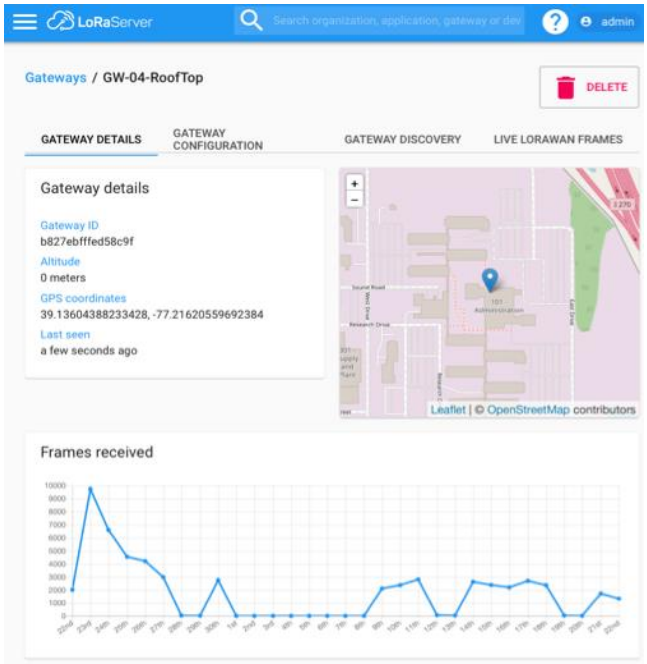

Figure 6: Gateway Status in LoRaServer. Altitude shows a wrong value due lack of GNSS sensor. Bottom graph shows frames received per day.

3.2 Experimental Tests

All tests were exploratory. The intention was to learn about LPWAN technologies from first-hand experiences, over and beyond technical references and marketing brochures. All the test should be considered preliminary and their results cannot be considered as conclusive.

3.2.1 Transmission frequency test (pre-deployment test)

This test consisted of transmitting empty packets (no payload) from the End-Node without requesting acknowledgement or delay between cycles in the loop. It was possible to receive a message almost every second under nearly ideal condition. For this test, the Gateway and the End-Node were placed inside the same room with metal walls.

3.2.2 NIST Shuttle route coverage test

Second test showed that the NIST shuttle bus could be tracked throughout almost the entire route. There were some blind spots where the transmissions were lost, possibly due to ground conditions, bridges, electrical transformers, etc. Figure 7 shows all locations where signal was received during a work day. Unlike the first test, the frequency of reception of messages decreased – once every 2 seconds to 4 seconds, if not more.

3.2.3 Latency Test

Another interesting characteristic to consider was the responsiveness of the system (Latency). Packets were received from a number of locations, but was the NIST shuttle actually at the location at the time it was displayed on the map? To answer this question, the location of the shuttle on the map was checked when the shuttle was approaching the Administration Building, while both the NIST shuttle and the map could be observed at the same time. It was confirmed that the location of the shuttle on the map was correctly displayed during this test. This was a special situation where the shuttle was moving very slowly. But it was impossible to answer that question while the NIST shuttle was traveling on highway and was out of sight. Although there are many steps involved between acquisition of the geographic coordinates by the GNSS sensors and display of the orange dot on the map, the current test solely focused on the end-to-end latency of the system as a whole.

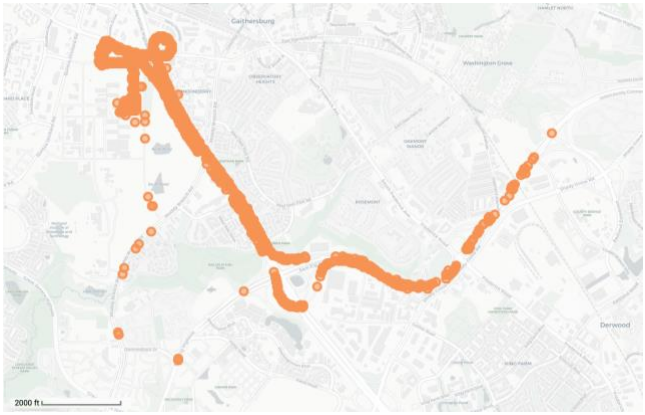

Figure 7: Accumulated locations received from the NIST Shuttle, including from unanticipated alternative routes.

