

6-26-2018

A Viable LoRa Framework for Smart Cities

Jiaming James Chen

Queensland University of Technology, james.chen.9415@gmail.com

Jiexuan Edward Chen

Queensland University of Technology, jiexuan.chen@hdr.qut.edu.au

Vicky Liu

Queensland University of Technology, v.liu@qut.edu.au

Laurence Fairbairn

Queensland University of Technology, laurence.fairbairn@qut.edu.au

Leonie Simpson

Queensland University of Technology, lr.simpson@qut.edu.au

See next page for additional authors

Follow this and additional works at: <https://aisel.aisnet.org/pacis2018>

Recommended Citation

Chen, Jiaming James; Chen, Jiexuan Edward; Liu, Vicky; Fairbairn, Laurence; Simpson, Leonie; Wang, Charles; and Caelli, William, "A Viable LoRa Framework for Smart Cities" (2018). *PACIS 2018 Proceedings*. 59.
<https://aisel.aisnet.org/pacis2018/59>

This material is brought to you by the Pacific Asia Conference on Information Systems (PACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in PACIS 2018 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Authors

Jiaming James Chen, Jiexuan Edward Chen, Vicky Liu, Laurence Fairbairn, Leonie Simpson, Charles Wang, and William Caelli

A Viable LoRa Framework for Smart Cities

Completed Research Paper

Chen, Jiaming James

Queensland University of Technology
2 George St, Brisbane City QLD 4000
j251.chen@qut.edu.au

Liu, Vicky

Queensland University of Technology
2 George St, Brisbane City QLD 4000
v.liu@qut.edu.au

Simpson, Leonie

Queensland University of Technology
2 George St, Brisbane City QLD 4000
lr.simpson@qut.edu.au

Chen, Jiexuan Edward

Queensland University of Technology
2 George St, Brisbane City QLD 4000
jiexuan.chen@hdr.qut.edu.au

Fairbairn, Laurence

Queensland University of Technology
2 George St, Brisbane City QLD 4000
laurence.fairbairn@qut.edu.au

Wang, Charles

Queensland University of Technology
2 George St, Brisbane City QLD 4000
cc.wang@qut.edu.au

Caelli, William

Queensland University of Technology
2 George St, Brisbane City QLD 4000
w.caelli@qut.edu.au

Abstract

This research is intended to provide practical insights to empower designers, developers and management to develop smart cities underpinned by Long Range (LoRa) technology. LoRa, one of most prevalent long-range wireless communication technologies, can be used to underpin the development of smart cities. This study draws upon relevant research to gain an understanding of underlying principles and issues involved in the design and management of long-range and low-power networks such as LoRa. This research uses empirical evidence that has been gathered through experiments with a LoRa network to analyse network design and identify challenges and then proposes cost-effective and timely solutions. Particularly, practical measurements of LoRa network dependencies and performance metrics are used to support our proposals. This research identifies a number of network performance metrics that need to be considered and controlled when designing and managing LoRa-specific networks from the perspectives of hardware, software, networking and security.

Keywords: Smart cities, Internet of Things (IoT), low power wide area networks (LPWAN), LoRa, IoT security.

Introduction

The purpose of implementing a “Smart Cities” program is to improve city operations, reduce costs, increase service quality, and community engagement. The City of Ipswich in Queensland Australia has developed the “Ipswich Smart City Blueprint” and implemented its “Smart City Pilot Projects” including smart waste, smart lighting, smart parking, smart poles, smart mowing, security sensing, and environmental sensing for Ipswich City Council (2018). Ipswich was named one of the Top 7 Intelligent Communities of the World by the New York based think-tank “Intelligent Communities” forum of 2017 (Krisman). With the aim of improving the city livability, productivity and sustainability, Ipswich has been developing its Smart City Pilot Projects by harnessing various Internet of Things (IoT) technologies, such as LoRa (Long Range), SigFox and WIFI. Physically visiting the two Ipswich’s Smart City Precincts, North Ipswich Reserve and Rosewood Showgrounds, the improvements to various facets of quality of life that are realised with Smart City infrastructure are clearly tangible and there is a clear, positive view from members of the public who are affected in these test areas. The local tourism industry is also adopting Smart City solutions. The theme park “Dream World”, which is located on the Gold Coast in Queensland, is developing an IoT enabled attraction with plans to open to the public in February 2018. This is mirrored elsewhere, such as enabling a virtual tour of the forbidden city (Zhou et al. 2012) or used as development tools for accurate client models (Solmaz et al. 2015).

Various low-power wide area networking (LPWAN) technologies are available including Ingenu, Weightless W/N/P, SigFix, and LoRa (Adelantado et al. 2017; Augustin et al. 2016). LoRa Wide Area Network (LoRaWANTM) (LoRa Alliance), supported by LoRa Alliance, is a network architecture defining the network structure, behavior and communication protocol and operating on unlicensed bands. LoRa is based on the chirp spread spectrum (CSS) technique to define the wireless modulation for long-range communications at the physical layer. This research is focused on LoRa, one of most prevalent long-range wireless communication technologies, used to underpin developments of smart cities, such as environmental monitoring, smart lighting, smart parking and smart waste collection.

The key research question investigated and reported upon in this study is stated as: “Is the LoRa technology a practical solution for smart cities?” In providing a viable and holistic LoRa framework for enabling designers, developers and management to make smart cities effective and efficient, this research is aimed at gaining understanding of underlying principles and issues for LoRa network design and management from hardware, software, network and security perspectives.

This research used empirical evidence that has been gathered through a deployment and experimentation of a LoRa network to analyse the network design, identify network challenges, and then propose cost effective and timely solutions. Practical measures of network properties and performance metrics were utilised to support our proposal. Based on our findings, this research has revealed a number of network performance metrics that need to be considered when designing and managing IoT systems from security, performance and management perspectives. Interoperability with other IoT technologies is considered outside the scope of this research, as it was focused on the design and management of a LoRa network.

