IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 21, 2019, accepted January 13, 2020, date of publication January 20, 2020, date of current version January 28, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2968057

Low-Power Wide-Area Networks: Design Goals, Architecture, Suitability to Use Cases and Research Challenges

BEN BUURMAN, JOARDER KAMRUZZAMAN, (Senior Member, IEEE), GOUR KARMAKAR, (Member, IEEE), AND SYED ISLAM, (Fellow, IEEE)
School of Engineering and Information Technology, Federation University Australia, Churchill, VIC 3840, Australia

Corresponding author: Joarder Kamruzzaman (joarder.kamruzzaman@federation.edu.au)

ABSTRACT Previous survey articles on Low-Powered Wide-Area Networks (LPWANs) lack a systematic analysis of the design goals of LPWAN and the design decisions adopted by various commercially available and emerging LPWAN technologies, and no study has analysed how their design decisions impact their ability to meet design goals. Assessing a technology's ability to meet design goals is essential in determining suitable technologies for a given application. To address these gaps, we have analysed six prominent design goals and identified the design decisions used to meet each goal in the eight LPWAN technologies, ranging from technical consideration to business model, and determined which specific technique in a design decision will help meet each goal to the greatest extent. System architecture and specifications are presented for those LPWAN solutions, and their ability to meet each design goal is evaluated. We outline seventeen use cases across twelve domains that require large low power network infrastructure and prioritise each design goal's importance to those applications as Low, Moderate, or High. Using these priorities and each technology's suitability for meeting design goals, we suggest appropriate LPWAN technologies for each use case. Finally, a number of research challenges are presented for current and future technologies.

INDEX TERMS Low power wide area network (LPWAN), Internet of Things (IoT), design goals, MAC layer, channel access, long range, scalability, data rate, licensed and unlicensed band, operational lifetime.

I. INTRODUCTION

Since the concept of the Internet of Things (IoT) was introduced to the scientific and commercial world, it has grown at a rapid pace. It has been estimated over 30 billion devices will be connected by 2020 [1] with the global market for IoT valued at 267 billion USD [2].

IoT has traditionally relied on short-range radio protocols such as ZigBee and Bluetooth or leveraged off existing networks such as cellular and Wi-Fi. These are sufficient for short-range IoT systems but are unsuitable for large and geographically spread networks of things, needed for many industrial and commercial applications. Short-range radio protocols are energy-efficient but limited by their transmission coverage range. Cellular networks are capable of long-range communications but are both expensive and power consuming. Wi-Fi is relatively inexpensive but is power consuming and limited by range.

Since the widespread rise of IoT devices requires energy-efficiency and long-range communication, it demands inexpensive, energy-efficient IoT networks capable of long-range communications. Low Power Wide Area Networks (LPWANs) fulfil these requirements, often at the expense of more 'traditional' network requirements such as latency and throughput. These more specific requirements such as low power consumption and long range form the design goals of LPWAN networks. LPWANs are intended to coexist with existing short-range radio and cellular IoT networks, however choice of particular network(s) depends on the individual user or application.

A few studies in literature have provided comparisons between LPWAN solutions, including the works of Raza *et al.* [3], Ismail [4], Sinha *et al.* [5], Lavric and Popa [6], Mekki *et al.* [7], Al-Sawari *et al.* [8], Qadir et al. [9], Poursafar *et al.* [10], and Finnegan and Brown [11]. For cellu-

The associate editor coordinating the review of this manuscript and approving it for publication was Shaohua Wan.

lar standards developed by 3GPP, the works of Yang *et al.* [12] and Tabbane [13] provided technical specifications and comparison. Most existing literature only discusses SigFox, NB-IoT and LoRa which are the three most prominent LPWANs (e.g., [5], [7]), provide a comparatively shallow evaluation (e.g., [3], [4], [8]), or mostly focus on interoperability issues (e.g., [9]). However, several other LPWANS exist offering their own features, advantages, and disadvantages. Thus, it is essential to provide a detailed analysis for a wider range of LPWANs as the suitability of each will vary between application use cases and situations.

There is a lack of existing literature analysing available LPWANs from a network or system design perspective. While many papers provide specifications for one or more LPWANs, none provide justification for why these specifications were selected. An LPWAN's specifications are the outcome of decisions made during the design process, with decisions aiming to best fulfil multiple LPWAN design goals as discussed in the following section. However, these decisions often incur a trade-off between goals – for example, increasing communication range can come at the expense of energy-efficiency. We identify these design decisions in this paper and determine what impact each decision has on the LPWAN design goals. For the first time, this paper systematically compares and analyses the impact of each design decision on eight different LPWANs.

Each use case will prioritize its application requirements (e.g., range, data rate, latency, integration with other systems, cost) to varying degrees and try to match them with the LPWAN that best meets those requirements for the deployment purpose. Use cases can also be classified as *critical* or *non-critical.* An example of a critical system is a network of biometric sensors monitoring patients suffering from serious illness, as failure could result in patient death. For each of the seventeen use cases discussed in this paper, we have performed an exhaustive analysis of their application requirements with respect to low power networking needs. Following this, we have determined those LPWANs whose specifications, capabilities and design objectives match a use case's requirements at varied levels. During this process we have also discussed the limitations of LPWANs that emerge due to many factors including restrictions imposed by regulatory bodies. Using this analysis, we have recommended a variety of LPWANs for each use case and, where appropriate, provided conditions for each recommendation. To the best of our knowledge, no current literature provides this extent of use-case analysis for LPWANs.

The paper is organized as follows. Section II determines LPWAN design goals and provides a comprehensive discussion for each. Following this, design decisions used in an attempt to meet these goals, and the impact of these decisions, are discussed in Section III and IV, respectively. In Sections V and VI, a variety of LPWAN solutions using unlicensed and licensed bands are presented analysing their technical features. Section VII compares and evaluates the presented LPWAN technologies by ranking them as per the level to which they meet the goals defined in the earlier section. Using these rankings, in Section VIII, the most suitable LPWANs are identified for a large variety of use cases, with requirement analysis and justifications for LPWAN choice. Finally, research challenges for LPWANS are discussed in Section IX while the paper is concluded in Section X.

II. DESIGN GOALS OF LPWANs

Several studies have discussed LPWAN goals from a research perspective. Raza *et al.* concluded that LPWANs are ideal for IoT systems spread over a large area requiring energy-efficient, low-cost devices at the expense of latency and data rate [3]. This is supported by Ismail [4] and Sinha *et al.* [5] who describe LPWANs as long-range, low cost, low-power networks connecting many devices suited to tiny amounts of information. These studies converge on the same basic characteristics and usage requirements of LPWAN, leading us to categorize the design goals of LPWAN as follows.

A. ENERGY EFFICIENCY

In many applications, IoT devices need to be deployed in inaccessible or nomadic locations. Consequentially, most devices are battery powered and unlikely to have access to a constant power source. Replacing batteries consumes both time and resources, and when applied to large networks presents an unrealistic expense. Lavric and Popa [6] measured a node's battery life in decades, while it has also been measured as '10 years or more' in a conservative estimate [3]. Given these statements, this paper considers 10 years the target battery life for nodes.

B. LONG RANGE

As wide-area networks, LPWANs must communicate over long distances. The target range for LPWANs is generally agreed upon as a few kilometers in urban areas, and tens of kilometers in rural areas [3], [4]. Mekki *et al.* provided more concrete benchmarks, expecting 1-5 km in urban areas and 10-40 km in rural environments [7]. When deployed in urban environments, LPWAN signals experience path loss, shadowing, multipath fading, and other types of signal deterioration from obstacles, infrastructure, moving objects, etc. Considering the above statements, this paper considers 5 km as the target urban range for an LPWAN, and 10 km for rural areas.

C. SCALABILITY

Scalability can be broadly defined as a system's ability to maintain quality of service as it grows. Bondi [14] further refines the concept of scalability into several sub-types depending on the nature of that growth - for example, the number of end devices growing is significantly distinct to an increase in traffic across these devices. While his definitions describe a relatively generic information system, we can easily apply them to an LPWAN.

Following [14], structural scalability defines how many end devices an LPWAN can support. This is determined by

both devices per base station and base stations per network or geographic area. Load scalability is more complex and refers to the amount of traffic each device in an LPWAN can handle without experiencing unacceptable delay, resource inefficiency or contention. This is often influenced by regulatory limits placed on LPWANs such as duty cycling, which are discussed further in Section III.A.

Scalability can also be classified as horizontal or vertical, concepts discussed for the IoT in [15]. Horizontal scalability is closely equivalent to structural scalability, defining how many hardware or software entities a system can support. Vertical scalability is a superset of load scalability, considering the resources available to each network component. While our discussion of load scalability is concerned with network access and availability as a resource, vertical scalability more broadly considers other resources such as CPU cycles, memory, and storage. For the discussion that follows, we will use the term structural and load scalabilities for simplicity.

In this study, we will consider 50,000 nodes per base station the target structural scalability. This number assumes 40 devices are present per house in a city with the density of London [6]. We have not provided a target value for load scalability, as requirements vary significantly for each use case (Section VIII).

D. LOW COST

Even if LPWANs support many nodes, it will be impractical to deploy them if nodes are expensive to manufacture and maintain. As all organizations have a limited budget, cheaper nodes always result in a larger possible system. If an LPWAN is provided by a public network, each node is likely to incur annual subscription fees. Conversely, if an organisation has its own private LPWAN, annual costs will be incurred by ongoing maintenance and support.

Some studies (e.g., [3]) suggested devices should cost less than US$5 and incur annual subscription fee as low as US$1, while others (e.g., [7]) proposed devices should cost less than 2 Euros and incur 1Euro annual subscription fee. In this paper, we consider the typical cost per node no more than US$20, working towards a goal of US$5. Subscription fees of US$5 are also desired, striving toward a goal of US$1.

E. INTERFERENCE MANAGEMENT

Due to the high cost of licensing a frequency band, many LPWANs utilize the unlicensed Industrial, Scientific, and Medical (ISM) spectrum. While lowering potential cost, using the ISM band may impede performance and reliability.

Interference in LPWANs can be classified as internal or external. Internal interference is caused by nodes in that network simultaneously transmitting in a shared or overlapping frequency band. This is often mitigated through channel access schemes and overlaps with the scalability design goal. External interference is a significant issue when utilizing the ISM band as frequencies cannot be reserved. The ISM band will only become increasingly congested as the number of wireless networks grows. To address this issue, LPWANs operating in ISM spectra should be especially resistant to noise.

While no quantitative number can be placed on this goal, we assume a network must employ some form of interference management strategy to meet LPWAN goals. This paper also considers deployment in the licensed spectrum as one of the interference management techniques.

F. INTEGRATION

In this paper, integration refers to an LPWAN's ability to work with other LPWANs and information systems. Data from sensors will be largely worthless if it can never be retrieved, and actuation systems should be controllable from external systems. Integration is achieved through the following:

- Many users, resulting in greater investment and wider support base.
- Ease of connection to the public Internet or application servers.
- Availability of APIs and user-facing solutions.

III. DESIGN DECISIONS IN LPWANs

Several decisions need to be made when deploying a wireless network, such as frequency spectrum and modulation technique. Each LPWAN attempts to achieve Section II's goals by applying different techniques to these decisions, with each having advantages and disadvantages. Often a trade-off is present, such as sacrificing bandwidth for data rate and vice-versa.

Below we examine each design decision with respect to a variety of techniques employed in LPWANs on their ability to meet design goals and a summary is presented in Table 1.

A. UNLICENSED OR LICENSED SPECTRUM

Operating in a licensed frequency band prevents external interference alongside improves Signal-to-Interference-plus-Noise Ratio (SINR), security and reliability. However, obtaining a license for these bands incurs a steep upfront cost and periodic renewal fee. Any increased cost will inevitably be passed on to subscribers, increasing Capital Expenditure (CAPEX) for deployment and ongoing Operational Expenditure (OPEX).

On the other hand, utilizing unlicensed spectra causes further difficulty in meeting integration goals, in addition to increased potential interference and congestion. Networks can intuitively select operating frequencies (Section III-B), modulation techniques (Section III-C), or multiple-access schemes (Section III-D) in attempts to mitigate these disadvantages. Regulatory bodies such as the *European Telecommunications Standards Institute*(ETSI) and the United States *Federal Communications Commission*(FCC) also work to prevent interference and congestion by imposing restrictions on unlicensed spectra. Restrictions limit transmission range or load scalability through techniques including limiting transmission power and enforcing duty cycle restrictions. More techniques and their operations are detailed in [16].

TABLE 1. Impact of design decisions on LPWAN goals and leading techniques.

	Power Consumption	Range	Cost	Structural Scalability	Load Scalability	Interference Management	Coexistence
Unlicensed or Licensed Spectrum	None	**High** Licensed Spectrum	**High** Unlicensed Spectrum	**None**	**High** Licensed Spectrum [16]	**High** Licensed Spectrum	**Moderate** Licensed Spectrum
Carrier Frequency	**None**	**High** Lower-Frequency	None	**None**	**High** (for Unlicensed Spectrum) Licensed Spectrum	None	None
Frequency Range	None	**Moderate** Narrow-band	**Low** Narrow-band	**Moderate** Narrow-band, Wide-Band (Spread Spectrum)	**High** (for Unlicensed Spectrum) Depends on local regulations	**High** Narrow-band, Wide-Band (Spread-Spectrum)	**High** Narrow-band
Modulation Technique	**Moderate** Binary schemes (Small packets), M-ary FSK (large packets) [48] LoRa [49]	**Low** (for Licensed Spectrum), **High** (for Unlicensed Spectrum) UNB, Spread-Spectrum [3]	**Low** Binary schemes, DPSK [50], LoRa [27]	**Moderate** UNB [51], QPSK [50], LoRa [27]	**High** (for Unlicensed Spectrum) Spread Spectrum [18] [19], Hybrid DS-SS/LoRa [20]	**High** FH-SS [52] [25], LoRa [26] [27], UNB [51]	**High** UNB [51]
Channel Access Method	**Moderate** ALOHA [3]	**Low** Spread-Spectrum	**Moderate** ALOHA [3]	**High** OFDMA [31], DS-SS (CDMA) [53]	**High** (for Unlicensed Spectrum) LBT/AFA [16] [17], FH-SS [18]	**High** OFDMA, FH-SS [52] [31], C-SS [26]	**Moderate** Spread-Spectrum [52]
Signal Diversity Technique	**High** No Diversity Scheme	**Moderate** S, T, F	**High** No Diversity Scheme	**Low** No Diversity Scheme	**Low** No Diversity Scheme	**Moderate** S, T	**Moderate** S, T
Duplexity	**High** No Duplexity Scheme	None	**High** No Duplexity Scheme	**Low** No Duplexity Scheme	**Moderate** No Duplexity Scheme	**Low** Full Duplexity	**Low** No Duplexity Scheme
Business Model	**Low** SD	**Moderate** MD	**High** SD	**Moderate** MD	None	None	**High** SD

The impact each design decision is likely to have on each LPWAN goal, along with the leading available techniques. Each cell contains the impact, followed by leading technique on the next line. For *Business Model*, 'Subscriber-Driven has been abbreviated as SD and 'Manufacturing-Driven as MD. For *Signal Diversity Technique*, 'Space' has been substituted with 'S', '*Time*' with 'T' and '*Frequency*' with 'F'.

Regulators often apply distinct restrictions to specific sub-bands or channels. In addition, restrictions may apply based on network characteristics such as modulation technique or multiple access scheme. Restrictions may be relaxed if a network can sufficiently reduce congestion or interference by design – examples include multiple access techniques utilizing *Listen Before Talk*(LBT) and *Adaptive Frequency Agility*(AFA) [16], [17].

ETSI provides an unlicensed spectrum of 863-875.6 MHz with transmission power limited to 27 dBm in the 869.4-869.6 MHz band and 14 dBm in all others [16]. If LBT/AFA are not utilized, duty-cycling limits are enforced mostly ranging from 0.1-1%, with the 27 dBm band allowing a higher 10%. Duty cycle limit is relaxed to 2.8% if LBT and AFA are utilized [18] – however, a minimum listening time of 160μs and minimum TX-Off Time of 100ms are enforced.