In an LoRa/LoRaWAN infrastructure, the timestamp is assigned to a message by packet-forwarder software running in the gateway that receives the message. The gateway clock is synchronized with GNSS time, or with the Network Time Protocol (NTP) server in case that there is no GNSS Sensor. LoRa/LoRaWAN does not require end-nodes to have an RTC. This way, the end-nodes can be more inexpensive and more power efficient. If needed, an end-node may have an RTC to add a timestamp to sensor data. But this timestamp should be transmitted as part of the payload, which makes messages longer.

Our end-node was equipped with GNSS which could be used to add a timestamp to the location data. Unfortunately, Location Library offered by Location Sensor Manufacturer did not offer GNSS Time [14]. New libraries were developed by Pycom's user community to solve this problem, but they were not ready at the time of this test. Another option was to add a hardware RTC, but that would make the end-node more complex.

The problem was easily solved by using a separate reference system. A passenger equipped with a smartphone aboard the NIST Shuttle volunteered to help the study and reported independent real-time location data using a smart-phone LTE connection. The End-Node transmitted its location through the LPWAN setup in the NIST Facility as designed. Both location data sets were observed at the same time on the same screen. With the exception

of some lost messages, it was possible to observe a good correlation between the two data sets, as shown in Figure 8.

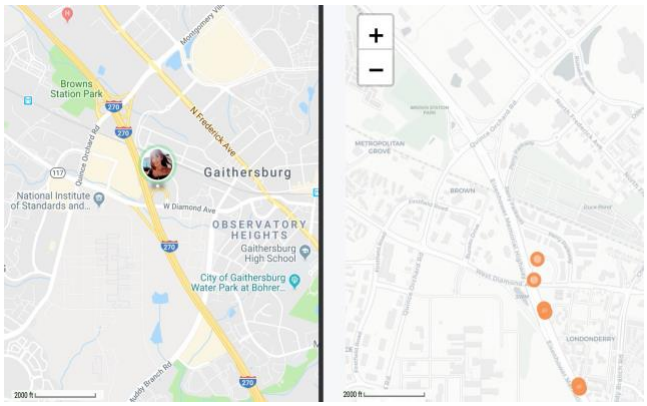

Figure 8: Side-by-side comparison. On the left, real-time location received through LTE connection. On the right, location received through the NIST LPWAN infrastructure. The upper orange dot shows the last received location, coinciding with same location reported through LTE link at that time.

3.2.4 Range test

Typical marketing brochures and white papers about wireless communications specify communication range in terms of physical distance. However, comparison of different technologies should use link-budget as the main parameter. Even with the same link-budget, communication range is seriously affected by terrain shape, weather condition, and existence of physical objects like buildings and trees that affect propagation of signal. A range test would tell us more about the context of the deployment than the technology itself.

The last test was conducted to check the communication range of a device in the LPWAN infrastructure at NIST which was deployed to cover the suburban area of Gaithersburg, MD. The End-Node was attached to a vehicle that drove around during a weekend in the vicinity of the NIST Campus. An analysis of the data during the test showed that a message from the farthest distance was received when the car was traveling on I-270 just before crossing Fall Rd Bridge, which was 8 km (5 mi) away from the gateway. Due to the characteristics of the landscape, most of the messages before that were lost even when they were transmitted at a shorter distance than the farthest location that a message was received from. The map in Figure 9 was configured to show all historical data, not just the last data point. As can be seen in Figure 9, an orange area covered almost the entire path of the Shuttle. The system ran continuously for a week.

4 Discussions

The paper described a tracking system using a LPWAN setup developed to analyze characteristics of the wireless technology. The experiment focused on a subset of important characteristics, i.e., transmission frequency, coverage, latency, and communication range. However, there are a number of additional characteristics that may have a significant impact on the overall performance of the IoT system based on the LPWAN technology. Examples includes, but not limited to, scalability, power consumption, robustness against interference, and co-existence with other types of wireless technologies. The timescale used in the latency test in this experiment was in the order of minutes and the measurement was done based on qualitative human observation. Future experiments may need to employ more quantitative measurement methods using more accurate references.