We consider our contribution from this research as:

1. A practical, effective and efficient network strategy for the LoRa network implementations challenges.
2. A viable LoRa framework design, specifically for signal coverage calculation, gateway placement and cost-effective hardware selection, smart gateway, communication protocol with considerable empirical evidence with testing and measurements to support our arguments.
3. Guidelines for LoRa network management in terms of understanding and administering network dependencies to achieve optimal network performance.
4. Authentic experimentation data from varied urban environments in Brisbane Australia.

This paper begins with the significance of the concept of Smart Cities with an introduction to LoRa technology and the intended contribution of this research. Secondly, it discusses the existing studies on

LoRa technology and then describes how the present study fills the gap in existing research. Thirdly, it presents our LoRa network setup with experiment design details. Fourthly, it presents challenges and solutions from our LoRa implementation. Fifthly, a holistic LoRa framework is proposed and supported by experiment results. In sixth place lessons learned during this study and undertaking are given and then finally a conclusion is drawn and future work is outlined.

Related Work

Understanding the limitations of LoRa technology is critical to the design and management of LoRa networks. Adelantado et al. (2017) detailed the characteristics and limits of LoRa/LoRaWAN in terms of the relationships between duty cycle and throughput with various packet sizes. Duty cycle defines the ratio of the time that a device can transmit data, in order to regulate signal transmission and avoid signal collisions. They described how LoRa can be used in real-time monitoring, metering, smart transportation and logistics, but not for video surveillance. As mentioned by Augustin et al. (2016), the packet payload is up to 255 bytes with a low duty cycle limit. Their study led to a number of open research challenges, particularly in channel management, such as time division multiple access over LoRaWAN and random-based access in unlicensed bands.

To design and improve LoRa network performance, understanding network-related dependencies is essential. Bor and Roedig (2017) identified more than 6000 various parameter combinations for LoRa networks and developed an algorithm for automatic selection on LoRa transmission parameters. The performance measurements on our LoRa network also were related to some of their parameter selections. Augustin et al. (2016) also studied network-related parameters for performance improvements and also measured network sensitivity and coverage. Our study proposed an appropriate strategy on gateway placement based on signal intensity and sensitivity in the context of three building density environments in Brisbane, Australia.

Elkhodr et al. (2016) reviewed various IoT communication technologies, including ZigBee, 6LoWPAN, Bluetooth Low Energy, LoRa and Wi-Fi. The capabilities and behaviours of these technologies were analyzed. Khutsoane et al. (2017) surveyed a number of various LoRa technologies applications and contended that LoRa was ideal for low-power, long-range communications where low data rates were acceptable. However, there had not been a common, comprehensive or holistic strategy for IoT network design, development and management from Elkhodr et al. and Khutsoane et al.

Petrić et al. (2016) deployed a LoRa experiment using an Arduino module and a Froggy Factory LoRa shield in the city of Rennes with their key focus on the quality of service. They measured traffic between the gateway and the end devices. The traffic generated was like that of a sensor monitoring network. They focused on an observation of the performance metrics, not on overall LoRa design and deployment. Our study fills this gap by proposing a viable LoRa framework for Smart Cities, particularly, using practical measurements of LoRa network dependencies and performance metrics to support our proposal.

Memos et al. (2017) focused on the security and privacy issues on IoT network and proposed a security scheme to protect routing in IoT networks. Their study contribution is on a design of an algorithm for surveillance systems used in Smart Cities. Mesh networks may increase the coverage areas; however, forwarding traffic to other devices through multi-hop communications increases transmission latency and routing traffic, as stated by Filho et al. (2016). Our study focused on LoRa networks which are based on a star topology with single-hop communication and no routing complexity. In particular, security complication is also alleviated and it has better throughput compared to mesh networks.

Centenaro et al. (2016) stated that LoRa is a viable solution for the deployment of a Smart City and tested LoRa coverage based on one of modulation parameters and then proposed a LoRa system architecture based on the number in a particular urban population in Italy. Our proposed architecture considered practical network coverage and signal attenuation in various building density environments.

Research Method

To develop a realistic and reliable framework it was required to empirically examine LoRa in a real-world environment. No authoritative permissions were required, as we complied with the Australian Radiofrequency Spectrum Regulations to conduct our experiments. The examination was performed in a real world exploring on a LoRa network within three varied city environments in the city of Brisbane, Australia, over a month of testing in various weather conditions:

- **Low density** (up to 2 storey) in Botanic Gardens: A public park populated with ground vegetation, water features, open grass fields and numerous trees.
- **Medium density** (3 to 8 storey) in South Bank: An entertainment precinct where buildings no higher than three stories are intermingled with open spaces, vegetation and eating areas.
- **High density** (8 storey above) in City Business District (CBD): The city centre that consists of a central business district and shopping precinct. There is an eight-storey shopping centre surrounded by a high density of buildings most of which are considered high-rises.

Experiment Design

Generally a fundamental LoRa network consists of: end devices, gateway(s) and application server(s). End devices transmit data to gateways over a single-hop and then gateways are connected to the network/application server through a high bandwidth network, such as WiFi, Ethernet or Cellular to connect. A LoRa gateway operates on minimal firmware and functions as a router to forward data between end devices and backend network/application server, as well as performing signal demodulation and protocol translation as required for interoperability. To act as a LoRa gateway requires having a transceiver capable of demodulating multiple signals/frequencies/channels simultaneously. Our LoRa network is based on a star network topology, namely all end devices are directly linked to the gateway through single-hop communications via an Ethernet link to reach the data server.

Hardware Specifications

End Device

The final end device has LoRa Chip SX1276 with a vendor provided helical antenna, Adafruit Ultimate GPS Breakout - 66 channel w/10 Hz updates, Arduino Nano and 4X AA battery case and a couple of sensors.

During the measurement all the end devices were handheld. They moved around at walking speed within the three environments and periodically broadcast packets using the 915MHz ISM band, regional regulations determining this frequency (Australian Communications and Media Authority 2017). Downlink traffic was disabled for this experiment so as to avoid network join and network management messages from the gateway causing anomalies in the data. Each end device sent its own location information to the gateway.