Transmissions must also not exceed 1s for single-direction protocols or 4s for bi-directional message exchanges, and these must collectively remain under 100s per hour over 200 kHz of bandwidth.

FCC provides an unlicensed spectrum of 902-928 MHz and encourages using spread-spectrum techniques by restricting transmission power to −1.25 dBm if they are not used [18]. Channels in frequency-hopping spread-spectrum (FH-SS) systems are restricted to 500 kHz bandwidth and 400ms dwell time. Networks with bandwidth over 250 kHz are permitted 24 dBm transmission power and 4% duty cycle but must hop between at least 25 channels. Conversely, bandwidths under 250 kHz are permitted 30 dBm transmission power but limited to a 2% duty cycle and required to hop between at least 50 channels.

30 dBm transmission power is permitted for networks utilizing direct-sequence spread-spectrum (DS-SS) techniques, however, this power must be spread evenly between bandwidths exceeding 500 kHz [19]. In addition, FCC allows hybrid techniques combining spread-spectrum modulation with an additional scheme such as LoRa [20]. Hybrid deployments are limited to 21 dBm transmission power, with additional restrictions depending on whether frequency-hopping is activated.

B. OPERATING FREQUENCY AND BANDWIDTH

Following the decision of licensed or unlicensed spectrum, the specific frequency band within that spectrum is to be selected. This decision consists of two elements:

1. The carrier band,
2. Total frequency ranges the network can occupy across all simultaneous messages.

Carrier frequency has significant impact on an LPWAN's communication range, and many implement lower frequencies to achieve greater range. Others such as LTE-M utilize higher frequencies to achieve higher data rates at the expense of range.

If an unlicensed spectrum is utilized, the carrier chosen impacts interference management and integration as other networks could be operating in the same band. This also affects the number of channels usable for Frequency-Division Multiple Access (FDMA) channel access, potentially impacting structural scalability. This impact does not occur if licensed spectra are utilized.

As discussed in Section III.A, regional authorities can enforce various limits to duty cycle and transmission power for individual bands within their unlicensed spectrum or depending on message bandwidth [16]. As transmission power determines communication range and duty cycle significantly impacts load scalability, the frequency band and carrier chosen in unlicensed spectrum networks considerably affect both of these parameters.

C. MODULATION TECHNIQUE

Modulation technique influences a wireless network's Bit Error Rate (BER) and SNR, impacting its effective link budget. Link budget determines the distance a network can realistically communicate, alongside its tolerance to signal impairment. In addition, modulation technique affects a network's cost and energy consumption.

Message bandwidth is determined by the modulation technique used – Ultra-Narrowband (UNB) messages use very low channel bandwidth, while spread-spectrum techniques utilize an entire band. Both techniques aim to manage noise and increase scalability through opposite means.

UNB signals for LPWANs are often produced by utilizing PSK (phase shift keying) techniques, which produces a lower BER than ASK (amplitude SK) or FSK (frequency SK) at the same bandwidth. In some LPWANs, PSK is combined with ASK or FSK to produce QAM (quadrature amplitude modulation) modulation. QAM allows for high data rates and spectral efficiency but is 400% less power-efficient than PSK [21]. Increasing the order of PSK or QAM modulation increases data rate and spectral efficiency at the cost of increasing BER [22]. Decreasing BER is possible, however consumes excess power.

Spread-spectrum modulation has high spectral efficiency and scalability, along with being heavily tolerant to noise and malicious jamming [23]. Spread-spectrum signals also co-exist well with high power-density UNB signals due to their very low power density [24]. Singh demonstrated in [25] that DS-SS is capable of 11 Mbps throughput while FH-SS is only capable of 3 Mbps. However, FH-SS provides superior resistance to interference and multipath, alongside performing well in harsh environments. LoRa modulation is a derivative of Chirping Spread Spectrum (C-SS) stated to exhibit robust Doppler Effect resistance [26] alongside resistance to multipath and fading, high network capacity, low power consumption and simple receiver design [27].

Section III.A discusses how restrictions placed on unlicensed-spectrum networks by regulatory bodies can vary between modulation schemes. Some of these restrictions, such as limiting transmission power, limit network range. Others, such as channel dwell time, limit load scalability. For unlicensed-spectrum networks, these respectively strengthen the relationship between modulation technique and range, and create a relationship between modulation techniques and load scalability.

D. CHANNEL ACCESS METHOD

Channel access method significantly influences a network's scalability by determining how many devices can connect at a given time. The ALOHA random-access protocol is very simple to implement and inexpensive and is consequentially used by several LPWANs [3]. However, it is also very inefficient and has lower load scalability, with asymptotic capacity of only 18% [28]. Frequency-Division Multiple Access (FDMA) is also simple to implement, however, is less scalable and more expensive alongside being spectrally inefficient [29]. Time-Division Multiple Access (TDMA) is more complex to implement than FDMA, however, it is more spectrally efficient and less expensive. Code-Division Multiple

Access (CDMA) is complex and potentially costly, however has high fault tolerance, low latency, and a lack of primary collisions [30]. Despite being a modulation technique, the use of spread-spectrum solutions is also considered a channel access method. For example, DS-SS and C-SS are utilized as forms of CDMA.

Orthogonal FDMA (OFDMA) and its variants eliminate FDMA's issues with spectral efficiency and have demonstrated superior scalability to both CDMA and TDMA, along with increased resistance to multipath fading and obstacle obstruction [31], [32]. This makes OFDMA a popular choice for LPWANs despite the potential cost.

Earlier discussion shows how restrictions imposed on networks can also depend on channel access method. These operate by limiting load scalability or range through techniques including enforced limits on duty cycle and transmission power. This creates relationships between load scalability and range with channel access methods in unlicensed-spectrum networks.

E. SIGNAL DIVERSITY TECHNIQUES

In systems with a lower probability of successful message transmission, diversity schemes can be utilized to raise it to an acceptable level. This is useful if LPWANs are operating in remote areas, are sparsely distributed, or encounter significant physical obstruction. Diversity is also implemented to overcome low throughput problem of random-access techniques such as ALOHA for use in LPWAN [33]. An example of this is SigFox's R-FDMA multiple access [9], [34], [35], that utilizes frequency diversity to increase reliability of otherwise random access.

Space and time diversity techniques increase scalability by reducing collisions between increasing numbers of nodes. This impact is significant if LPWANs utilize random access techniques. The probability of successful transmission and receipt can be increased by utilizing multiple diversity techniques together [36].

Time and frequency diversity allow for limitless diversity branches; however, each branch used consumes more power. Frequency diversity also reduces structural scalability by requiring additional frequency bands, and all types of diversity schemes reduce load scalability because of inefficient use of resources as traffic increases.

F. DUPLEXITY

Simplex systems are completely unsuitable for any LPWAN requiring actuation or message acknowledgements. Duplex systems can meet these requirements, however, incur a higher cost and consume more power. Simplex systems may be useful for providing very inexpensive and energy-efficient LPWANs where no actuation or acknowledgement is needed.

Most LPWANs utilize half-duplex (HD) connections as full-duplex (FD) connections often require twice the frequency band and power to operate, with potential increases in cost if operating in the licensed spectrum. However, LPWANs serving critical systems or systems requiring similar performance from uplink and downlink communications may benefit from FD communications. Time-Division Duplexing (TDD) has an obvious advantage over Frequency Division Duplexing (FDD). Duplexity impacts both structural and load scalability.

G. BUSINESS MODEL

A business model is an organization's strategy for profiting from LPWAN technology, allowing its existence to continue while rewarding investment. Through observing existing LPWANs, two main business models have been observed: *Subscriber-Driven* and *Manufacturing-Driven.* While most LPWANs have components of both, one model is generally prominent.

Under the subscriber-driven model, organizations aim to profit from network subscribers. These subscribers pay monthly fees and potentially an upfront cost to use the LPWAN. Amount paid may influence the number of connected devices, volume of data transfer, message size and message priority. Organizations are responsible for deploying and maintaining infrastructure but have the power to revoke or restrict a user's access to the network.

Under the manufacturing-driven model, organizations aim to profit from manufacturing devices for their LPWANs. Profits either originate from reserving exclusive manufacturing rights or claiming royalties from other manufacturing organizations who are held to a set of standards. Networks are deployed privately by each organisation or network operators.

Subscriber-driven networks limit structural scalability and range to the network operator's base stations; however, they also present a fixed and predictable cost. Manufacturing-driven networks allow users to deploy their own networks and extend structural scalability and range through additional base stations or repeaters. However, there is a practical limit on the extent to which this can be done. Deploying, maintaining, and managing a network also introduces increased and unpredictable cost.

IV. DESIGN DECISION IMPACT ON GOALS

Section III's design decisions impact a range of Section II's goals to a different extent. The impact of each design decision can be classified as presented below:

High – Changing this decision will always have a significant impact towards meeting the goal, or under most combinations of other decisions.

Moderate – Changing this decision will always have a moderate impact on meeting the goal or may have a significant impact under certain combinations of other decisions.

Low – Changing this decision will always have a small impact on meeting the goal or may have a non-significant impact under certain combinations of other decisions.

None – Changing this decision will never have an impact on meeting the goal.

Table 1 lists the impact of various techniques adopted in design decisions on the goals of LPWANs. Leading techniques for achieving each design goal are also presented

in Table 1, based on the discussions presented in the previous two sections.

In the following sections, we present unlicensed and licensed based LPWAN technologies which are either already commercially deployed or emerging, followed by a comparison among the technologies.

V. UNLICENSED SPECTRUM BASED LPWANs

Having evaluated a range of design decisions, we now examine LPWANs developed from these decisions. This section explores solutions where the design decision was made to operate in unlicensed spectra. Table 1 shows that unlicensed spectrum solutions are less expensive than their licensed counterparts, however, they are more likely to experience interference. Unlicensed spectrum networks are developed and maintained by various private organizations.

A. SIGFOX

SigFox is a French organisation founded in 2009 [37] who planned to deploy its LPWAN service in over 60 countries by the end of 2018 [38]. Devices require a compliant radio transceiver to connect to SigFox's network, and almost any organisation can manufacture these transceivers if terms and conditions are followed [39]. SigFox follows a completely subscriber-driven model and devices are relatively inexpensive.

Architecturally, SigFox defines their network as having two 'layers' – the Network Equipment and SigFox Support System as shown in Figure 1. Network Equipment consists of all base stations and their attached antennae, following a star network topology resulting in energy-efficient endpoints and high spectral efficiency. Devices send messages over radio interface to the closest base station, which is responsible for receiving the message and backhauling it to the SigFox Support System over the public Internet. This backhaul utilizes VPN (virtual private network) tunneling and is generally based on DSL (digital subscriber line) with LTE (long-term evolution) and satellite as backup media [8], [36].

By default, SigFox base stations do not acknowledge message receipt, and compensate for reduced reliability with time and frequency diversity schemes [35], [36]. Additionally, if multiple base stations are in range, each base station will receive and process each message [36]. This is an example of spatial diversity.

The *SigFox Support System* is hosted in a cloud environment by SigFox and consists of individual services carrying out most network functionality. These services can be divided into four major groups – i: *Back-End Servers*, ii: *Storage*, iii: *Front-End Servers*, and iv: *Data*.

Back-End Servers communicate directly with each base station over the backhaul network. These are responsible for monitoring and managing the base stations in addition to processing incoming messages. If multiple base stations receive a message, the back-end servers determine which copy to keep.

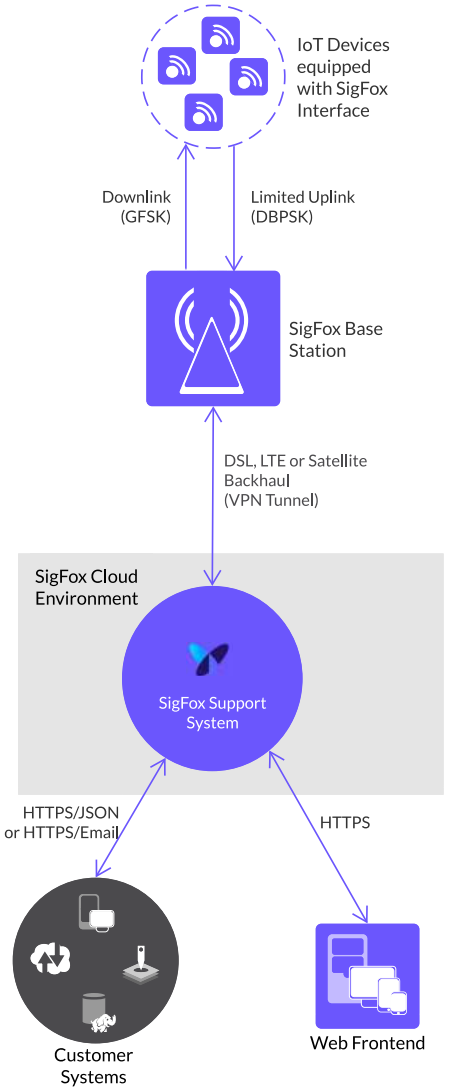

FIGURE 1. SigFox's overall network architecture. GFSK: Gaussian frequency shift keying; DBPSK: Differential binary phase shift keying.

Storage consists of two sets of databases – one stores all data retrieved from devices, and other stores metadata regarding each device. Messages are stored in the first database after being processed by back-end servers.

Front-End Servers communicate exclusively with storage's metadata database, presenting a web interface for subscribers to manage devices and configure user or group permissions.

Data communicates with message databases in the storage layer, presenting a JavaScript Object Notation (JSON)-based API for subscribers to retrieve data and integrate with business systems. Both uplink (UL) and downlink (DL) are supported, although the system is optimized for uplink communications.

SigFox divides the world into six distinct regions [40] numbered RC1 to RC6 with each having different channel characteristics, specifications, multiple access mechanisms, and performance. RC2 and RC4 have uplink data rates of 600 bps while all other RCs utilize 100 bps. In contrast, downlink data

rate is 600 bps in all regions. Each region also utilizes its own center frequency, falling between 865 and 924 MHz.

RC1 uses a strict duty cycling mechanism that limits the transmission to 36 seconds per hour, while others use either *Frequency Hopping* or *Listen Before Talk*. Frequency hopping broadcasts each message three times on different frequencies and limits on-air time to 400ms per channel. In addition, any new transmission is prevented for a further 20 seconds. *Listen Before Talk* forces a device to verify whether an intended channel is free before it starts transmission if the detected signal is stronger than -80 dB. Downlink messages are even more restricted and can only be sent in response to uplink messages [41]. SigFox's cloud backend also limits each device to six uplink messages per hour and four downlink messages per day [42]. These strict policies limit the load scalability of SigFox networks.

Previous research provided conflicting results on SigFox's rural range. Mroue *et al.* [43] claim SigFox can achieve a maximum range of 63 km, while Raza *et al.* [3], Poursafar et al. [10], Qadir *et al.* [9], and Finnegan and Brown claim it is 50 km. Mekki *et al.* state that SigFox's range is 40 km. [7]. SigFox provides little information in their own specifications, with only their United States website [44] stating it can communicate 'upwards of 20 miles' (32.2 km). Link budget is also contentious in previous literature, with Qadir *et al.* [9] and Pietrosemoli [45] providing a range of 146-162 dB. Zuniga [46] is more specific, claiming it is 162 dB UL and 163 dB DL in ETSI-compliant regions and 165 dB UL and 159 dB DL in FCC-compliant regions. SigFox's own site [47] states UL link budget of 163.3 dB is achieved by balancing bitrate with base station receiver sensitivity and transmission power. For example, if 600 bps is used, the base station's sensitivity will be 8 dBm lower and device transmission power is up to 8 dBm higher.