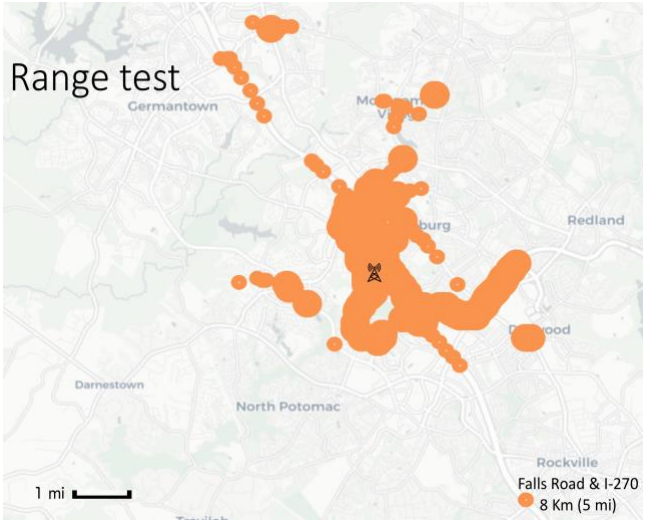

Figure 9: NIST LPWAN Infrastructure range test. The furthest received message was transmitted 8 Km far from the Gateway. Location of the Gateway is drawn on the map.

ACKNOWLEDGMENTS

Special Thanks to:

- Dhananjay *DJ* Anand, for invaluable help and support to set-up these experiments on time.
- Charles Prado, for his assistance to set up a demo.
- Jorge Carrasco, for his willingness to supervise the end-node while driving the NIST Shuttle.
- Maria Betania Antico, for sharing her smart-phone real-time location while traveling in NIST Shuttle as a volunteer passenger, and constant support in my professional development, and life.
- Nanita Yeboah, for carrying end-node during entire weekend to test LPWAN NIST Infrastructure range.
- Gurmindersingh *Gini* Khalsa, for his inspiring safety restrictions, source of inventiveness and creativity that guided me to find LPWAN.

- Héctor Laiz and Osvaldo Jalon, for trusting my professionalism to represent INTI with world-class excellence abroad.

DISCLAIMER

Official contribution of the United States government; not subject to copyright in the United States. Certain commercial products may be identified in order to adequately specify the procedure; this does not imply endorsement or recommendation by the National Institute of Standards and Technology, nor does it imply that such products are necessarily the best available for the purpose.

REFERENCES

[1] A. Ross, "Information Age's guide to the low-power wide area network (LPWAN) landscape," 27 June 2019. [Online]. Available: https://www.information-age.com/low-power-wide-area-network-lpwan-123483151/. [Accessed 25 July 2019].

[2] LoRa Alliance Technical Committee Regional Parameters Workgroup, "LoRaWAN 1.1 Regional Parameters," January 2018. [Online]. Available: https://lora-alliance.org/sites/default/files/2018-04/lorawantm_regional_parameters_v1.1rb_-_final.pdf. [Accessed 25 July 2019].

[3] LoRa Alliance Technical Committee, "LoRaWAN 1.1 Specification," October 2017. [Online]. Available: https://lora-alliance.org/sites/default/files/2018-04/lorawantm_specification_-v1.1.pdf. [Accessed 27 July 2019].

[4] LoRa Alliance Strategy Committee, "Geolocation Whitepaper," January 2018. [Online]. Available: https://docs.wixstatic.com/ugd/eccc1a_d43b3b29dfff4ec2b00f349ced4225c4.pdf. [Accessed 25 July 2019]

[5] B. Ray, "LoRa Localization," 30 6 2016. [Online]. Available: https://www.link-labs.com/blog/lora-localization. [Accessed 25 July 2019].

[6] I. Butun, N. Pereira and M. Gidlund, " Analysis of LoRaWAN v1.1 Security," in *MobiCom Mobile Computing and Networking*, Los Angeles, 2018.

[7] I. Butun, N. Pereira and M. Gidlund, "Security Risk Analysis of LoRaWAN and Future Directions," in *4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects*, Los Angeles, California, 2018.

[8] "Loraserver documentation," [Online]. Available: https://www.loraserver.io/loraserver/overview/. [Accessed 25 July 2019].

[9] "Loraserver-Application-Server," [Online]. Available: https://www.loraserver.io/lora-app-server/overview/. [Accessed 25 July 2019].

[10] "InfluxDB," [Online]. Available: https://www.influxdata.com/time-series-platform/. [Accessed 25 July 2019].

[11] "Grafana," [Online]. Available: https://grafana.com. [Accessed 25 July 2019].

[12] "Grafana Worldmap Panel," [Online]. Available: https://grafana.com/grafana/plugins/grafana-worldmap-panel. [Accessed 25 July 2019].

[13] "SIM Week," September 2018. [Online]. Available: https://sim-metrologia.org/2018/09/21/sim-week-2018-gaithersburg-september-24-28-2018/. [Accessed 25 July 2019].

[14] Pycom, "PyTrack Documentation," [Online]. Available: https://docs.pycom.io/pytrackpysense/apireference/pytrack/. [Accessed 25 July 2019].