Gateway

The gateway consisted of one LoPy 1.0 module, with a SemTech™ SX1272 transceiver capable of receiving transmission from end devices on a single Spreading Factor which was connected via USB serial cables to a laptop. The gateway was fixed atop the 13-storey Science and Engineering building in the Gardens Point Campus at Queensland University of Technology in Brisbane Australia.

Challenges and Solutions in Our LoRa Implementation

This section outlines challenges that were encountered and the solutions implemented. They were categorised into the following areas: hardware, software, network, and data Fidelity.

Hardware

The LoRa gateway with the SemTech™ SX1301 chipset can scan/demodulate on multiple frequency channels simultaneously; however, such products in the market are often expensive and "hard-coded" (not programmable) on the device. Cutting down the costs of IoT implementation, the hardware used for end devices and gateways must be conscientiously considered. Instead of using a transceiver SX1301 chipset for our LoRa gateway, we chose to use the SemTech™ SX1272 transceiver chipset for the LoRa gateway as a cheaper alternative. The SX1272/6/8 chipset can only scan one spreading factor on one frequency channel at a time. For a small network deployment, using the SX1272/6/8 chipset for the transceiver of LoRa gateway is a cost-effective solution; however, for large scale networks, SX1301 chipsets could be used for much higher throughput.

Initially, we used Arduino Uno microcontrollers (cost of 1 @ AUST\$35) and LoRa shields for Arduino (cost of 1 @AUST\$33). To reduce the overall cost of end devices, we chose Arduino Nano microcontrollers (cost of 1 @AUST\$3) with SemTech™ SX1276 transceivers (cost of 1 @AUST\$5). Arduino Nano and Uno have a similar capacity in terms of CPU and memory. The cost for each end device was reduced from AUST\$68 to AUST\$8. With a massive IoT deployment, this has a significant difference on deployment costs.

Any microcontroller has a physical limitation when it comes to connecting various sensors. The number of sensors that can be connected to the microcontroller depend on the number of I/O pins on the microcontroller. Instead of purchasing a greater capacity microcontroller with more of I/O pins, unused analogue pins can be used as digital outputs by changing the value of the pin mode in the pre-existing code, from analog (A0) to digital (D0) in the code. This was sufficient for our testing; however for a greater range of sensor inputs, adding a breakout board on top of microcontroller would be necessary. A breakout board can provide a plug-and-play feature to integrate more sensors, control elements or output devices.

The limited memory on the end devices would restrict the number of sensors that could transmit data at any one time. As we needed various types of data transmission at the same time, we merged two end devices as one. One end device was used for collecting data from the sensors and another was used for data transmission. Alternatively, a greater memory capacity for end devices could be deployed, such as an Arduino Mega microcontroller, or an additional external memory module inserted, if the budget allows.

Firmware and Software

Various sources encourage the use of the latest firmware updates. Firmware automatic update and installation may be enabled by default, yet this feature can cause serious operational and firmware incompatibility dilemmas. During our implementation tests, the firmware updates based on LoPy modules on the gateway did cause an operational and incompatible problem. To avoid firmware update failures, one must backup the previous version and test extensively for compatibility with the new version prior to a network wide update. Thus, it is essential to keep the previous version of firmware, in case a firmware rollback is required.

When running a Python script that used vendor provided libraries to read the data from a LoPy over serial ports, data corruption occurred due to how memory allocation is handled in Python. Once the code was rewritten in C# this issue was resolved.

There were multiple Arduino libraries required for sensor function, however they were incompatible with each other. In addition to this it was found that the libraries had inconsistent code quality and inefficient memory concerns. This was solved by re-writing the necessary functions and optimising for memory management and interoperability.

Network

The primitive nature of the LoRa network meant that no physical addressing scheme is used and communications are anonymous. To have a more meaningful experiment data media access control

(MAC) addressing was implemented and the identity of the sender and receiver were added to the header of LoRa data packets.

Antennas come in various forms and types. Selecting an appropriate antenna is crucial for optimal wireless network performance. Specifically, the type and length of an antenna have an effect on the strength of a signal and directionality that can be transmitted and received. Initially, we used the vendor provided helical antenna for our end devices, but that had weak signal reception. We soldered our own quarter-wavelength monopole antenna to replace the vendor provided helical antenna on the end device, and found ~10dB more powerful than the helical antenna. To visualise the signal strength coverage, this study used Heatmaps (Figures 1 – 3) with three levels to define measurements of received strength signal indicator (RSSI): red for strong signals $>-100\text{dBm}$, yellow for medium signals $-100\text{dBm}\sim-125\text{dBm}$, and green for weak signals $<-125\text{dBm}$. Figure 1 shows the monopole antenna presents better signal quality and strength than the helical antenna, when signal coverage was measured in the area of Southbank, Brisbane, Australia.

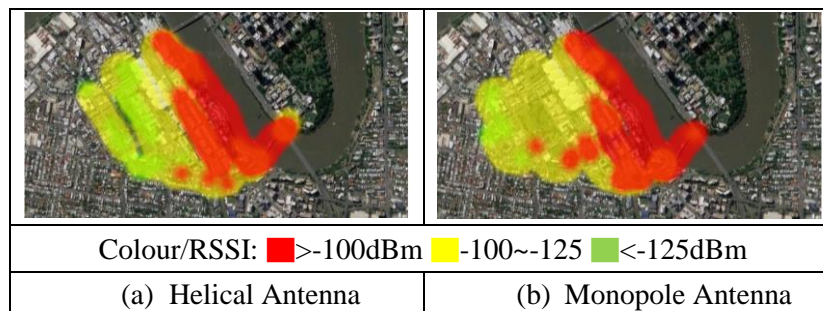


Figure 1. Signal Strength for Helical and Monopole Antennas.

Data Fidelity

Originally we used the vendor provided software to transmit data with no error-detecting function, namely cyclic redundancy check (CRC). Signal pollution occurred, owing to environmental interference, as shown in Figure 2 (a). Then we added a CRC function into the message that ensures that the gateway could identify the traffic that belonged to its network, are shown in Figure 2 (b). As such, a CRC must be included in the signals at source node to detect noise and other burst errors that is introduced into data during transmission.