While conflicting information is reported in the literature regarding SigFox's security mechanism, the official white paper states it supports optional AES-128 encryption based on a device key [36]. This could introduce a security risk if users forget to enable security or willingly disable it. Despite this, the SigFox Support System is hosted in very secure data systems and utilizes VPN tunneling for backhauling. This suggests SigFox's backend is much more secure than its air interface.

B. LoRaWAN

While SigFox provides a proprietary solution with a completely subscriber-driven model, LoRa is an open standard relying on a manufacturing-driven model. LoRa consists of two protocols when acting as an LPWAN:

i. *LoRa*, which defines the physical layer and modulation technique.

ii. *LoRaWAN*, which defines the network's greater architecture and wide-area capabilities.

Unlike SigFox, LoRa uses a mostly manufacturing-driven business model with transceivers exclusively manufactured by Semtech [39]. While actual transceivers can only be manufactured by Semtech, any hardware manufacturer is permitted to integrate them into their devices provided LoRa's specifications are followed.

LoRaWAN has been developed by an open group called the LoRa alliance which any individual or organisation is free to join. Ray [39] noted that this leads to more flexible development but slows progress. The LoRaWAN alliance also certifies products developed for connecting to it, however, it does not restrict how organizations deploy or charge for access to their networks [49]. The LoRa alliance defines two types of LoRaWAN networks- i. *Private* and ii. *Public* networks. Private networks are operated by individuals or organizations for their own purpose, while organizations may offer public networks as a service to paying subscribers.

Like SigFox, LoRaWAN utilizes a star-of-stars network topology where star topology is employed but messages are received by all base stations in the range. LoRaWAN's network architecture is illustrated in Figure 2. LoRaWAN base stations are named gateways and connected to a network server through a higher-throughput backhaul. These backhauls utilize the public Internet or a private WAN, with examples including Ethernet, LTE, Satellite and Wi-Fi [54]. Mekki *et al.* also noted how LoRaWAN's spatial diversity prevents complex message handover as seen in traditional cellular networks [7]. This makes LoRaWAN ideal for high-mobility use cases where nodes are likely to move between gateways.

The network server decodes packets received from connected gateways and encodes packets destined for nodes connected to them. If multiple copies of the same packet are received via multiple gateways, the network server determines which message to keep. It is also capable of locating devices based on the time difference among duplicate messages [7]. The network server is also responsible for message acknowledgement, network security, and communicating with connected application servers [54].

LoRaWAN employs an *Adaptive Data Rate*(ADR) mechanism in which each node's spreading factor is adjusted to select the highest practical data rate while maintaining an acceptable SNR. Finnegan and Brown [11] stated LoRaWAN cannot achieve practical structural scalability without ADR and would only support 120 nodes per base station without it. With ADR, LoRaWAN base stations are capable of serving over 1,000,000 nodes.

LoRaWAN end devices only receive downlink messages when a 'receive window' is open, and devices can be classified as follows to determine when this occurs [55]. These classifications are shown in Figure 3.

Class A devices only open two temporary receive windows (shown in Figure 3 as RX) after sending a message uplink (shown as TX). Downlink messaging is only used for message acknowledgement.

Class B devices share the acknowledgement functionality of class A devices but also open receive windows at scheduled times known to the network server. The network server

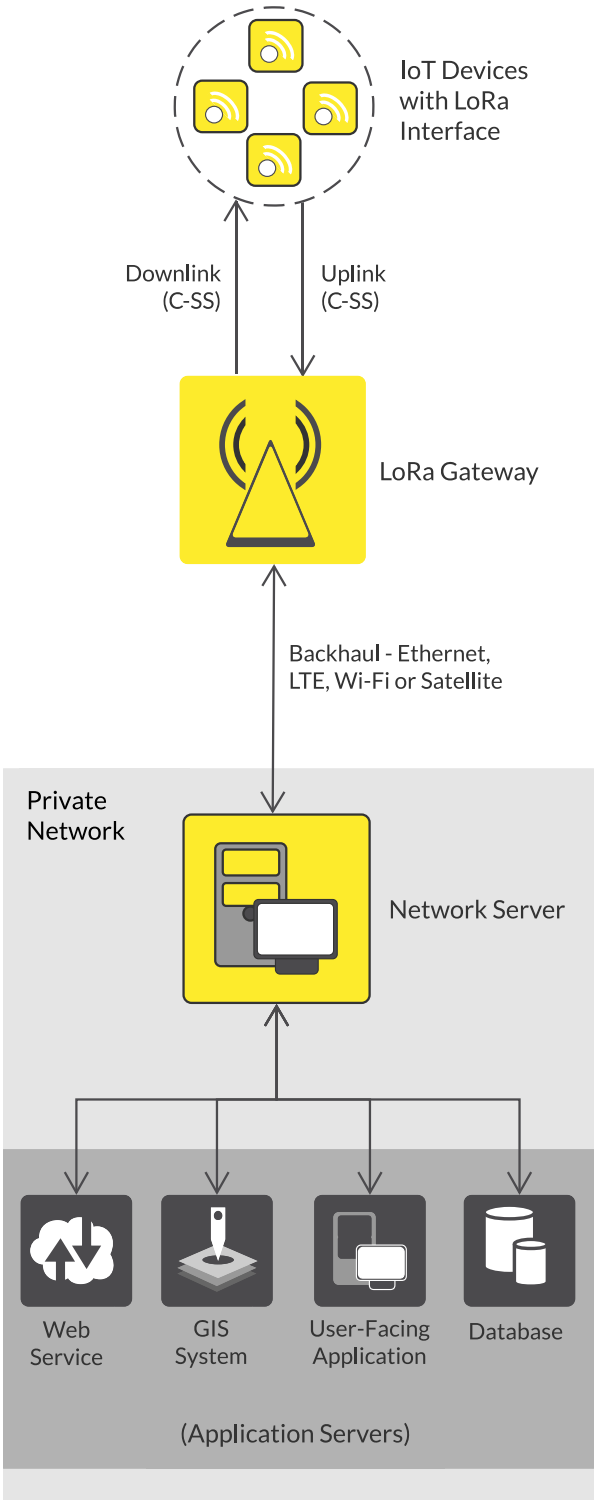

FIGURE 2. LoRaWAN network architecture. Common examples of application servers that interact with the network server are provided.

ensures that pending downlink messages are only sent to devices during these times.

Class C devices have receive windows constantly open except for when a message is being transmitted.

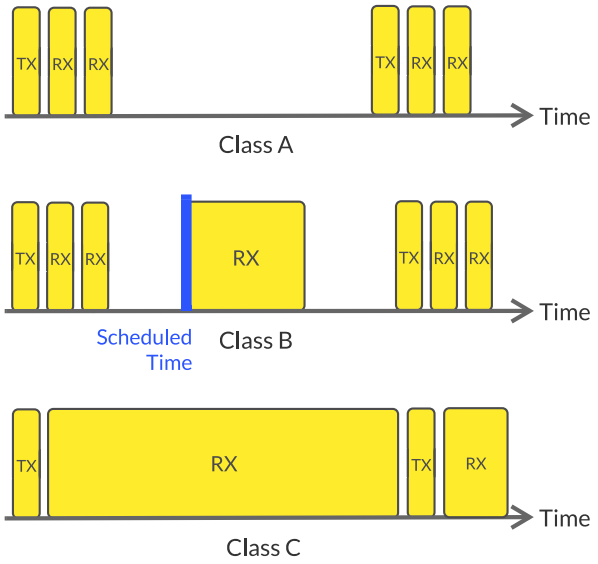

FIGURE 3. A visual representation of LoRaWAN device classes. Class B opens a receive window when the scheduled time is reached, represented by the blue line.

Open receive windows consume additional power, meaning organizations should strive to use the lowest practical class.

Sinha *et al.* [5] stated that all devices join the network as Class A devices and can 'decide' to switch to Class C if needed. Mekki et al. [7] also mentioned that the LoRa alliance plans for future versions of the LoRaWAN protocol to support temporary switching between classes A and C.

LoRa's modulation technique utilizes a form of C-SS with available spreading factors between 7 and 12 [56]. Higher spreading factors increase the range and SNR limit while decreasing data rate [57]. LoRaWAN gateways can receive messages with different spreading factors, allowing it to vary between connected nodes.

FCC territories allow LoRaWAN to be deployed using either DS-SS or hybrid techniques, with hybrid techniques integrating LoRa's modulation scheme [20]. In addition, LoRaWAN utilizes the simple ALOHA technique for multiple access. As no LBT or AFA mechanism is implemented, this subjects the protocol to duty cycles from 0.1 to 1% in ETSI territories with the exception of a single high-capacity 10% band [58]. However, as discussed in Section III.A, FCC territories are much less restrictive when ALOHA is used.

Bandwidth on LoRa transceivers can be adjusted between 7.8 and 500 kHz, however, only 125, 250 and 500 kHz are used in practice [11]. LoRa's range depends on both spreading factor and the maximum transmission power permitted by local regulatory bodies. Bands utilized by LoRaWAN in ETSI territories are subject to 14 dBm, with a single exception for the 869.4-869.6 MHz band allowing 27 dBm [16], [20], [58]. Conversely, in FCC territories LoRaWAN utilizes between 20-30 dBm for DS-SS and 21 dBm for hybrid deployments [20].

LoRaWAN's urban range is unanimously agreed on as 5 km, however, there are different values reported for rural range. Mekki et al. [7] stated LoRaWAN has a rural range of 20 km, while Raza *et al.* [3] reported a higher value of 25 km. Ismail [4], Qadir *et al.* [9], and Finnegan and Brown [11] all reported a rural range of 15 km. Considering all the above, 18 km which is close to the mean of the above reported values can be regarded as the rural range.

LoRaWAN further attempts to avoid congestion or interference by enforcing a minimum TX-Off time after each message derived from the previous message's time-on-air [11], [59]. Messages that take longer to send will result in further downtime before an additional message can be sent.

LoRaWAN's data rate depends on the spreading factor and bandwidth. Sinha *et al.* [5], Mekki *et al.* [7], and Finnegan and Brown [11] all state that LoRaWAN's maximum data rate is 50 kbps. Raza *et al.* [3] further elaborate that LoRaWAN's data rate is between 0.3-37.5 kbps if LoRa's C-SS modulation is used, while the 50 kbps rate is achieved using FSK. Ismail [4] and Lavric and Popa [6] provide conflicting maximum data rates of 27 and 5.5 kbps, respectively. The LoRa alliance's official specification [60] states the data rate is between 0.3 and 50 kbps, and these claimed values are likely to be closest to the actual achievable rate. Increasing the spreading factor will improve network reliability but consequentially lower data rate and load scalability.

C. WEIGHTLESS-IoT

Though SigFox and LoRaWAN have achieved widespread success with deployment in many application domains, not all LPWAN technologies achieved this level of success. The Weightless family of LPWAN standards has made two attempts at penetrating the market and have only seen some success with the third.

Weightless is a set of standards maintained and developed by the Weightless Special Interest Group (Weightless SIG), originally intending to provide LPWAN communications in TV whitespace (TVWS) [61]. Weightless SIG developed three different LPWAN standards, each with different technical capabilities:

i. Weightless-W
ii. Weightless-N
iii. Weightless-P

Weightless-W is based on the original concept of delivering LPWANS in TVWS, operating in the 470-790 MHz band [62]. Worldwide availability of TVWS differs based on regional regulations and spectrum allocation, making Weightless-W unsuitable for deployment in many parts of the world. This lack of potential market share saw development on Weightless-W cease before 2015 [63], however, Ray [62] noted the standard has potential in the oil and gas sectors where TVWS is likely to be available. If TVWS is available, Weightless-W provides a solution with a very high data rate.

The architecture of Weightless-W can be found in a 2013 report for the Weightless SIG by Webb [64]. Weightless-W follows star topology, and base stations communicate with a cloud-hosted network manager server over a backhaul utilizing either the public Internet or private WAN. Once uplink messages reach the network manager, they are forwarded to a second server called the synchronization database. This acts as an interface to the subscribers' own systems, with Webb's report outlining SAP and Oracle as examples. Conversely, information from outside the system is sent to the Synchronization database before being forwarded to the network manager and correct node.

Raza [3] noted Weightless-W signals can be sent with multiple spreading factors allowing a trade-off between link budget and data rate as seen in LoRaWAN. Webb's report [64] notes that alongside the spreading factor, receiver sensitivity also varies based on coding rate and downlink data rate – as expected, 16-QAM modulation results in much shorter range than DBPSK. The minimum achievable RX sensitivity is −128 dBm with a data rate of 0.0025 Mbps, and the maximum −82.5 dBm with a data rate of 16 Mbps.

Weightless-N is the second standard developed by a company Neul, with an organisation named NWave developing most of the hardware [62]. Weightless-N operates in the ISM band as opposed to TVWS [65] and has no downlink capabilities [3]. McClelland [66] also noted that Weightless-N has a superior MAC-layer implementation to SigFox. This was likely an attempt at gaining some of SigFox's market share, however, Weightless-N was ultimately unsuccessful and the responsibility for the standard was given to ETSI [65]. This failure is attributed to factors including an unbalanced link budget and the required *Temperature Compensated Crystal Oscillator*(TCXO) component [62]. Despite its perceived failure, Weightless-N networks were deployed in both Denmark [67] and London [68].

Weightless-P is the latest standard released by Weightless SIG, and like Weightless-N it targets low data rate networks operating in the ISM band. The technology has been championed by a Taiwanese company named Ubiik, who has become the main manufacturer and distributor for Weightless-P solutions. Weightless has finally seen more success with this standard, and Ubiik claimed to have shipped hardware to 20 countries as of 2017 [69].

Weightless-P fully supports downlink communications, allowing it to be suitable in applications where Weightless-N was not [3], [70]. Weightless-P's use of GMSK modulation eliminates the requirement of the problematic TCXO unit, mitigating one of the main issues with Weightless-N. Moreover, Weightless-P's GMSK and QPSK modulation are improvements over Weightless-N's DBPSK. But QPSK has a higher error rate and requires more power to lower this [71], [72] while the use of GMSK also lowers Weightless-P's effective range and makes it potentially less suitable for use in WANs. Weightless SIG have also taken effort to ensure the standard achieves the best performance within ETSI and FCC regulations. Weightless-P's use of LBT and AFA mechanisms relax duty cycling limits in ETSI territories, while its use of FH-SS also grants it exemption from the strictest FCC regulations [70].

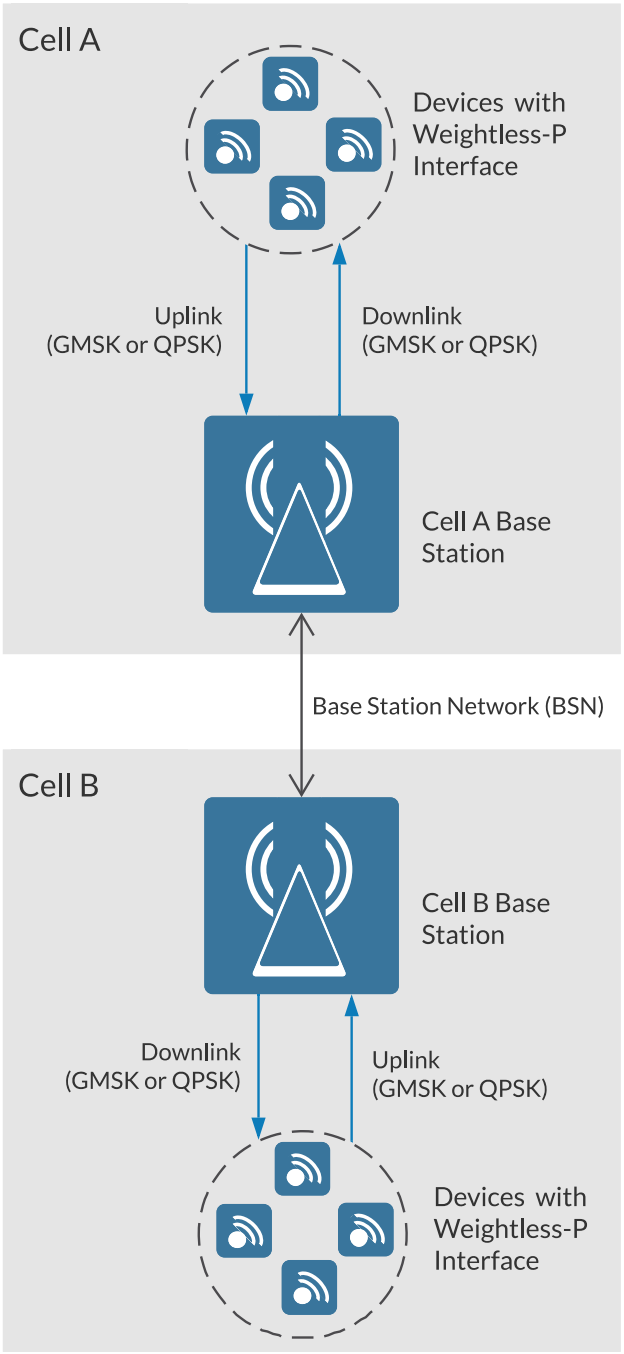

FIGURE 4. Weightless-P network architecture.

Weightless SIG provided some information about Weightless-P's network architecture in [70], breaking a Weightless-P network into End Devices (Eds) and Base Stations (BSs). Figure 4 provides a graphical representation of this architecture. Eds are generally simple, inexpensive and have a lower duty cycle, while BSs are more complex. All Eds communicate with a single BS to form a cell, and BSs are connected by a network called the Base Station Network (BSN). The BSN manages resource allocation, scheduling, roaming, ADR [73] and security. Interestingly, it appears Weightless-P is heavily inspired by LTE architecture. Another similarity with LTE is Weightless-P's mobility functionality, with Weightless-P supporting handover, roaming, and cell re-selection [74].

Raza *et al.* [3] claim that Weightless-P has an urban communication range of 2 km. Ubiik elaborates on this by stating Weightless-P can cover 2 km in a dense urban environment [75], but is also capable of covering 4 km in a 'medium city' environment. On another site [76], Ubiik compares Weightless-P's link budget of 160 dB to LoRaWAN's budget of 150 dB. Despite Weightless-P's 160 dB link budget, Ubiik only provided achievable range for 150 dB on their website. The site states a link budget of 150 dB covers a range of ∼5 km in a medium city and ∼25km in a rural area. Considering this we can state that Weightless-P has a range of 2-5 km in an urban environment depending on density, and a range of ∼25 km in a rural environment.

Weightless-P allows organizations to deploy private networks with complete ownership of the infrastructure, ensuring exclusive access to the network [77], [78].

D. NB-Fi

The NB-Fi standard is developed by a standardization body named the *NB-Fi* alliance and an organisation named WAVIoT. WAVIoT will work with other parties to develop custom devices for the protocol, while the NB-Fi alliance provides licenses to build devices for an annual fee. NB-Fi is also not a single protocol, but instead a protocol suite encompassing all layers of the OSI network model [79].

NB-Fi devices connect to a local base station which backhauls over Ethernet, GPRS or satellite to a cloud-based server [80]. Interestingly, NB-Fi base stations utilize a form of edge computing and perform a significant amount of data processing internally. This allows NB-Fi networks to continue operating during outages [79].

WAVIoT offers three deployment methods for NB-Fi LPWANs [80]:

i. *Public Networks* are marketed towards large telecom organizations and can cover an entire state or even a country. These contain many base stations acting as cells.

ii. *Private Networks* are marketed towards smaller organizations and cover a single city area, consisting of several cells.

iii. *Enterprise Networks* are marketed towards the simplest use-cases and cover a small area using a single 'mini-gateway' cell.

Private and enterprise networks are purely subscriber-driven models managed by WAVIoT, who hosts the cloud server on its own network. Subscribers communicate with devices and monitor the network by utilizing proprietary software packages and APIs. Public networks are managed by the operating organisation who hosts the cloud server on its own infrastructure. This allows the organisation to be responsible for subscriptions, billing, maintenance, and support of the network.

NB-Fi devices can have transmission power adjusted to 14, 16, or 27 dBm. Increasing transmission power increases the link budget at the cost of higher power consumption. NB-Fi's own site claims link budget can reach 'up to 174 dB'. Ikpehai *et al.* [81] support this, stating that 174 dB is reached with TX power of 30 dBm. Finnegan and Brown [11] claimed that NB-Fi offers an uplink latency of 30 seconds and a downlink latency of 60 seconds. The NB-Fi alliance states that NB-Fi has a minimum data rate of 11 bits per second [82], and a white paper by WAVIoT [83] provides a range of accepted data rates for NB-Fi's physical layer; 50, 400, 3200, or 25600 bps. Finnegan and Brown [11] claim that NB-Fi is capable of communicating over 16.6 km in an urban environment, however WAVIoT's own site [79], [80] provides a range of 10 km. As it is unlikely WAVIoT would advertise specifications lower than actual performance, this value can be considered as the correct estimation.

E. DASH7

DASH7 Alliance Protocol (D7AP) originates from ISO18000-7, an active radio frequency identification (Active RFID) specification utilized by the US Department of Defense (DoD) [84]. D7AP extends this standard to a full-stack protocol reaching up to the application layer and expands its functionality from RFID systems to WSN environments. The D7AP standard is developed and maintained by the *DASH7 Alliance*.

Architecturally, D7AP networks are very similar to LoRaWAN, allowing users to deploy their own private network. Alongside end devices and gateways, D7AP networks can also contain *sub-controllers* – devices that relay communications between gateways and multiple end devices [84], [85]. Sub-controllers have the entire suite of gateway functionality, but unlike gateways they are permitted to enter low-powered 'rest' mode. D7AP end devices spend most of their time in rest mode, only 'waking' when required to send or receive messages. The use of sub-controllers allows D7AP to implement a *tree* topology alongside the more common star and star-of-stars [11], [84], [86].

All gateways connect to a Network Server (NS) responsible for administrative functions including data aggregation and handling duplicate messages. NS further connect to a customer cloud, with the NS and customer cloud respectively similar to LoRaWAN's network server and application servers.

D7AP is built around five concepts with the acronym *BLAST*– Bursty, Light, Asynchronous, Stealth, and Transitive [84]–[86]. *Bursty* refers to D7AP messaging being intermittent with short time-on-air, while *light* refers to the small maximum packet size of 256 bytes. *Asynchronous* references the fact that periodic synchronization and handshaking is not required between devices, which instead communicate as needed. *Stealth* describes each device's capability to restrict incoming communications to those on a stored whitelist, and the fact that beaconing is not required. Finally, *Transitive* simply illustrates the standard's mobility features – devices can move freely between gateways.

Lo-Rate, Normal, and *Hi-Rate* modes are offered for communication respectively allowing data rates of 9.6, 55.555, and 166.667 kbps [84], [86]. Frames are either classified as *foreground* or *background* - foreground frames contain actual data being communicated, while background frames are responsible for network management and controlling foreground communications. Background frames are a fixed 6 bytes in length, while foreground frames have variable length of up to 256 bytes. Alongside commonly seen FEC encoding, D7AP also implements *PN9* data whitening. Data whitening distributes a signal's power evenly over the occupied bandwidth to avoid DC offset [87] without introducing processing gain [88]. The term *PN9* simply refers to the use of a 9-bit pseudorandom number generator [89].

D7AP provides an API for abstracting network addressing and other complexities behind simple file system commands and queries [84], [90]. Commands access the file systems of network devices, with each device containing both *system* and *user files*. System files specify network configuration parameters, while user files contain data for application-specific purposes. Commands can read or write sensor/actuator values in user files or perform remote configuration and maintenance through reading and writing system files. Permissions are also enforced on files as per any standard system with support for over-the-air authorization.

Queries accompanying file system commands can specify which devices to execute the command on, and under which (if any) conditions to do so. Devices are queried based on contexts such as the type of device or its current value.

Communications between D7AP end devices and gateways or sub-controllers can occur using one of three methods [4] – the *D7AP Advertising Protocol*(D7AAdvP), the *D7AP Action Protocol*(D7AActP), or *dormant sessions*. D7AAdvP is used for tag-talk-first uplink communications and D7AActP for downlink communications, with both designed to uphold the *BLAST* concept and maximize energy-efficiency. Dormant sessions queue downlink communications for a specific period of time before initiation, however, if uplink communications are initiated during this time the gateway will request a new session to exchange the queued message. More information on these mechanisms can be found in the DASH7 alliance's specification document [86], alongside the works in [84] and [90].

VI. LICENSED SPECTRUM BASED LPWANs

Following the preceding section's analyses of unlicensed-spectrum standards, this section examines the standards operating in the licensed frequency spectra. All licensed-spectrum standards are developed by 3GPP and based on the existing cellular protocols.

Licensed-spectrum solutions are more expensive to implement, however provide more reliable services because of exclusive access to their assigned frequency band. In addition, the lack of regulatory restrictions that unlicensed spectra are

subject to brings significant improvements to load scalability for licensed spectra. Increased cost can be easily borne by larger telecom organizations, who are likely to already own 3GPP infrastructure. As these solutions can be utilized by the existing 3GPP infrastructure, telecom organizations can implement them without purchasing or radically changing assets.

As of Release 13, 3GPP provides three standards for deploying IoT solutions in LTE or legacy GSM infrastructure based around the lowest-capacity categories of User Equipment (UE) [4], [91]:

i. LTE-M, consisting of UEs in LTE Cat M1,
ii. NB-IoT, consisting of UEs in LTE Cat NB1,
iii. EC-GSM, utilizing legacy GSM infrastructure.

In Release 14, additional LTE device categories were added to cater to further use cases [92], [93]:

iv. Cat M2 for LTE-M
v. Cat NB2 for NB-IoT

High worldwide penetration of GSM and LTE infrastructure allows standards based on them to be made quickly available.

A. 3GPP ENERGY-SAVING TECHNIQUES

3GPP utilizes three techniques to help their LPWAN protocols meet low-power requirements: i) Extended Discontinuous Reception (eDRX), ii) Power Saving Mode (PSM), and iii) Coverage Enhancement (CE).

DRX is a technique used to increase battery life by periodically de-activating a UE's radio transmitter. The time the transceiver is inactive is known as *DRX time*, and in human-facing devices such as smartphones it is imperceptibly small. Because of less stringent latency requirements for non-critical use cases, IoT UEs can tolerate minutes or even hours of delay in these situations. In response, 3GPP introduced the eDRX standard in release 13, supporting DRX times up to 10.24 seconds in connected mode and 2.91 hours in idle mode [91], [94].

Using Power Saving Mode, a UE sends two messages to the base station specifying a negotiable time to cache UE information for. UEs must 'reattach' to the network after a DRX cycle, consuming additional power. However, if the information is cached, UEs are not required to reattach to the network and energy is conserved. A store-and-forward mechanism can also be used to prevent message loss during deactivated periods [94].

Coverage Enhancement is a time diversity scheme providing two modes for UEs – Mode A or Mode B [95]. CE Mode A provides small-to-medium range improvements while Mode B provides long-range improvements. Utilizing CE increases range but also increases power consumption while limiting throughput and data rate, confirming the relationship between diversity techniques and range shown in Sections III-IV. Both advantages and disadvantages of CE are seen at much greater extents if Mode B is used. Table 2 summarizes the energy saving techniques adopted by 3GPP.

TABLE 2. 3GPP LPWAN energy-saving techniques ([13], [92], [95], [97], [98]).

	eDRX	PSM	Coverage enhancement
NB-IoT	Yes	Yes	Yes
LTE-M	Yes	Yes	Yes
EC-GSM	Yes	Yes	No

B. NB-IoT

NB-IoT is by far the most prolific 3GPP cellular standard, with industries and research communities [5], [43], [96] predominantly assessing NB-IoT. NB-IoT's low data rate, UNB modulation, long range and low power consumption are clearly 3GPP's attempt to compete with proprietary LPWAN standards such as SigFox and LoRaWAN.

NB-IoT is based on a slightly modified iteration of the standard LTE architecture. UEs connect to the LTE UTRAN (*Universal Terrestrial Radio Access Network*) which backhauls information to other UEs or external systems over a central network. Some LTE functionalities have been removed from NB-IoT UEs to conserve energy including Inter-RAT (*Radio Access Technology*) mobility, handover mechanisms, public warning functions, dual connectivity, carrier aggregation and emergency calling [91]. Many of the LTE's standard physical channels have been altered for NB-IoT to conserve energy, including limiting modulation techniques to only QPSK or BPSK and fitting both primary and secondary synchronization signals into one *Physical Resource Block* (PRB) and supporting Transport Block Sizes (TBS) smaller than a single PRB [99]–[102].

Two optimizations for the EPC (*Evolved Packet Core*) are outlined for NB-IoT on the control and user planes, collectively named the CIoT EPS (*Cellular IoT Evolved Packet System*) Optimization [103], [104]. Control Plane optimization ensures that UE data is sent over the signaling bearer without an additional data bearer being established. This eliminates the overhead of establishing a data bearer, reducing the overall transmission time, and conserving power. User Plane optimization ensures UEs cache RRC (Radio Resource Control) protocol information when entering into an inactive state, removing their need to establish a new RRC connection upon 'waking up'. This reduces transmission time, therefore conserves power. CIoT also specifies a new EPC node for handling *Machine-to-Machine*(M2M)-type data, named the SCEF (*Service Capability Exposure Function*). The SCEF handles non-IP data and allows it to be sent and received over the LTE network using the control plane [103]. Figure 5 provides a graphical outline of the EPC architecture and its optimizations.

One of NB-IoT's most attractive traits for telecom organizations is its ability to be deployed in one of three modes – i. *In-band*, ii. *Guard-band*, or iii. *Stand-alone*. Which one is

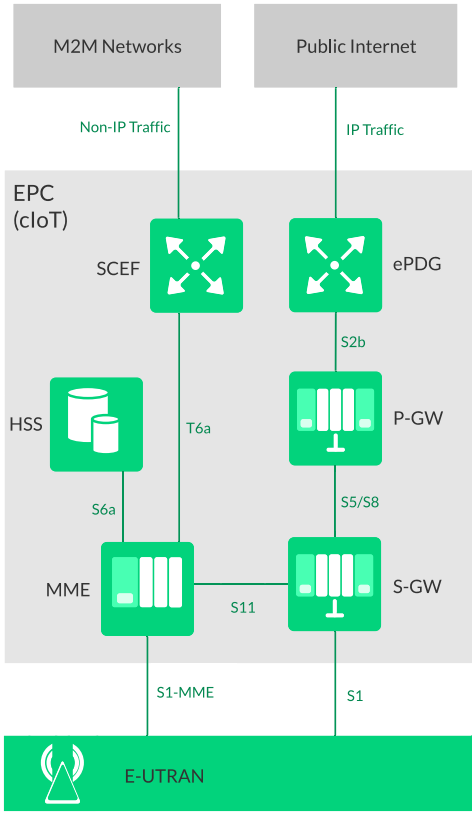

FIGURE 5. Evolved Packet Core (EPC) architecture with CIoT (Cellular IoT) enhancements for NB-IoT. This is an enhancement of the existing LTE cellular architecture. SCEF: Service Capability Exposure Function; ePDG: Enhanced Packet Data Gateway; PGW: Packet Data Node Gateway; S-GW: Serving Gateway; HSS: Home Subscriber Server; MME: Mobility Management Entity.

deployed depends on available infrastructure [4], [94], [100]. Each of these is differentiated in Figure 6.