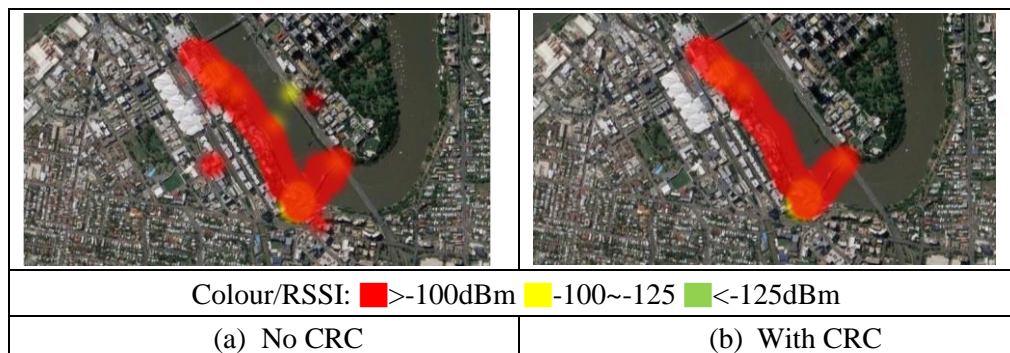


Figure 2. Signal Tests with no CRC and CRC

Proposed LoRa Network Framework

There are a number of considerations when designing smart city infrastructure that focuses on long range networks. We proposed a viable framework based on LoRa as practical guidance for design and delivery of smart city solutions from network design and network management perspectives.

Network Design

Understanding the characteristics of LoRa is the first step to design and manage LoRa networks. The key features LoRa include: long-range connectivity, low-power consumption, low bandwidth, high network capacity for connecting up to a million network nodes and high link budget (the expected received signal to noise ratio) and high-interference immunity. Unlike mesh networks which forward traffic to gateways through multi-hop communications, LoRa is based on a star topology with single-hop communication to reach gateways. LoRa is a low-throughput communication technology with low data rates up to 0.3 ~ 27 kbps (Adelantado et al. 2017); however, it is not a suitable candidate for frequent transmission of large data blocks.

LoRaWAN (LoRa Alliance, 2015) is a star of stars network architecture by which end devices send data through gateway(s) over a single hop then the gateway(s) forwards data between end devices and a network server. According to the LoRaWAN specification, gateways are only a transparent bridge (namely a forwarder); the intelligence, security checks and complexity is performed at a network server. A potential risk of such a network architecture is that the network bandwidth may be clogged as result of a massive amount of unfiltered and uncontrolled data transmitted from end devices. This study proposes that smart gateways can perform some tasks to reduce network traffic to avoid inundating network bandwidth and a network server. That is, smart gateways can examine, filter/aggregate and process received data from end devices before the data is transferred to the backend server. Additionally, smart gateways can be equipped to perform a number of security functions, such as authentication, uplink and downlink traffic control, security validation and defence. Such a proposed design and implementation will be further detailed in a forthcoming paper.

Hardware Selection

Two transceiver chipsets are widely used for LoRa networks: Semtech™ SX1276 and SX1301. The main difference between these two chipsets is that SX1276 can only scan one channel and demodulate one spreading factor at a time. SX1301 can scan eight channels, all spreading factors with eight demodulators simultaneously in half-duplex. Generally, SX1301 is suitable to be used as a transceiver for a LoRa gateway, SX1276 is as a transceiver for an end device. SX1276, however, can be also used as a transceiver for a gateway, as an affordable solution. A gateway with a SX1276 chipset containing a demodulator can serve up to 1,000 end devices, when the duty cycle is 0.1%. A gateway with one SX1301 chipset can serve up to 8,000 end devices, when the duty cycle is 0.1%. The throughput of SX1301 is, therefore, eight times more than SX1276. When end devices exceed more than 8000, we recommend that aggregating multiple SX1276 chipsets for a gateway to enable scanning and demodulating on multiple frequency channels simultaneously. This research originated a formula (1) to calculate the number of end devices served by a gateway using multiple SX1276 chipsets, namely

$$\text{Number of end devices} = \frac{N}{\text{duty cycle}} \quad N \in [9,48]; N \text{ is the number of demodulator(s)} \quad (1)$$

The reason we designated the range of demodulators 9 to 48 for SX1276 is because that 9 demodulators are more than the maximum demodulators of SX1301. As a LoRa frequency bandwidth is divided into 8 physical channels, each channel can use spreading factors of 7 to 12; namely 8 uplink channels * 6 spreading factors to achieve 48 virtual channels. For example, a LoRa gateway with 48 SX1276 chipsets can serve up to 48,000 end devices within these virtual channels when the duty cycle is 0.1%. Such a capacity aggregation, with multiple SX1276 transceiver chipsets can maximise the network capacity allowing the transmission of two signals simultaneously in uplink and downlink directions. This can result in achieving higher throughput, avoiding single-point of failure and increasing network performance, compared to just using a SX1301 chipset for a gateway.

Gateway Placement

The placement of gateways and end devices can affect the network coverage and connection quality. When possible, a gateway is placed on a raised or elevated structure and end devices surround the

gateway. LoRa is designed for long range communications and can achieve 2-5 km in urban areas and 15 km in suburban areas (Adelantado et al. 2017).

We conducted signal coverage tests in three real world environments: high-density (HD), medium-density (MD) and low-density (LD) building environments with Spreading Factor (SF) 12 and Bandwidth (BW) 125 kHz. Figure 3 depicts the intensity of signal strength in these three environments. The white dash lines represent the testing covered area, the areas of high signal intensity are coloured in red and the areas of lower signal intensity coloured in green.

In the high-density building environment, numerous obstacles cause shadowing, multipath, fading effects, significant signal attenuation. As a result, the percentage of packet loss in this environment is the highest and the intensity of the signal attenuation is the most obvious, comparing to the other two environments. In Figure 3 (a), the uncoloured area within the white dash range shows a lack of signal reach. In Southbank (MD) the packet loss rate is 37.5% while Botanic Gardens (LD) has the best signal intensity with the packet loss only 1.796%, as shown in Figure 3 (b) and (c). The test results indicate that the type of physical environment has a significant impact on signals propagation and attenuation as well as gateway placement, as radio waves can be absorbed by objects in their path, resulting in power loss and limiting transmission distance.