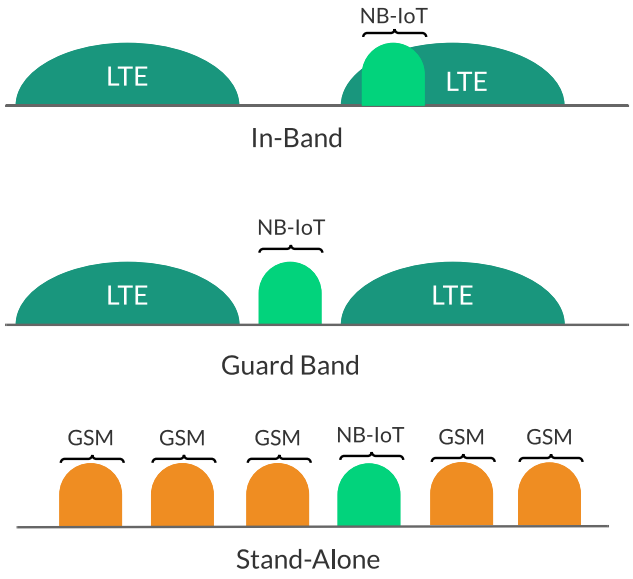

FIGURE 6. A visual representation of each NB-IoT deployment mode. This representation assumes that GSM networks are being utilized for deploying stand-alone NB-IoT.

Using In-band deployment, NB-IoT signals are assigned an existing PRB on the current LTE band in use. NB-IoT's 180 kHz messages can easily be multiplexed into a 180 kHz LTE PRB, however caution must be exercised to avoid overlap with legacy control and reference signals [99], [105]. Guard-band deployment involves transmitting NB-IoT signals in an existing LTE signal's guard-band. Guard-band increases with signal bandwidth, and guard-bands for signals under 5 MHz are too narrow to support this deployment. Consequentially, 3GPP release 13 advises UNB manufacturers to employ power boosting techniques for 5 MHz signals [101]. Stand-alone deployment involves NB-IoT signals being transmitted entirely separately from existing LTE signals. Existing GSM carriers utilize 200 kHz signals, creating a perfect opportunity for organizations to refarm unused GSM channels and decommissioned infrastructure for NB-IoT [12], [99]. However, if the GSM band is utilized for stand-alone deployment, NB-IoT message bandwidth will increase to 200 kHz.

In-band and Guard-band solutions provide greater spectral efficiency than stand-alone deployment as they utilize unused bands in an existing signal. A study by Ratasuk *et al.* [101] also proved that guard-band deployment exhibits better downlink performance in poor conditions. Despite this, utilizing 200 kHz GSM signals in Guard-band deployment may reduce spectral efficiency due to the slight bandwidth increase. This is likely to be overlooked by telecom organizations because of the economic benefits offered by re-using the existing infrastructure.

3GPP Release 14 introduced enhancements to the NB-IoT protocol intending to conserve additional power, further increase the data rate, and expand its suitable use cases [92]. A new NB-IoT device category named Cat. NB2 was developed to enhance Release 13's Cat. NB1 category. Improving on Cat. NB1's maximum TBS of 680 bits downlink and 1000 bits uplink, Cat. NB2 supports TBS of 2536 bits both uplink and downlink. Cat. NB2 also permits a second *Hybrid Automatic Repeat Request*(HARQ) process, utilization of which will increase uplink data rate from 106 to 158.5 kbps and downlink data rate from 79 to 127 kbps. In contrast, Cat NB1 only supported data rates of 62.5 kbps uplink and 25.5 kbps downlink. [106]

To make NB-IoT suitable for additional use cases, Release 14 adds multicast capabilities, significantly improved location services, and specifies a new UE power class. Standard NB-IoT devices are restricted by a maximum transmission power of either 20 or 23 dBm [106], [107], while Release 14's new class imposes further restrictions of 14 dBm. Smaller, simpler batteries such as relatively common *coin batteries* can feasibly power 14 dBm devices, leading to physically smaller UEs. Allowing smaller UEs makes NB-IoT feasible for use cases requiring compact devices, however the reduced transmission power also decreases link budget from 164 to 155 dB. As always, a trade-off between energy-efficiency and range is present.

Release 14's multicast capabilities allow for more energy-efficient transmission to systems where many UEs require the same downlink message such as smart streetlights, and improved handling of over-the-air firmware management. In addition, improved location services significantly increase NB-IoT's applicability to logistics, transportation, and other use cases where devices 'move'.

Existing literature presents conflicting values for NB-IoT's range. Ismail [4] and Qadir *et al.* [9] both provide values of 15 km, in contrast to Li *et al.*'s [108] claim of 35 km. These inconsistencies are possibly explained by Wang *et al.* [100] who demonstrate NB-IoT's range depends on the length of the *cyclic prefix*(CP) prepending PRBs. PRBs with CP time-on-air of 66.67 μs achieve up to 10 km range, while PRBs with CP time-on-air of 266.7 μs achieve up to 40 km range. However, these do not separate the range into *urban* and *rural* settings. In 2018, Ericsson and Australian provider Telstra [109] used enhanced software to extend NB-IoT's rural range from 40 to 100 km without requiring modifications to base station hardware. This will logically increase the urban range by a similar magnitude; however, no numeric measurement is available. Consequentially, we can only conclude that the maximum urban range is below 100 km.

C. LTE-M

LTE-M was introduced alongside NB-IoT in 3GPP Release 13 and further enhanced in Release 14. Both standards deliver very different solutions and are intended to complement each other and co-exist. NB-IoT is a typical LPWAN standard targeting a massive number of UEs transmitting small amounts of data, while LTE-M endeavors to deliver high-performance networking to a smaller number of UEs.

LTE-M is set apart from all other solutions in this paper for its broadband-like networking capabilities. The demand for higher-performance IoT solutions is only growing with time, and a larger number of stakeholders are requesting high-criticality or low-latency functionality over IoT. Release 13 ensured LTE-M was capable of positioning, voice streaming, and video streaming [95] and Release 14 further optimized these capabilities for greater performance and efficiency. Release 14 also introduced multicast capabilities to LTE-M for greater efficiency in over-the-air firmware updates and simultaneous commands or actuations to many devices.

Deployment of Cat M1 demonstrated its low-level broadband capabilities that are often insufficient for high-performance IoT systems, providing a maximum data rate of 1 Mbps both uplink and downlink with a bandwidth of 1.08 MHz [110]. In response, Release 14 introduced Cat M2 allowing bandwidth of 1.4, 5, or 20 MHz downlink and 1.4 or 5 MHz uplink [93]. Utilizing a 5 MHz uplink bandwidth achieves data rates up to 4 Mbps downlink and 7 Mbps uplink, while 1.4 MHz bandwidth can reach 3 Mbps uplink. Increasing maximum TBS contributed to this improved performance, alongside increasing the allowed number of HARQ processes as seen in Cat NB2.

TABLE 3. LTE-M coverage enhancement modes.

	Repeated transmissions	Allowed modulation schemes	Power output
Mode A	32	QPSK, 16-QAM	Variable
Mode B	2048	QPSK	Always Maximum

Nokia's white paper [97] stated that while LTE-M UEs require less transmission power than NB-IoT, the modems themselves are over 5% more complex. Unlike NB-IoT, LTE-M makes no changes to the standard LTE architecture, allowing UEs to operate on any LTE network assuming cells can process bandwidth-limited communications [95].

Several steps have been taken to extend the physical coverage and range of LTE-M signals. By default, LTE-M has a coverage extension of 15 dB to help signals penetrate through obstacles such as walls [12], [95], [97], [111]. It is unknown how useful this will be, as indoor penetration increases power requirements by 20 dB and 'deep indoor' penetration such as basements increases it by 30 dB [96].

LTE-M implements 3GPP's *Coverage Enhancement*(CE) technique. Table 3 summarizes the characteristics of the modes available for this standard.

D. EC-GSM

As the name suggests, EC-GSM (*Extended Coverage* GSM) uses existing GSM and GPRS infrastructure for IoT connectivity [13]. Existing infrastructure has been enhanced for IoT by improving coverage, security, and energy efficiency, while remaining backward-compatible with GSM [112]. This is achieved through an additional 20 dB of link budget, PSM, and eDRX. GSM's voice capability has been removed, but SMS messaging is still supported [13]. Furthermore, GSM only supports DRX cycles up to 11 minutes while EC-GSM can support 52 minutes.

EC-GSM uses the GSM network for communications and therefore, conforms to the GSM architecture. IoT traffic is sent through the GPRS sub-system's Gateway GPRS Support Node (GGSN) and multiplexed with existing traffic. GSM/GPRS communications are widely distributed worldwide, though have been decommissioned in many wealthier countries. Fully decommissioning sites is costly, making the concept of re-purposing GSM hardware and frequencies attractive to telecom organizations. The sheer amount of GSM infrastructure gives the platform a vast potential market presence, particularly in developing countries where LTE is yet to be widely deployed.

EC-GSM supports both GMSK (Gaussian Minimum Shift Keying) and 8PSK modulation schemes. Tabbane [13] stated that depending on coverage extension scheme used, GMSK

TABLE 4. LPWAN specifications.

Specification	SigFox	LoRaWAN	Weightless-P	NB-Fi	D7AP (DASH7)	NB-IoT	LTE-M	EC-GSM
Operating Frequencies	Between 865-924 MHz [40]	433/868/780/915 MHz ISM [63]	Sub-GHz ISM Band [3]	433 MHz, 868.8 MHz, 915 MHz ISM [79] [82] [113]	433 MHz, 868 MHz, 915 MHz ISM [86]	LTE Licensed Spectrum	LTE Licensed Spectrum	GSM Licensed Spectrum
Message Bandwidth	100 Hz [114]	7.8-500 kHz – In practise either 125, 250 or 500 kHz. [5] [7] [11]	12.5 kHz [77]	50 Hz [82]	18-21 kHz (*Lo-Rate*), 150-180 kHz [86]	180 kHz 200 kHz if deployed in GSM band [99] [107]	1.08 MHz UL/DL (Cat M1) [110] 1.4, 5, or 20 MHz DL, 1.4 or 5MHz UL (Cat M2) [93]	200 kHz (GSM Bandwidth) [12]
Downlink Communications	Very limited	Yes	Yes [3] [77]	Yes [82]	Yes	Yes	Yes	Yes
Duplexing Scheme	Limited HD [3] [4] [7]	HD C-SS [3] [4] [5] [7] [11]	HD [77]	Full Duplex [82]	Half Duplex [85]	HD FDD [110] [107]	FD, HD FDD, HD TDD [112] [110]	HD FDD [110]
Packet Size	12 bytes UL, 8 bytes DL [3] [7]	19-250 bytes	5-260 bytes (GMSK) 131-514 bytes (OQPSK) [70]	Unknown	0 - 256 bytes [86]	16-2536 bit TBS [107] [92] [106]	Max TBS 1000 bits (Cat M1) [111] Max TBS 2984-6968 bits UL, 4008 bits DL (Cat M2)	Unknown
Uplink Modulation	DBPSK [3] [4] [7]	LoRa C-SS [3] [4] [5] [7] [11]	GMSK, offset-QPSK [3]	DBPSK [82]	2-GFSK [86]	QPSK, BPSK [4] [5] [91] [12] [115] [107]	BPSK, QPSK, 16QAM or 64QAM [12]	GMSK or 8PSK [13]
Downlink Modulation	GFSK [3] [4]	LoRa C-SS [3] [4] [5] [7] [11]	GMSK, offset-QPSK [3]	DBPSK [82]	2-GFSK [86]	QPSK [4] [5] [91] [12] [115] [107]	BPSK, QPSK, 16QAM or 64QAM [12]	GMSK or 8PSK [13]
Multiple Access Scheme	R-FDMA [9] [114] [34] [36]	Pure ALOHA [3] [11] [9] [116]	TDMA/FDMA [3] [73]	Unknown	CSMA-CA [86]	SC-FDMA (UL), OFDMA (DL) [5] [43] [99] [12] [115] [105] [107]	OFDMA (DL), SC-FDMA (UL) [12] [117]	TDMA/FDMA [110]
Encryption	Optional AES-128 [3] [4] [36] [118] [11]	AES-128 [3] [11]	AES-128, AES-256 [3]	XTEA-256 [79] [82] [113]	AES-128 [86]	3GPP 128-256 bit [7] [11]	3GPP 128-256 bit	3GPP 128-256 bit [7] [11]
FEC	No [3]	Yes [3]	Yes [3]	Unknown	Yes [86]	Yes [119]	Used for e-MBMS [120]	Yes [121]

achieves speed between 350 bps to 70 kbps. 8PSK is capable of a much faster 240 kbps, however, this also increases power consumption and BER [72].

VII. COMPARISON

This section compares all LPWANs examined above and ranks them on the extent to which they meet LPWAN's design

TABLE 5. Power parameters.

Specification	SigFox	LoRaWAN	Weightless-P	NB-Fi	D7AP (DASH7)	NB-IoT	LTE-M	EC-GSM
Uplink Sensitivity	-142 dBm (100 bps) -134 dBm (600 bps) [114]	-137 dBm [118] [12]	131 dBm at 0.625 kbps [77]	-148 dBm [83] [122]	-97 to -110 dBm [85]	LTE Tower Sensitivity	-132 dBm [12]	GSM Tower Sensitivity
Downlink Sensitivity	-130 dBm (100 bps), -129 dBm (600 bps) [46]	-137 dBm [118] [12]	120 dBm at 6.25 kbps [77]	-148 dBm [83] [122]	-97 to -110 dBm [85]	-141 dBm [123] [107]	-132 dBm [12]	-121 dBm [121]
Sleep Mode Power Consumption	6 nA [36]	1 µA [5]	Less than 4µA [77]	1.5µa [82]	1-2 µA [124] [90]	3 µA [125]	8 µA [125]	10 µA [121]
Transmission Power	14 dBm UL/27 dBm DL (100 bps) 22 dBm UL/30 dBm DL (600 bps) [46]	14 dBm UL/DL (Europe) 20-30 dBm UL, 27 dBm DL (USA) [20]	15 dBm [77]	14 dBm, 16 dBm, 27 dBm [126]	10 dBm (433 MHz), 27 dBm (868/915 MHz) [85]	20-23 or 14 dBm [96] [91] [101] [107] [92]	20 dBm [12]	23 or 33 dBm [13]
TX Power Consumption	10-50 mA [36] [118]	28 mA [118]	49 mA [77]	250 mA at 27 dBm, 90 mA at 16 dBm, 44mA at 14 dBm [82]	29.2 mA at 10 dBm [124]	74-220 mA [125]	380 mA [127] [125]	1228 mA (33 dBm, 4.051W, 3.3V) [106]; 152 mA (23 dBm, 0.503W, 3.3V) [106]
RX Power Consumption	10 mA [118]	10.5 mA [118]	13 mA [77]	12 mA [83]	15 mA [124]	46 mA [125]	53.33 mA [127] [125]	66 mA [121]
Reported Battery Life	4 years (3.3V/1Ah) [128] 10 years (3.6V lithium AA-cell) [129] [130]	10 years [118] (9V battery) [131]	3-8 years (Coin-cell) [132]	20 years (AA-cell) [11] [133]	10 years [85] [134] [135] (Coin-cell or thin-film) [136]	10 years (5Wh battery) [11]	10 years [97] (5Wh battery) [137]	10- 14 years (5Wh battery) [11]

goals as stated in Section II. Rankings are determined by examining specifications and test results reported in previous research. The ranking outcomes are then compared to the design decisions discussed in Section III and their impact as summarized in Section IV. All specifications discussed in the preceding two sections are summarized in Table 4. Additionally, power consumption metrics are summarized in Table 5, and performance metrics in Table 6. Weightless-W and Weightless-N have been excluded from these rankings as they have been superseded in favor of Weightless-P.

Data rate is not a core LPWAN requirement like those laid out in Section II, however, it is evaluated for each LPWAN in the remainder of this paper. Data rate often determines whether an LPWAN is suitable for a given business case, especially for supporting time-critical applications.

A. ENERGY EFFICIENCY

Three measures of power consumption have been provided for each LPWAN in Table 5, which are: i. *RX Power Consumption*, ii. *TX Power Consumption*, and iii. *Sleep Mode Power Consumption.* Alongside these, existing literature has provided reports on battery life for each protocol. In practice, battery life will vary between use cases and the type of battery. For example, using the same transceiver, a data logger that sends a small value once daily will last much longer than a water quality monitoring sensor sending hourly data from a treatment plant. Values reported for battery life in the table are averages or estimates provided by the manufacturer or through independent research.

Some LPWANs allow operators to adjust TX power to more specifically suit their requirements. Increasing TX

TABLE 6. Performance specifications.

Specification	SigFox	LoRaWAN	Weightless-P	NB-Fi	D7AP (DASH7)	NB-IoT	LTE-M	EC-GSM
Link Budget	163.3 dB [47]	155 dB UL/DL (Europe) 154 dB UL, 157 dB DL (USA) [20] [5]	160 dB [76]	Varies with TX Power – 30 dBm allows 174 dB	140 dB [85]	164 dB (20 or 23 dBm), 155 dB (14 dBm) [4] [99] [106]	155.7 dB [110]	164 dB (33 dBm), 154 dB (23 dBm) [118] [13]
Estimated Range (Urban)	10 km [3] [4] [7] [10]	5 km	2-5 km (Depending on Urban Density) [76] [75]	10 km [79] [80]	1-2 km [85]	<100 km [109]	<11 km [97] [13]	<15 km [4] [97] [13]
Estimated Range (Rural)	50 km [3] [7] [10] [43]	18 km	~25 km [76]	30 km [79] [80]	1-2 km [85]	100 km [109]	11 km [97] [13]	15 km [4] [97] [13]
Base Station Capacity	Over 1,000,000 [11]	Over 1,000,000 [11]	Unlimited [138]	2,000,000 nodes [79] [82]	Unlimited [85] [135]	52,547 [101] [105]	80,000 (security enabled) 1,000,000 (security disabled) [139]	50,000 [13]
Uplink Data Rate	100/600 bps [40]	0.3 – 50 kbps [5] [7] [11] [3] [60] (Dependent on spreading factor)	0.625 kbps – 100 kbps [77]	50-25600 bits/second [82] [83]	9.6 kbps *(Lo-rate)*, 55.555 kbps *(Normal)*, 166.667 kbps *(Hi-Rate)* [86]	106 kbps (1 HARQ), 158.5 kbps (2 HARQs) [92]	1 Mbps (Cat M1) [12] [110] 3-7 Mbps (Cat M2) [93]	0.35 – 70 kbps (GMSK) [97] 0.35-240 kbps (8PSK) [72]
Downlink Data Rate	600 bps [40]	0.3 – 50 kbps [5] [7] [11] [3] [60] (Dependent on spreading factor)	6.25 kbps – 100 kbps [77]	50-25600 bits/second [82] [83]	9.6 kbps *(Lo-rate)*, 55.555 kbps *(Normal)*, 166.667 kbps *(Hi-Rate)* [86]	79 kbps (1 HARQ), 127 kbps (2 HARQs) [92]	1 Mbps (Cat M1) [12] [110] 4 Mbps (Cat M2) [93]	0.35 – 70 kbps (GMSK) [97] 0.35-240 kbps (8PSK) [72]

power will increase the link budget and therefore range, however, it will also increase TX power consumption and decrease battery life. This is an embodiment of the trade-offs seen in LPWAN requirements and supported by NB-Fi, EC-GSM, and NB-IoT as of 3GPP Release 14. TX power can also vary between regions depending on local regulations.

It can be observed that cellular solutions consume more power than unlicensed-spectrum solutions. RX power consumption varies little between unlicensed-spectrum solutions, however there is significantly more variety in TX power consumption. SigFox, LoRaWAN, and D7AP have the lowest TX power consumption – however, it should be noted D7AP's value was obtained for 10 dBm transmission power, while the lowest available value for SigFox and LoRa is 14 dBm. This is followed in ascending order by NB-Fi and Weightless-P. TX power consumption for 14 dBm transmission power almost doubles between LoRaWAN and NB-Fi, while there is no significant increase between NB-Fi and Weightless-P.

TX power consumption significantly increases between Weightless-P and NB-IoT, and even further between NB-IoT and LTE-M. The increase between NB-IoT and LTE-M is significant, as transmission power is very similar in both networks. In addition, RX power consumption increases by over 300% between DASH7 and NB-IoT. RX power consumption is significantly more varied between licensed-spectrum solutions than between those utilizing the unlicensed spectrum.

Interestingly, observing link budgets between LPWANs shows that link budget does not always increase with TX power consumption. Increases in TX or RX consumption can also be caused by complex modulation schemes, channel access techniques, and signal diversity schemes requiring repeated transmission. For example, SigFox uses approximately 50 mA to transmit a message, however, transmits each message multiple times due to its frequency and time diversity schemes.

Sleep-mode power consumption is another important parameter, and arguably the most influential for the many sensors that spend the majority of time in a low-power state. As always, cellular solutions consume more power than unlicensed-spectrum LPWANs – however, the gap between

NB-IoT and unlicensed-spectrum networks is quite narrow. Notably, SigFox uses far less power during sleep-mode than other LPWANs. This, combined with its highly restricted downlink capabilities, solidify its suitability for uplink-only sensors or data loggers.

Comparing LPWAN energy consumption supports several assessments made in Sections III-IV. The ALOHA multiple access method and similar R-FDMA are respectively utilized by LoRaWAN and SigFox, which utilize the least power during message transmission and receipt. Table 1 of Section IV indicates moderate impact of modulation techniques such as binary schemes on energy efficiency. This is supported by the fact that SigFox and NB-Fi are very energy-efficient and utilize BPSK on the uplink channel. LoRa modulation is also claimed to be very energy-efficient, and this is reflected in LoRaWAN's low power consumption.

Sections III-IV also state that duplexity significantly affects power consumption, with FD solutions consuming the most power. NB-Fi and LTE-M are the only LPWANs capable of FD communications, and respectively consume the most power of all unlicensed solutions and out of all solutions. However, without knowing NB-Fi's multiple-access scheme, the full significance of its duplexity is unknown.

B. LONG RANGE

Range can be evaluated by considering both how far an LPWAN can communicate from its base station, and its ability to penetrate obstacles. Consequentially, many LPWANs have both *urban* and *rural* ranges provided, assuming rural areas are less obstructed. However, obstructions such as trees and geological features are still present in rural areas [140]. While we have provided distinct urban and rural ranges for unlicensed-spectrum LPWANs in Table 6, only single values were found in previous literature for cellular solutions. However, we can provide a relative ranking with the assumption that higher rural ranges result in higher urban ranges, and vice versa. In the case of NB-IoT, we know that the high range of 100 km was achieved in a rural area [109].

We also assume that the values provided for EC-GSM and LTE are achieved in rural areas, as LoRaWAN achieves similar values in urban areas with a very similar link budget. In these cases, urban range is specified as *less than* the rural range. Weightless-P is an unusual example, capable of communicating over very long distances in rural areas but having a very short range in urban areas. In fact, Weightless- P fails to meet Section II-B's target of 5 km in urban environments.

Lauridsen *et al.* evaluated the obstacle penetration capability of various LPWANs in wide rural areas in [96] and [139]. These studies demonstrated that indoor environments with 20 dB penetration loss respectively cause 1% outage for NB-IoT, LTE-M, and SigFox, and 2% for LoRaWAN. Additionally, deep-indoor environments with 30 dB penetration loss respectively cause 8% outage for NB-IoT, 13% for SigFox, and 20% for LoRaWAN and LTE-M. Other studies [141], [142] have shown LoRaWAN performs well at through-wall indoor communications, with Petajajarvi *et al.* [143] reporting an average success rate of 96.7%. WAVIoT, the manufacturers of NB-Fi, claims it has superior obstacle penetration to SigFox and LoRaWAN. Cetinkaya and Akan [135], alongside Piromalis et al. [134], claim D7AP performs well at penetrating walls, water, and concrete. While not referencing specific obstructions, both [90] and [124] generally state D7AP has good obstacle penetration.

Sections III-IV observes that signal diversity techniques are used to extend communications range, and this is a well-known principle demonstrated by 3GPP's Coverage Enhancement (CE) feature [92], [95]. LTE-M has a comparable range with other LPWANs and a significantly wider band in the order of megahertz. NB-IoT also has a wider band than several LPWANs but is capable of the longest-distance communication. The relationship between diversity techniques and range is further supported by SigFox, which utilizes triple diversity techniques and has the second-highest range following NB-IoT. Manufacturing-driven systems are also assessed to provide better range as network owners can install additional base stations or repeaters without restriction from a provider. However, there is still a practical limit to the effectiveness of doing this.

Licensed-spectrum solutions theoretically provide better range due to the lack of regulatory restrictions limiting transmission power. While the licensed-spectrum NB-IoT's have significantly higher ranges than other LPWANs, the second and third-highest ranges (rural) belong to SigFox and NB-Fi respectively; both unlicensed-spectrum solutions. SigFox and NB-Fi also achieve very good urban range. It is thus observed that even with these enforced limitations on transmission power, LPWANs are able to increase coverage through the other techniques discussed in this paper. Despite this, NB-IoT's range is significantly higher than all other LPWANs discussed, and it is uncertain at this stage whether this could be achievable with regulatory limits on transmission power.

We consider NB-IoT, SigFox, and NB-Fi as having the leading communication ranges of all LPWANs discussed. NB-IoT is the clear leader, capable of communicating up to 100 km in rural areas and exhibiting leading obstacle penetration. This is followed by SigFox, which had the second-best obstacle penetration in Lauridsen *et al.*'s studies and is capable of communicating 50 km in rural areas. NB-Fi also has a very long range of 30 km, and reportedly good obstacle penetration. Weightless-P and D7AP both have comparatively short ranges, with both falling short of the 5 km target established in Section II. D7AP has the lowest overall range, limited to a single kilometer if sub-controller relays are not utilized [85].

C. SCALABILITY

Structural scalability is relatively easy to rank, as quantitative measurements of base station capacity are available for each LPWAN. Weightless-P and D7AP are the clear leaders with unlimited capacity, followed by NB-Fi with 2,000,000 nodes. SigFox and LoRaWAN both place third, allowing 'over

1,000,000' potential devices. LTE-M has the highest structural scalability of licensed spectrum solutions, allowing 80,000 nodes when security is enabled. While a value comparable to unlicensed spectrum solutions of 1,000,000 nodes is achievable when security is disabled, we will not consider this as the risk is unacceptable. NB-IoT follows LTE-M with 52,547 nodes, and EC-GSM has the lowest observed structural scalability with only 50,000 nodes. While Weightless-P and D7AP have the highest capacity, we will rank them below NB-Fi as the practical number of connected nodes are limited by their low communication ranges.

Licensed spectrum networks have superior overall load scalability to unlicensed networks as they are not subjected to regulatory restrictions. As unlicensed solutions are impacted by restrictions, their load scalability depends on the specific regulations that apply.

SigFox ranks the lowest due to harsh restrictions where devices are only permitted to send six uplink messages per hour and receive four downlink messages per day in response to uplink messages. This is followed by LoRaWAN and D7AP – a lack of LBT/AFA mechanisms subjects LoRaWAN to heavier restrictions in ETSI zones, while a lack of spread-spectrum modulation subjects D7AP to heavier restrictions in FCC zones. In contrast, Weightless-P supports both LBT/AFA and spread-spectrum functionality, allowing it to rank higher in scalability. At the time of writing, no further information was available regarding NB-Fi's multiple access techniques or compliance with regulatory restrictions.

This section's rankings show that unlicensed-spectrum solutions provide greater structural scalability while licensed-spectrum solutions provide higher load scalability. Deploying a network often requires stakeholders to choose between structural and load scalability, with no solution currently offering both - this is addressed further in Section IX.A while discussing research challenges. This section's ranking confirmed the relationships between load scalability and LPWAN design decisions outlined in Sections III-IV.

D. LOW COST

It is difficult to estimate a definite cost for each LPWAN as many variables are involved such as regional prices, subscription fees, and inflation. However, it is possible to scale prices by reviewing previous studies and compare prices offered by manufacturers or telcos. We will prioritize the subscription fees of *Subscriber-Driven*(SD) networks and ongoing maintenance costs of *Manufacturing-Driven* networks (MD) before upfront transceiver cost, as periodic payments soon exceed outright device investment. All dollar values provided in this section are in United States Dollars (USD).

Most LPWANs discussed in this paper are SD networks, and those using the licensed spectrum are more expensive because of licensing fees imposed on the provider. LoRaWAN, Weightless-P, and D7AP are the only *Manufacturing-Driven* networks discussed, allowing organizations to deploy their own networks and infrastructure. Both business models will incur annual cost; SD networks require the obvious subscription fee, while organizations deploying MD networks incur the cost of running and maintaining the network. Interestingly, as a consequence of its popularity, LoRaWAN can also be offered as a SD network by third-party organizations including The Things Network [144].

Depending on an organization's available resources and skill level, maintaining an MD network and its infrastructure could incur a higher cost than SD network fees. The size and complexity of a network also influence which business model is more cost-effective, however available resources and skills also contribute to this.

The NB-Fi Alliance state [126] NB-Fi annual subscription fees range from $5.60 to $4.10 per device depending on the total number of devices. SigFox and their trusted providers offer both *discovery* and *enterprise* subscriptions [145]. Discovery pricing is made on a per-device basis, and annual cost per device varies with country and desired daily message limit. As of December 2019, this ranges between $13.75 and $33.00 in the United States. *Enterprise* subscription is available for networks exceeding 1000 devices; however, customers are instructed to directly contact SigFox to establish a pricing agreement.

As there is no subscription fee, comparing manufacturing-driven requires comparing the individual device cost. An article [146] by the Chair of Weightless SIG's marketing group states that Weightless-P transceivers can be implemented for between $1-5. A study by Mekki *et al.* [7] also claims that LoRa devices cost between 3 and 5 euro, or $3.3 - 5.6. Thus, we can consider Weightless-P and LoRaWAN equivalent in cost. However, if deploying and maintaining a private network is too costly when compared with the network's purpose, we consider LoRaWAN cheaper as there are many options available for subscribing to a third-party-network.

Ayoub *et al.* [85] report that D7AP gateways cost between $100-1000, contrasting this with a $15000 NB-IoT base station. Piromalis state that D7AP end devices are expensive to implement for a number of reasons stated in [134]. However, no specific price information for end devices could be found at the time of writing.

When comparing subscription costs for licensed spectrum solutions, LTE-M is the most expensive. Telcos charge according to data usage and bandwidth, and LTE-M offers far more of those resources than NB-IoT and EC-GSM.

In light of the above discussion. SigFox and NB-Fi appear to be the least expensive solutions, as their low subscription fees will incur less cost than maintaining and powering even small private networks. SigFox transceivers have upfront costs of $2-3 per device [147], while NB-Fi transceivers cost $4.99 [126]. LoRaWAN can often also allow this, as there are many providers offering connection to existing LoRaWAN networks as a service. As we have considered Weightless-P and LoRaWAN equivalent in cost, unlicensed spectrum solutions lead at cost-efficiency.

This discussion confirms the statements in Sections III-IV that licensed spectrum solutions are more expensive, however

other relationships established in that section also play a role in determining cost. Utilizing ALOHA multiple access is stated to reduce cost, and two of the lowest-cost LPWANs utilize either ALOHA (LoRaWAN) or the similar R-FDMA (SigFox). LoRaWAN's own LoRa modulation is also stated to be very low-cost, although modulation technique has a relatively small effect on cost.

However, not all relationships in Sections III-IV are supported. Using diversity techniques or full duplexity are stated to significantly impact cost. SigFox makes heavy use of diversity techniques and NB-Fi offers full duplexity, and these are both among the least expensive LPWANs.

E. INTERFERENCE MANAGEMENT

In contrast to the previous discussions throughout this sub-section, we will supplement this by utilizing the analysis in Sections III-IV to evaluate the relative interference-management capability of the LPWANS discussed.