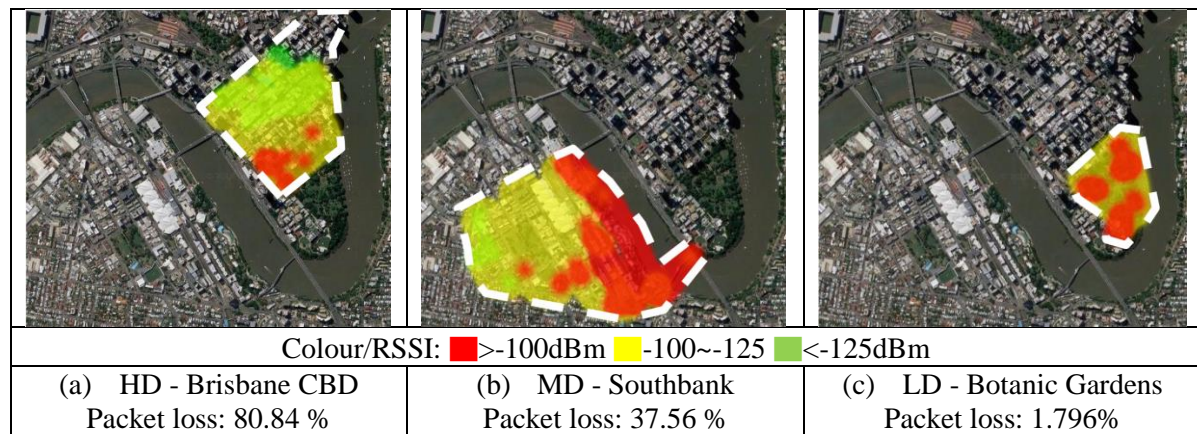


Figure 3. Intensity of Signal Strength in Three Environments

The tests conducted from this research contribute a calculation of the Expected Path Loss (attenuation) and estimated maximum transmission distances between the gateway and end devices.

Calculation (2) of the Expected Path Loss is based on the Measured Path Loss (Petajajarvi et al. 2015)

$$\text{Measured Path Loss} = |\text{RSSI}| + \text{SNR} + P_{\text{Tx}} + G_{\text{Rx}} \quad (2)$$

where RSSI is the Received Signal Strength Indicator, SNR is the Signal-to-Noise Ratio, P_{Tx} is the effective isotropic radiated power and G_{Rx} is receiver's antenna gain.

Expected Path Loss (EPL) can be calculated (3) using the following formula (Petajajarvi et al. 2015)

$$\text{EPL} = B + 10n \log_{10}(d/d_0) \quad (3)$$

where B is the a constant which accounts for system losses, n is the path loss exponent, d is the distance between the gateway and end devices (measured in meters) and d_0 refers to a 1000-meter reference distance.

As shown in Figure 4, the Measured Path Loss (marked with black dots) is calculated based on the transmitted packets received at the gateway, containing geographical positioning, RSSI and SNR. Based on the black dots, we can build and train the signal attenuation model (or EPL) to form the solid red curves for these three different environments. Meanwhile, the Path Loss Threshold is determined by the maximum value of the Measured Path Loss, according to the analysis of received packets (Figure 4). After obtained the Path Loss Threshold and the EPL, we can estimate the maximum transmission distance between the gateway and end devices. Actually, the estimated maximum transmission distances tested from the high density in Brisbane CBD and medium density in Southbank are 1321

meters and 1879.95 meters. We, however, were unable to estimate the maximum transmission distance for low density in Botanic Gardens, owing to its restricted physical area.

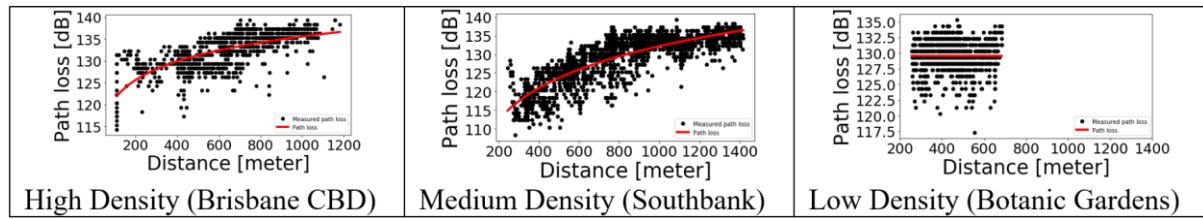


Figure 4. Measured and Expected Path Loss in Three Different Environments

When designing to extend the existing coverage to other areas, one must appreciate the existing signal coverage and then survey the most appropriate gateway position with the same method mentioned above.

Communication Protocol

We defined a new message format for communications between end devices and a gateway involving the authentication and data transmission process. Our proposed LoRa uplink and downlink messages carry two layers of messages: (1) Application layer and (2) Media Access Control (MAC) layer, as shown Figure 5.

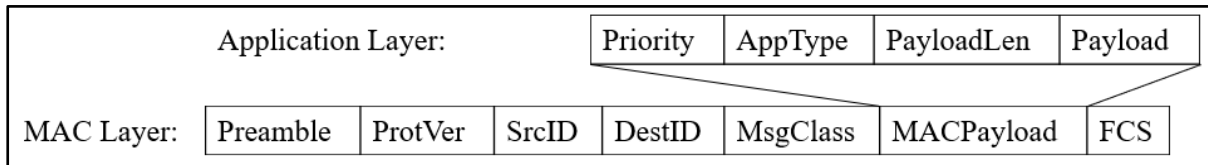


Figure 5. Message Format

1. Application layer messages contain the following fields:
 - 1.1 Priority (Priority): This 4-bit field defines the priority of the message should be delivered.
 - 1.2 Application Type (AppType): This 8-bit field identifies the type of application service.
 - 1.3 Payload Length (PayloadLen): This 8-bit field defines the entire payload size in bytes.
 - 1.4 Payload (Payload): The maximum length of payload is up to 233 bytes.
2. MAC layer messages contain the following fields:
 - 2.1 Preamble (Preamble): The preamble consists of an 8-bit field of alternating 1 and 0 bits, allowing devices on the network for synchronization.
 - 2.2 Protocol Version (ProtVer): This is an 8-bit protocol version field.
 - 2.3 Source Identification (SrcID): This 64-bit field is the addressing of the sender.
 - 2.4 Destination Identification (DestID): This 64-bit field is the addressing of the receiver.
 - 2.5 Message Classification (MsgClass): This 4-bit field indicates the type of the message:

0000: Join request	0101: Confirmed data uplink
0001: Join accept	0110: Confirmed data downlink
0010: Join acknowledgement	0111: Data uplink acknowledgement
0011: Unconfirmed data uplink	1000: Data downlink acknowledgement
0100: Unconfirmed data downlink	1001: Reserved for future use
 - 2.6 Frame Check Sequence (FCS): This is a 16-bit cyclic redundancy check (CRC) field that enables detection of corrupted data for the entire frame.

LoRaWAN (LoRa Alliance 2015) defines that a gateway is a transparent bridge to transfer data between end devices and a network server. The intelligence and complexity are performed at the network server, namely a gateway operates as a forwarder. Whereas we proposed a smart gateway that can reduce

network traffic generated from end devices and can provide authentication, data filtering/aggregation, delivery priority, and incident response functions. The data flow between the end device, gateway and network server is described as follows (Figure 6).

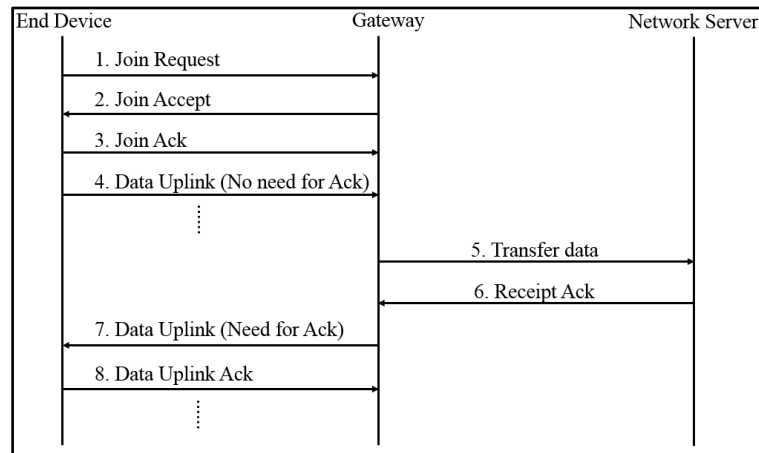


Figure 6. Communication Flow

1. The end device initiates the communication process with a Join Request message.
2. The gateway authenticates the end device and then returns a Join Accept message.
3. The end device acknowledges the response from the gateway.
4. The end device transmits data to the gateway with no need for acknowledgment.
5. The gateway interprets the received data, and then examines/filters/aggregates the received data. In turn, the gateway transfers the processed data to the network server, based on the priority marked on the received data.
6. The network server sends an acknowledgement to the gateway on receipt of transferred data.
7. The end device transmits data to the gateway with need for acknowledgment.
8. The gateway sends an acknowledgement to inform the end device of the data being received, if the received data is marked with need for acknowledgement.

With a large scale network, a network structure can be divided into separate cluster networks. The gateways from each cluster network form a hierarchical structure to communicate with the backbone network.

Security

Smart Cities consist of interconnected complex systems and networks. This creates numerous security risks and challenges and an exploited vulnerability in this system could have catastrophic ramifications. All too often, cybersecurity is an afterthought and has been left out of the system development life cycle and this could create a system wide vulnerability. A massive number of insecure and unprotected IoT devices may be recruited as botnets to launch distributed denial-of-service (DDoS) attacks. This can lead to potential disruption to critical infrastructure, interruption of business operations, theft of sensitive data and loss of consumer privacy or other malicious activities. It is, therefore, imperative to incorporate security into IoT ecosystem design and development, regardless of whether the IoT network is used to gather sensitive data or not. One of the approaches to mitigate DDoS attacks to IoT networks is to limit IoT ecosystems exposure to IP-based communications. LoRa is not an IP-based network, so it does not have IP-based communication from end devices to the LoRa gateway. Thus, IP-based attacks are not able to compromise LoRa networks.

Information security requirements and functions can be commonly addressed from confidentiality, integrity and availability (CIA) aspects. Similarly, this study argued that security for IoT network architectures can be designed and enforced from the CIA perspectives.

In case of confidentiality and integrity, sensitive data gathered prior to transmission should be digitally signed and encrypted. Digital signing and encryption mechanisms can and should be used to achieve data confidentiality and integrity in transit for end-to-end security against threats based on eavesdropping as well as message protection against impersonation, substitution or spoofing. The cryptography used for general computing to achieve confidentiality and integrity may not be feasible for resource constrained IoT devices. This research suggests that lightweight cryptography can be applied on resource constrained IoT devices. Alternatively, a Trusted Platform Module (TPM), standardized by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) as ISO/IEC 11889, can be embedded into end devices and gateways as an encryption/decryption and digital signature solution. In addition, it provides a key management scheme to provide confidentiality and integrity security projection. TPM is physically separated from the on-board microcontroller. If the encrypted data with TPM has been read, it cannot be decrypted. The chipset stops functioning when it is removed from the end device once installed.

In terms of increasing availability, this study proposed that aggregating more than eight SX1276 transceiver chipsets for a LoRa gateway to scan and demodulate on more than eight frequency channels side by side, rather than just using one SX1301 transceiver chipset for a LoRa gateway to scan and demodulate eight channels, as mentioned in the hardware selection section previously. Such a proposed approach can result in provisioning:

- **Redundancy:** avoiding single-point of failure when one transceiver chipset becoming unavailable does not affect the rest network operations
- **Higher throughput:** enabling more end devices to communicate with the gateway simultaneously
- **Full-duplex:** allowing multiple messages in uplink and downlink directions concurrently.