While both licensed and unlicensed-band solutions are at the risk of malicious jamming, unlicensed-band solutions also risk 'accidental' interference from co-existing networks. UNB modulation greatly reduces the risk of accidental interference, however, increases the ease of malicious jamming. Spread-spectrum technologies are somewhat resistant to both malicious and accidental interference, particularly when used with a Forward Error Correction (FEC) mechanism.

Sources (e.g., [5], [7]) claimed that NB-IoT has a 'low' interference immunity compared to LoRaWAN and SigFox. While it is far less likely to encounter interference in a licensed band, its use of UNB modulation makes it open to malicious jamming. SigFox also utilizes UNB modulation, however its use of frequency-hopping mitigates the risk of malicious jamming. While comparable to NB-IoT operating in a narrow band of licensed frequency, EC-GSM is at even greater risk of malicious jamming as it utilizes less-advanced TDMA/FDMA channel access. LTE-M is perhaps the most resistant of all cellular solutions to malicious jamming as it operates over a wider band and utilizes robust OFDMA channel access. This is further enhanced in Release 14's Cat. M2 standard that communicates over an even wider band.

LoRaWAN's C-SS modulation sees it rank first for interference handling, however, other unlicensed spectrum networks employ their own methods. D7AP utilizes FEC and PN9 data whitening, does not require beaconing or periodic synchronization messages, and each end device can maintain a whitelist of devices permitted to communicate [84]. Weightless-P and SigFox are both capable of frequency-hopping [70], with Weightless-P also utilizing FEC error correction [3]. SigFox and NB-Fi are very interference-resistant by nature due to their respective UNB bandwidths of 100 Hz [114] and 140 Hz [82].

This discussion supports the statements in Sections III-IV that LoRa and UNB modulation schemes provide robust interference resistance, along with resulting frequency bands that are either very narrow or distributed over wide bands using a spread-spectrum technique. SigFox and Weightless-P also utilize FH-SS spread spectrum at the multiple access level, which is stated to significantly benefit interference resistance. Considering that SigFox uses UNB and FH-SS alongside several diversity techniques, and LoRaWAN uses its own LoRa protocol, the claims that the two protocols resist interference better than NB-IoT can be theoretically supported. Considering the previous paragraph's discussion, we also rank D7AP highly among unlicensed-spectrum solutions.

F. INTEGRATION

SigFox and NB-Fi rank very highly for integration as cloud platforms, user-facing tools, and APIs are core components of the system and are offered with every subscription. While D7AP is manufacturing-driven and users deploy their own networks, we have ranked it equally with SigFox and NB-Fi because of its robust API and querying system described in Section V.E. Piromalis *et al.* additionally state that D7AP is natively compatible with RFID readers and tags [134], potentially allowing a wealth of integration with existing systems.

Weightless-P also offers a cloud platform and APIs for users [74], however as users can deploy their own network, this is likely an optional and less coupled feature.

LoRaWAN and cellular technologies do not have central platforms provided by the specification-holder. However, LoRaWAN's specification includes an *Application Server* intended to facilitate integration with external systems. In addition, NB-IoT has components for machine-type data not found in the general LTE standard, fostering integration with M2M systems.

The large market-share of LoRaWAN has resulted in a myriad of platforms and tools being made available. Third-party organizations offer LoRaWAN as-a-service, and many of these provide their own cloud platforms; an example of this is the robust ecosystem offered by LoRaWAN-as-a-service provider *The Things Network* [148]– [150]. For organizations deploying a completely private network, integration tools such as *LoRaServer* [151] are also available. NB-IoT also has a high market-share, however telcos are responsible for providing methods of integrating with their network. An example of this is the Australian telco Telstra, who have provided their own platform [152] for integrating IoT devices. This platform is also compatible with LTE-M, as Telstra aims to incorporate both standards into its IoT network. It is therefore possible other telcos will do the same [153].

Most design decisions discussed in Sections III-IV are irrelevant to integration, and consequentially integration is not discussed in that section. However, subscriber-driven solutions generally rank higher for integration as the owning organization will provide first-party tools and services to subscribers. Despite this, some manufacturing-driven networks rank very highly thanks to robust tools developed by the standard holders or even third-party organizations.

We assess that SigFox, NB-Fi, and D7AP are the most integrable systems as first-party platforms exist facilitat-

TABLE 7. Performance of LPWANs for each requirement.

Requirement	Leading Performers	Worst Performers
Energy Efficiency	Unlicensed-spectrum networks	LTE-M, EC-GSM
Range	NB-IoT, SigFox, NB-Fi	Weightless-P, D7AP
Structural Scalability	Unlicensed-spectrum networks	EC-GSM, NB-IoT
Load Scalability	Licensed-spectrum networks	SigFox, LoRaWAN
Low Cost	Unlicensed-spectrum networks	Licensed-Spectrum Networks
Interference Management	Licensed-spectrum networks	Unlicensed-Spectrum Networks
Integration	SigFox, NB-Fi, D7AP	EC-GSM

ing integration and providing management tools. We also assess that EC-GSM is the least integrable system – not only are there no first-party tools provided, but it is based on older infrastructure than other licensed-spectrum systems.

G. DISCUSSION

Table 7 identifies which systems are the most effective ones at meeting each of Section II's LPWAN goals. This confirms earlier statements that data rate is often sacrificed for LPWAN requirements. LTE-M has a data rate significantly higher than any other solution but consumes more power and has a lower communications range. Most of the assessments in Sections III-IV are also confirmed, with the stated impact of design decisions and use of leading techniques observed throughout the LPWANs discussed. However, as so many design decisions apply to each LPWAN, these relationships are rarely straightforward.

A degree of trade-off is present between each LPWAN ensuring that no individual network can surpass others at meeting all requirements. SigFox is the least expensive LPWAN, has excellent communications range and obstacle penetration, however, it also has the lowest load scalability and data rate. NB-Fi improves on these parameters but is more expensive and has lower communications range. This pattern can be seen when observing each platform – each excels in one or more areas but also falls short in others.

Each application places a different priority on the LPWAN requirements; some applications will require higher data rates, some will require longer communications range, and so forth. The trade-offs between LPWANs we have determined in this section creates an ecosystem where each LPWAN is more suitable for some applications and less for others. In the next section, we will elaborate on this and assess which LPWANs are suitable for a variety of applications. The results of this section will be used to determine this.

VIII. APPLICATION SUITABILITY OF TECHNOLOGIES

In this section, we examine eight LPWANs to assess their suitability for diverse use cases across various domains. For each domain and prominent use cases, we systematically evaluate how well each LPWAN outlined in preceding sections fulfills LPWAN requirements. Table 8 summarizes the importance of each LPWAN requirement to each domain categorized in different levels and lists suggested LPWAN technologies to use.

In the following section, each domain, and its more specific use cases are discussed in an individual subsection. We extensively review works in literature that reported trails of LPWAN technologies in each domain as well as previous works recommending LWPANs for each and provide justifications if our assessment is different from previous recommendations. Subsections also discuss requirements that are more specific to individual use cases and not listed in Table 8. Finally, we conclude each subsection by selecting appropriate LPWANs and explaining our reasoning.

We also classify use cases as critical or non-critical. Failure of systems implementing critical use cases risks human life, the environment, or significant financial loss. Unless otherwise specified, critical systems require high reliability and data rates capable of real-time communication. Qadir *et al.* [9] provide a minimum value of 28.8 kbps for real-time communications that we will use as a benchmark. In addition, LPWANs with low load scalability due to factors such as duty cycle restrictions are completely unacceptable for any critical system.

It should also be noted that in the right circumstances, any domain can have a small number of outlier use cases with different requirements to those we discuss, with business interests identifying several others under unique circumstances. Exceptions will always exist, but for the sake of brevity we only cover reasonably common or predictable use cases.

A. METER READING

Laveyne *et al.* [154] classify smart electrical meter communications as *Automated Meter Reading*(AMR), *Time of Use*(TOU), *Outage Monitoring*(OM) and *Quasi-Real-Time Monitoring*(QRM). AMR is the 'typical' meter reading function that sends utility consumption to the relevant authority, while OM sends alarms uplink if an outage or fault occurs. TOU messages are commands received to temporarily change prices, and QRM sends a wide range of information uplink at least every five minutes. AMR and TOU have low throughput requirements, while OM and QRM conversely require high throughput.

Qadir *et al.* [9] claim smart metering does not utilize mobility or real-time communications, only requiring low-medium bitrates. Consequentially they claim almost any LPWAN technology is suitable for meter reading, only excluding SigFox as its strict duty cycling limits its capability to send OM messages. Wang and Fapojuwo [116] support the claim that smart metering does not require high bitrates but stress

the importance of wide coverage. Unlike [9] they recommend SigFox as a potential solution, alongside NB-IoT and LoRaWAN.

Mekki *et al.* [7] recommend NB-IoT, claiming smart meters require high bitrates for frequent communications and alarms. They also state long range is not required as meters are usually deployed in densely-populated areas – an assumption which will no longer be valid as IoT systems are also seeing increasing deployment in rural areas. Cetinkaya and Akan recommend D7AP for smart metering in [135], however, we believe its short range could be insufficient for metering systems encompassing entire urban areas.

We assess NB-IoT as the first choice for meter reading considering its high data rate, its high load scalability, very wide coverage, and leading obstacle penetration over wide areas [96]. Multicast communications introduced in 3GPP Release 14 [93] facilitate more efficient TOU communications. However, NB-IoT may not always be affordable for smart meter systems, is less structurally scalable, and may not be available in some areas. LoRaWAN, NB-Fi, or SigFox can provide alternative solutions if NB-IoT is unaffordable or unavailable.

LoRaWAN has a data rate sufficient for AMR, TOU, and OM communications, supports a massive number of devices per base station, and has a good battery life [96]. As operators can deploy their own networks, LoRaWAN is technically available anywhere. However, LoRaWAN is somewhat inhibited by its relatively short range and low load scalability. In addition, SigFox and NB-IoT provide improved obstacle penetration [96] over long distances, especially in 'deep-indoor' environments.

NB-Fi is also a good candidate for those meters that solely utilize AMR and TOU communications. Of all the LPWANs we have discussed, NB-Fi has the longest reported battery life and highest number of devices per base station, while also exhibiting good communications range. However, its data rate is insufficient for OM and QRM use cases, and it is not available in all areas.

While not viewed favorably by [7] and [9], SigFox is still recommended for meter reading by [116] and in our assessment, it fills a particular niche. Many utility providers desire a simple, low-cost smart meter system simply reporting values a few times per day. SigFox has wide coverage, is inexpensive, supports over 1,000,000 devices per base station, and has been shown to provide superior deep-indoor penetration to LoRaWAN over long distances [96].

B. SCADA/INFRASTRUCTURE CONTROL

Other use cases discussed here provide network connectivity to previously inert systems. *Supervisory Control and Data Acquisition*(SCADA) systems are an exception, as they have connected industrial machinery and sensors to a central network for decades. SCADA systems range in scope from a single factory floor to urban infrastructure – an example of the latter is a SCADA system connecting an entire urban water infrastructure through integration of components such pumps, valves, and flow meters. In contrast, a smaller-scale SCADA system may only integrate machinery in a single production line. LPWAN-based SCADA solutions must be able to match or surpass the performance of current systems while providing additional benefits.

SCADA systems are often critical with many controlling essential services, dangerous machinery, or hazardous industrial processes. In addition to high speed and reliability, systems must prioritize security and ruggedization as discussed in [155] and [156]. As industrial machinery is often deployed in signal-hostile environments [157], obstacle penetration should also be prioritized.

Qadir *et al.* [9] claim that industrial systems require real-time communications (28.8 kbps) while not requiring mobility, recommending LoRaWAN and NB-IoT. Mekki *et al.* [7] somewhat echo this, recommending NB-IoT for frequent communications and high QoS alongside SigFox or LoRaWAN for non-critical systems requiring longer battery life and lower cost. Grabia *et al.* [124] recommend D7AP for industry 4.0 applications including SCADA in due to its obstacle penetration, low cost, and energy efficiency. D7AP also has a relatively high data rate even exceeding NB-IoT, making it a viable candidate.

LoRaWAN, Weightless-P, D7AP, and all cellular solutions have sufficiently high data rate for real-time communications. We recommend NB-IoT for critical systems requiring high reliability, load scalability, or security, in addition to any system covering a very wide area. For non-critical systems deployed over relatively short distances, we recommend Weightless-P or LoRaWAN. Weightless-P should be used when higher data rate and load scalability take priority or multicasting is required. Conversely, LoRaWAN should be used for systems deployed in signal-hostile or hazardous environments. If systems are deployed over very short distances under 2 km, D7AP is capable of high data rate, robust security, high resistance to interference, and good obstacle penetration.

Many SCADA systems currently utilize the GSM standard's GPRS [155] capabilities, making potential migration to EC-GSM relatively simple. Under these circumstances, a cost-benefit or risk analysis must evaluate the disadvantages of EC-GSM against the relatively simple migration process. As a cellular solution, EC-GSM will also have good load scalability.

C. TRANSPORT

V2X (Vehicle to Everything) is a paradigm where vehicles use attached sensors to communicate with other smart things or systems. V2X systems must be fast, reliable [9], [158], have robust mobility, and handle the Doppler effect well [159].

While many V2X use cases are critical, non-critical use cases such as fleet vehicle tracking also exist.

Li *et al.* [159] claim the performance exhibited by LPWANs is inadequate for critical V2X use cases but still sufficient for those with lower risk. For these lower-risk

applications, they recommend LoRaWAN or LTE-M based on their support for mobility and discourage NB-IoT for its lack of mobility support. This statement, however, has become obsolete as of 3GPP Release 14, reflected with Qadir *et al.*'s recommendation of NB-IoT [9] for transportation use cases on the basis of its mobility and speed. Qadir *et al.* conversely discourage the use of LoRaWAN, claiming it is prone to jitter and delay while noting the contentiousness of its ALOHA multiple access.

Shaik *et al.* developed a vehicular sensor in [160] that utilizes GSM communications to notify ambulances and healthcare workers of accidents, with results showing notifications were immediately sent to the appropriate destinations. This demonstrates EC-GSM is an appropriate solution for accident or fault monitoring in areas where LTE is unavailable, however we still recommend LTE-based networks if available due to their lower latency.

Data flow between electronic components such as brakes, steering, and airbags in vehicles is facilitated by a protocol named CAN Bus [161]. Sensors interfacing with this protocol can achieve autonomous control or real-time monitoring of vehicles. The latest version of CAN Bus is capable of 8 Mbps throughput, although [162] states automobile manufacturers often utilize data rates of 1, 2, or 5 Mbps. Of all protocols discussed, only LTE-M is capable of speeds in the megabit range. This makes it an obvious choice for high-performance interfaces with CAN Bus.

We recommend LTE-M be used for all high-risk V2X systems where possible, and exclusively used when CAN Bus interfacing is required. LTE-M has significantly higher data rate than any other LPWAN protocol and robust multiple access. Li *et al.* [159] also demonstrated LTE-M's Doppler resistance is roughly equal to LoRaWAN, which is known to perform well in this area [57]. Being in licensed band, LTE-M is less susceptible to interference and exhibits improved load scalability.

For lower-risk V2X systems we recommend NB-IoT or LoRaWAN. NB-IoT should be used when data rate or reliability are prioritized but LTE-M is impractical, or when a very wide range is required. If low cost takes priority and somewhat shorter range is not problematic, LoRaWAN should be utilized. We also considered Weightless-P for its mobility support, load scalability, and high data rate; however, it is limited by its short range in dense urban areas. Even vehicles registered in open or rural areas can potentially move through dense urban environments.

EC-GSM is a good alternative if none of the aforementioned systems are practical in a given deployment scenario, with examples of the GSM network being applied to V2X systems present in the existing literature.