Owing to paper-length limitations, the overall security architecture is described more detail in a forthcoming paper.

Network Management

This section reveals a number of network performance parameters that need to be considered and managed when designing and managing LoRa-specific networks effectively and efficiently.

Network Performance Dependencies

To optimize network performance, transmission parameters such as Carrier Frequency, Spreading Factor, Bandwidth and Code Rate must be managed between end devices and gateways (Adelantado et al. 2017; Augustin et al. 2016; Bor and Roedig 2017).

- **Carrier Frequency (CF)** is a central frequency between the upper and lower frequencies. CF depends on the regional regulations.
- **Spreading Factor (SF)** is a parameter in modulation, defined as $SF = \log_2 \frac{R_c}{R_s}$, where R_c is the chip rate and R_s is symbol rate. The range for SF is between 7 and 12.
- **Bandwidth (BW)** is the width of frequencies in the transmission band. The three typical configurable Bandwidth options are 125 kHz, 250 kHz and 500 kHz.
- **Code Rate (CR)** is the Forward Error-correction Code rate used by LoRa modem that protects from burst of interference. The four valid Code Rates are $\frac{4}{8}$, $\frac{4}{7}$, $\frac{4}{6}$ and $\frac{4}{5}$.

To effectively and efficiently manage LoRa networks, the key parameters of LoRa network performance must be understood and administered appropriately. This study analysed the relationships between the LoRa network performance parameters and their impacts on sensitivity, power consumption and data rate. For example:

- In order to improve signal coverage (sensitivity), a common approach is to increase SF and/or decrease BW. As SF increased and BW decreased, this leads to a lower data rate as well as causes

more power consumption. It is, therefore, not recommended to tune SF to the highest level and BW to lowest range for a maximum of signal coverage.

- In conserving power consumption, SF needs to be low and BW and CR need to be tuned high.
- To accelerate the transmission rate (or data rate), the spreading factor needs to be low, bandwidth and code rate can be increased.

The comparative analysis between SF, BW, CR against sensitivity, power consumption and data rate is summarised in Table 1.

Table 1. Network Performance Dependencies (↑ = increased ↓ = decreased)

	Sensitivity	Power Consumption	Data Rate
Spreading Factor (SF)	↑	↑	↓
Bandwidth (BW)	↓	↓	↑
Code Rate (CR)	NULL	↓	↑

CRC and Power Consumption

An experiment on CRC sizes of 8 bits, 16 bits and 32 bits was done to test power consumption, as this could impact on the battery lifetime of an end device. In a laboratory, power usage of the end device was measured while 2500 packets were sent using each of the CRCs. This study calculated the power consumption and estimated the impact on battery lifetime on the IoT device, as shown in Table 2. It is assumed that the payload size is 50 bytes without CRC.

Table 2. Power Consumption Comparison for n-bit CRC

	No CRC	CRC8	CRC16	CRC32
Packet Length (Bytes)	50	51	52	54
Power Consumption (Joule)	381.4	382.8	384.6	399.5

This study proposed power consumption measurement is based on the following equations (4) & (5)

$$\text{Transmitted packets allowance per day} = \frac{\text{Number of seconds per day}}{\text{Time-on-air} \div \text{Duty Cycle}} \quad (4)$$

The Duty Cycle varies, it is assumed that a Duty Cycle 0.1% and Time-on-air 70 milliseconds, a packet can be sent every 70 seconds. This infers 1,234 packets can be sent within a day or 450,410 packets per year. For instance:

$$\frac{(60 \times 60 \times 24) \text{ seconds/day}}{70 \text{ seconds/packet}} = 1234 \text{ packets/day}$$

When CRC16 is used, transmitting each packet spends $384.6 \div 2500$ Joule, which is 0.15384 Joule/packet. Based on 0.1% Duty Cycle and 70ms Time-on-air, the average AA battery containing 7228 Joule can be power on the end device.

$$\text{Power supplied days} = \frac{\text{Power Capacity}}{\text{Power consumption each packet}} \div \text{transmitted packets allowance per day} \quad (5)$$

For example, when CRC16 was used:

$$\frac{7228 \text{ Joule}}{0.15384 \text{ joule/packet}} \div 1234 \text{ packets/day} = 38.06 \text{ days}$$

An end device powered by an AA battery can be supplied for up to 38.24 days with CRC8, 38.06 days with CRC16, 36.64 days with CRC32, or 38.39 days with no CRC.

The power consumption with CRC32 is just too aggressive. CRC16 has fewer collisions than CRC8 and similar power consumption. As result, CRC16 is a feasible option for deployment.

Firmware and Software

In place of broadcasting firmware updates to each device over the network, this research proposed a creation of classification and labelling based on device types to enable a fine-grain management for firmware upgrades, with a better bandwidth usage in mind. Additionally, creating control and data channels, control channels are for upgrading firmware and carrying commands, which are separated from data transfer.

As the number of integrated devices in a Smart City solution could exceed a million, in situ software updates are not ideal and, in some cases, not feasible. Over-the-Air (OTA) software and firmware upgrades are a much more desirable option, as they require no physical access to any network enabled devices.

A key challenge with OTA updates for a LPWANs is the management of the large file sizes, power consumption, transfer rate and pack loss. It is suggested that fragmenting the files, synchronizing the update windows across all end devices, repeating the file transmission to avoid packet loss complications and verifying file authenticity can meet that challenge. Such a method for examining the integrity of the files could also be applied in a more generalised case for data redundancy and checking and garbage collection in software programming.

Lesson Learned

Prior to the beginning of testing, assumptions were made regarding the scope of work that was required to develop the hardware ready for testing. Initially it was planned to deploy off-the-shelf hardware modules. However, we realised that this hardware decision was prohibitive when considering the research budget. A decision was made to purchase the individual components and solder up the hardware, as this saved AUD\$79 per end device. This would be vital for future research where the savings would enable the deployment of a massive number of end devices. This decision, however, created several problems that were encountered during this study:

- The vendor provided code was immaturely written and unintuitive to understand. The lack of common coding conventions and practices highlighted that the code was written by hardware engineers and not software engineers. This increased the amount of time spent editing the code to make each chipset interoperable with the rest of the end device.
- Security was not provisioned by IoT vendors as well as digital signing for integrity and encryption for confidentiality was not provided. This required methods to be developed instead of adapting the ones provided by the vendors, so they would be scalable for Smart City infrastructure.
- The interdisciplinary skills required to design and troubleshoot an IoT project were underestimated. Researchers were required to upskill to meet the required milestones.
- Practical measurements of LoRa network dependencies and performance metrics must be understood and considered when designing and managing IoT ecosystems from network, hardware and software as well as network performance and management perspectives.

Overall, the decision to deploy custom designed end devices instead of using the off-the-shelf hardware enabled us to test LoRa without having to make concessions due to vendor propriety.

Conclusion and Future Work

This research investigated the practicality of LoRa implementation for Smart Cities. It was determined that LoRa is practical for Smart Cities. LoRa can be used to meet the requirements for long-range and low-cost IoT applications, and provides robustness against interference in a noisy environment. This study concluded that: (1) LoRa can be operated successfully in dense urban areas against noisy environments; (2) LoRa is a flexible technology that can be fine-tuned by varying parameters, such as spreading factor, code rate and bandwidth, to achieve optimal network performance. Existing LoRa infrastructure was used in empirical evidence-based experiments, the results of which informed the design decisions regarding a standardised LoRa framework for Smart City solutions. A generalised

framework was realistic as most Smart City projects will share scope constraints. Our framework provides guidelines for a practical and deployable LoRa-based solution that Smart City stakeholders can further customise for their needs. Owing to resource limitations, this study only conducted experiments on signal coverage within Brisbane and tested power consumption on 8/16/32-bit CRC to evaluate the impact on the battery lifetime. The LoRa networks can be further investigated from security, performance and manageability perspectives.

Moving forward, we plan to continue this research in the area of IoT network performance and security. We will test lightweight IoT specific security options that will inform an update to the framework proposed in this paper. It is also planned to implement a LoRa network with one hundred end devices and multiple smart gateways. This deployment will be used to research and test communication between the gateways and the server with key interest around reliability and efficiency. There is also a possible opportunity to work with the City of Ipswich to further develop their Smart City Blueprint in preparation for a larger scale deployment.

Acknowledgements

The authors thank Matthew Schultz from the Ipswich City Council for providing the information on Ipswich Smart City Projects and enabling us to visit the Ipswich Smart City Precincts.

References

- Adelantado, F., Vilajosana, X., Tuset-Peiro, P., Martinez, B., Melia-Segui, J., and Watteyne, T. 2017. "Understanding the Limits of LoRaWAN," *IEEE Communications Magazine* (55:9), pp. 34-40.
- Augustin, A., Yi, J., Clausen, T., and Townsley, W. 2016. "A Study of LoRa: Long Range & Low Power Networks for the Internet of Things," *Sensors* (16:9), p. 1466.
- Australian Communications and Media Authority. 2017. "Australian Radiofrequency Spectrum Plan 2017."
- Bor, M., and Roedig, U. 2017. "LoRa Transmission Parameter Selection," *2017 13th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 27-34.
- Centenaro, M., Vangelista, L., Zanella, A., and Zorzi, M. 2016. "Long-Range Communications in Unlicensed Bands: The Rising Stars in the IoT and Smart City Scenarios," *IEEE Wireless Communications* (23:5), pp. 60-67.
- Elkhodr, M., Shahrestani, S., and Cheung, H. 2016. "Emerging Wireless Technologies in the Internet of Things: A Comparative Study," *International Journal of Wireless & Mobile Networks (IJWMN)* (8:5).
- Filho, H. G. S., Filho, J. P., and Moreli, V. L. 2016. "The Adequacy of LoRaWAN on Smart Grids: A Comparison with Rf Mesh Technology," *2016 IEEE International Smart Cities Conference (ISC2)*, pp. 1-6.
- Ipswich City Council. 2018. "Ipswich Smart City." Retrieved 27/02/2018, from <https://www.ipswichsmartcity.com.au/>
- Khutsoane, O., Isong, B., and Abu-Mahfouz, A. M. 2017. "IoT Devices and Applications Based on LoRa/LoRaWAN," *IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*, pp. 6107-6112.
- Krisman, V. "Ipswich in World's Top 7 Intelligent Communities." Retrieved 27/02/2018, from http://www.intelligentcommunity.org/ipswich_in_world_s_top_7_intelligent_communities
- LoRa Alliance. "A Technical Overview of LoRa and LoRaWAN." Retrieved 27/02/2018, from https://docs.wixstatic.com/ugd/eccc1a_ed71ea1cd969417493c74e4a13c55685.pdf
- Memos, V. A., Psannis, K. E., Ishibashi, Y., Kim, B.-G., and Gupta, B. B. 2017. "An Efficient Algorithm for Media-Based Surveillance System (Eamsus) in IoT Smart City Framework," *Future Generation Computer Systems*.
- Petajajarvi, J., Mikhaylov, K., Roivainen, A., Hanninen, T., and Pettissalo, M. 2015. "On the Coverage of LoPwans: Range Evaluation and Channel Attenuation Model for LoRa Technology," *2015 14th International Conference on ITS Telecommunications (ITST)*, pp. 55-59.
- Petrić, T., Goessens, M., Nuaymi, L., Toutain, L., and Pelov, A. 2016. "Measurements, Performance and Analysis of LoRa Fabian, a Real-World Implementation of LoPwan," *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1-7.
- Solmaz, G., Akbaş, M. İ., and Turgut, D. 2015. "A Mobility Model of Theme Park Visitors," *IEEE Transactions on Mobile Computing* (14:12), pp. 2406-2418.
- Zhou, Y., Yang, L., and Shen, M. 2012. "From the Virtual Forbidden City to the Dream Wizard City: Virtual Tourism Landscape Design and Internet of Things Technology for Embedded Applications," *Journal of Guilin Institute of Tourism*(3), pp. 27-31.