D. LOGISTICS

Supply Chain Management(SCM) systems track goods throughout all stages of their progress in the eponymous supply chain. Pundir *et al.* [163] suggest tracking can occur at the vehicle, container, or package level, however we will not consider vehicular tracking in this section as it is covered by Section VIII-C. We will also consider the tracking of individual goods within a single package, as this is becoming increasingly demanded by consumers. The *granularity* of an SCM system becomes finer as tracking occurs at items further down this hierarchy – for example, tracking goods is finer-grained than tracking packages.

Use cases in the logistics domain [164], among some others discussed in this paper, benefit significantly from localization capabilities. Localization determines a device's position relative to another device known as an anchor, which is often a base station but can also be an end device in mesh networks [165]. Silva *et al.* [165] categorize commonly used techniques into power, time, and space domains. Power-domain localization estimates distance using *Received Signal Strength Indicator* (RSSI). However, this requires knowledge of the propagation environment and often relies on an underlying probabilistic model. Accuracy of power-domain methods decreases with network sparsity and frequency, and many devices also use relatively coarse RSSI measurements. Time-domain localization estimates distance using *time-of-arrival* (TOA) or *time-difference-of-arrival*(TDOA) for signals received by at least three nodes. This requires time synchronization between devices, which consequentially increases network complexity and potential overhead. Time-domain accuracy also decreases as bandwidth becomes narrower, with accuracy below one meter only achievable for at least 100 MHz. Finally, space-domain localization determines distance based on received signal's angle-of-arrival through sectorized antennas or antenna arrays. While capable of very high accuracy, its accuracy decreases with distance making it impractical for LPWANs covering a large area. Time and space-domain techniques are also impacted by modulation technique; however, power-domain techniques are not.

SCM systems can also vary in criticality depending on what is being tracked. Mohsin and Yellampalli [166] alongside Lu and Wang [167] discuss cold chain logistics, where goods in transit must be kept within a particular temperature range. Fore *et al.* [168] list other attributes monitored by SCM sensors, and for some goods these will also have acceptable ranges to maintain. For example, some goods must be kept within a particular pH range or not be exposed to a certain level of vibration. Values exceeding these ranges can lead to spoilage, expiry, or even dangerous reactions. To ensure message delivery for critical alarms or actuation commands, we recommend utilizing LPWANs with high load scalability. This allows an increased or even unlimited number of alarms with no minimum time between them.

Mekki *et al.* [7] recommend LoRaWAN for pallet tracking while discouraging the use of SigFox and NB-IoT. LoRaWAN is selected due to its low cost, energy efficiency, and mobility support. NB-IoT is discouraged as it is less likely to be available in rural areas, and SigFox is discouraged due to reduced mobility capabilities. Wang and Fapojuwo [116] partially support this conclusion,

claiming logistics systems require low data rates and long range before recommending SigFox, LoRaWAN, and NB-IoT. Grabia *et al.* recommend D7AP for container tracking in [124] as part of *Industry 4.*0. However, its very low range is insufficient for tracking goods that are in transit over long distances.

Few LPWAN standards offer robust localization capabilities, with Silva *et al.* [165] stating most LPWANs rely on power-domain techniques using regular network traffic. However, the same study also claims power-domain techniques currently offer the best compromise between accuracy and power-efficiency. LoRaWAN, SigFox, NB-IoT and LTE-M are capable of achieving the highest localization accuracy, with Valach and Macko [169] further clarifying NB-IoT has superior accuracy to LoRaWAN. LoRaWAN and SigFox are best suited to power-domain techniques, while NB-IoT and LTE-M are best suited to those in the time domain. As of 3GPP Release 14, both NB-IoT [92], [170] and LTE-M [93] utilize TDOA techniques.

Logistics organizations operating across national borders must also consider LPWAN international roaming capabilities. SigFox natively provides roaming through its monarch feature, which automatically selects the appropriate radio configuration for local regulations [171]. LoRaWAN has also been capable of handover roaming since version 1.1 of the specification [60]. For many other public networks, roaming depends on international agreements between operators. As of December 2019 several of these agreements have emerged or trials have been performed for LTE-M [172], NB-IoT [173], [174], and LoRaWAN-as-a-service [175], [176]. Private networks theoretically only require agreements between owners, however, in practice devices must be capable of adapting to local regulations.

Our assessment recommends NB-IoT for critical tracking systems such as cold-chain and NB-IoT or LoRaWAN for all others. NB-IoT has more accurate localization and a far longer range than LoRaWAN, however is less structurally scalable and more costly. Both networks also support international roaming, with this gaining increased support from operators.

E. RETAIL

In this discussion, the *retail* domain refers to using LPWAN technology for Point of Sale (POS) and Electronic Funds Transfer (EFT) systems. Considering that POS transactions exchange bank account information, security is the highest-priority requirement. Banks often issue firmware updates to connected hardware including critical security patches. Multicast communications should be employed to ensure fast and widespread application of these updates to all connected devices. Mobility is also a requirement for many retailers who move between locations or sell on vehicles such as trains and ships.

Mekki *et al.* [7] recommend NB-IoT for POS systems because of its high performance compared to LoRaWAN and SigFox. However, Mekki *et al.*'s study does not consider LTE-M, which vastly outperforms NB-IoT with respect to data rate. 3GPP Release 14 also introduced multicast capabilities for NB-IoT [92] and LTE-M [93], making both solutions much better suited to POS systems. NB-IoT's much greater communications range also gives it a distinct advantage for vendors in rural and remote areas. If only short communications range is required, D7AP provides excellent data rate and security suitable for handling time-sensitive and private financial information. In addition, its compatibility with existing RFID-based systems [134] could allow integration with existing retail barcode or inventory systems.

F. ENVIRONMENTAL MONITORING

Environmental monitoring is defined in [177] as detecting ecosystem health indicators in water, air, and soil. Criticality depends on what is being measured, with some environmental features indicating natural disasters or severe ecological damage if outside a certain range. Systems detecting values outside the 'safe' ranges can be considered critical. Conversely, many systems are never used for detecting disasters or ecological damage. Environmental data is often collected by these to develop time-series models for guiding strategy and detecting long-term problems early [178].

While we assume actuation is very unlikely to be required, Abraham and Beard [177] prioritize remote updates and sensor configuration. Many sensors require regular calibration to adapt to changing environmental values. Consequentially, multicast communications can provide significant benefits.

Kadir *et al.* [179] and Xue-Fen *et al.* [140] propose critical environmental monitoring systems using LoRaWAN for detecting forest fires and extreme weather respectively. Xue-Fen *et al.* also state air pressure and lightning will not undergo extremely rapid changes, and consequentially data rate and granularity can be sacrificed for communication range. LoRaWAN was also selected by Rahman *et al.* [180] for weather monitoring because of its reasonably long range and low cost. While LoRaWAN is very inexpensive and can be deployed anywhere, other protocols we have discussed have significantly longer ranges. Qadir *et al.* [9] suggest environmental monitoring systems prioritize long communications range and delay tolerance, also recommending LoRaWAN alongside SigFox.

Wang *et al.* [181] proposed a sensor network utilizing NB-IoT for monitoring tree health. NB-IoT has a very long range, low power consumption, high speed, high load scalability, and full multicast support. However, it is also relatively costly, has low structural scalability, and less likely to be available in remote areas. Wang and Fapojuwo [116] propose that no existing protocols are suitable for environmental monitoring, instead suggesting an LPWAN prototype derived from *Low Energy Critical Infrastructure Monitoring*(LECIM).

We assess that NB-IoT is the most suitable LPWAN for high-risk environmental monitoring when considering its low latency, high reliability, good obstacle penetration, high load scalability, and long communications range. If NB-IoT is too

expensive to afford, LoRaWAN is a good alternative although its shorter range and low load scalability must be considered. However, in situations such as discussed in [140] where environmental values are unlikely to undergo rapid changes, duty cycling restrictions are less problematic.

For non-critical environmental monitoring systems, we recommend NB-Fi or LoRaWAN. NB-IoT can also be used if very long range is required and the cost-benefit ratio is favorable; often, this implies a small number of devices.

G. WILDLIFE MONITORING

Liu *et al.* [182] provide three specific applications for wildlife monitoring: *location tracking, habitat observation,* and *behavior recognition.* We will not discuss habitat observation in this section as it is equivalent to *environmental monitoring*(Section VIII-F). This section is focused on location tracking and behavior recognition, which mostly require attaching wireless sensors to living animals.

Sensors attached to animals must be very small and lightweight to avoid discomfort and ensure captured behavior is not affected by the sensor. Schadhauser *et al.* proposed a system in [183] where sensors are attached to bats to track them in-flight. If these sensors weighed more than 2g or were larger than $1cm^3$, bat flight would be affected, and data would not indicate typical behavior. Wotherspoon *et al.* [184] provide another example, stating that sensor size should not exceed 40×60mm for rhinos. This is already very small, and rhinos are a large animal.

Wildlife monitoring systems can be critical, with an example outlined by Ayele *et al.* in [185] intending to protect endangered species from hunters, poachers, and natural predators. Because of this criticality, they recommend high reliability and low latency. Ayele *et al.* make the same recommendations in [186] and state previous solutions have been superseded for their combination of high cost and low latency. Both sources also note that animal distribution is sparse and can be unpredictable, requiring a clever approach to routing.

Wotherspoon *et al.* compared the communications range and power consumption of several radio platforms in [184], with LoRaWAN performing the best and achieving a 98% delivery rate over 5.5 km. Their experiments also showed 433 MHz was the most suitable frequency for wildlife monitoring, offering a smaller antenna than 169 MHz with very similar range. Ayele *et al.* also utilized LoRaWAN in [185] and [186], however did so with a dual-platform cluster-head architecture. In this architecture, low-energy Bluetooth (BLE) forms a mesh network between animals communicating with a LoRaWAN cluster head and packet concentration is utilized to compensate for duty cycling restrictions. Results showed that this architecture reduced energy consumption by up to 97%.

D7AP is recommended for animal tracking by Ayoub *et al.* [85] and Ergeerts *et al.* [90], with its localization capabilities noted by both studies. Ergeerts *et al.* demonstrated a successful bird tracking system utilizing D7AP, determining bird location when birds were within 60 meters of a bird cabinet. Sensors used in this study were also small enough to fit around a bird's ankle and only weighed 2.1 grams – Grabia *et al.* [124] also noted that D7AP sensors are very small. Ayoub *et al.* also recommend mesh topology for animal tracking systems and recommend D7AP for implementing it.

Liu *et al.* detail GSM and LTE methods for animal tracking in [182], suggesting cellular networks should always be used for wide-area tracking. Ayele *et al.* conflict this in [186], stating animals can inhabit remote areas outside cellular coverage. In [183], Schadhauser *et al.* state that network performance varies depending on the animal's proximity to a receiver and the presence of any environmental obstructions, however channel information is largely unknown to the animal sensor before transmission.

We assess that LoRaWAN is a good choice for wildlife monitoring as it uses little power, has high localization accuracy among LPWANs [169], and is capable of working well attached to fast-moving objects such as animals. NB-IoT is also a good choice as it provides longer range than LoRaWAN and demonstrated improved obstacle penetration in open areas ***[96]***. However, NB-IoT is more expensive and consumes more power – for example, NB-IoT consumes 74-220 mA during transmission while LoRaWAN consumes 28 mA. NB-IoT should be used if practical or available for critical use cases, and only for non-critical cases if LoRaWAN has insufficient range, load scalability, localization accuracy, or obstacle penetration. If animal tracking is only measuring animal location around a particular point (such as Ergeerts *et al.*'s study in [90]), D7AP is also an appropriate solution for both critical and non-critical use cases. However, its localization capabilities fall short of NB-IoT and LoRaWAN.

H. SMART BUILDINGS

Havard *et al.* propose a data custodianship model for smart buildings in [187], classifying use cases into *comfort* and *safety/security.* In this model, tenants should be able to access all data from their own sensors, while building management should be able to access safety/security data from all tenants. All data related to comfort sensors are completely restricted to the owning tenants. An additional category of sensors for monitoring water leaks is proposed in the same study - we propose extending this to form a third classification for monitoring building *integrity*. Building integrity data should follow the same custodianship rules as safety/security.

We can easily use the classifications in [187] to assist with identifying critical and non-critical use cases. Safety/security use cases are clearly critical, while comfort use cases are non-critical. We also consider most building integrity applications as non-critical, as faults such as leaks develop slowly over time. Sensors monitoring severe and sudden structural damage should be classified as *safety/security* instead of building integrity.

Much of the previous literature surrounding smart buildings prioritizes the ability of networks to penetrate indoor

obstacles and communicate through walls, with LoRaWAN commonly exhibiting good performance. Trinh *et al.* [141] evaluated LoRaWAN's obstacle penetration in the 868 MHz band and observed good results. Ameloot *et al.* [142] tested both 434 MHz and 868 MHz bands, observing good results in both but noticing superior performance from the 434 MHz band. However, systems deployed through multiple buildings over a wide area should consider Lauridsen *et al.*'s study [96] where SigFox and NB-IoT exhibited higher obstacle penetration than LoRaWAN. Alongside good through-wall penetration, LoRaWAN is also recommended on the basis of reliability, communications range, and low power consumption by Trinh *et al.* in [141].

Several sources also recommend NB-IoT for smart building initiatives. Chen *et al.* proposed a temperature monitoring system with NB-IoT in [188] praising its scalability, obstacle penetration, low power consumption, and potential for edge computing. NB-IoT was also selected by Jianxin *et al.* [189] when developing a smart smoke detector system due to its low power consumption, long range, reliability, and uniform deployment. NB-IoT has the longest range of the LPWANs surveyed in this paper, superior obstacle penetration to SigFox and LoRaWAN, and is very reliable. However, it has low structural scalability and consumes more power than all unlicensed-spectrum solutions.

Mekki *et al.* [7] describe what we have classified as building integrity use cases, suggesting that low cost and long battery lifetime are required but the quality of service and frequent communications are not. Consequentially, they recommend LoRaWAN and SigFox. Qadir *et al.* [9] state any LPWAN capable of delivering periodic reports and alarms is suitable in smart buildings, however, recommend NB-IoT for video surveillance monitoring as it meets a minimum data rate of 130 kbps.

Following the above discussion, we recommend NB-IoT for smart building use cases related to safety/security as it has low latency, high reliability, and high load scalability. NB-IoT can also be used for systems that cover multiple buildings over a wide area, however in these cases, its limited structural scalability could be challenging. In all other cases, LoRaWAN should be used. LoRaWAN's high structural scalability, good through-wall penetration capability, and low power consumption make it suitable. LoRaWAN's data rate is also theoretically sufficient for real-time communications, however this is limited in practice by its reduced load scalability. LoRaWAN has a comparatively short communications range, however, is sufficient for communicating in one or more closely-placed buildings. If the area covered does not exceed 2 km, D7AP is recommended for both comfort and safety/security use cases for its favorable characteristics mentioned earlier, and data rate superior to NB-IoT.

If communications approaching true real-time rates are required, Weightless-P is a valid alternative – however, its practicality is limited by its very short urban range. There is also a lack of literature testing Weightless-P's capacity for through-wall communications.

LTE-M should be utilized for any video surveillance. While NB-IoT meets the minimum speed requirements for video at 130 kbps [9], this is likely to achieve only very low quality. Consumer demand for high-definition surveillance is only increasing, and improved quality will allow much easier identification of burglars or other criminals.

I. AGRICULTURE

The agriculture domain has some overlap with others covered in this paper – for example, agricultural use cases can involve forms of animal tracking, environmental monitoring, or even infrastructure control. However, agriculture has unique requirements and challenges that apply to all use cases regardless of similarity to other domains. Farmers have ownership over land and animals monitored, removing some conservation restrictions, and allowing further actuation or 'intervention'. This is confirmed in [190] where Yoon *et al.* claim farmers not only collect environmental information, but also adjust the environment where possible. Yoon *et al.*'s own example of environmental adjustment is a highly controlled greenhouse environment, while Liu *et al.* also outline remote actuation for a piggery in [182]. A similar use case is discussed by Ergeerts et al. in [90], who recommend the D7AP protocol for a greenhouse monitoring system.

Localization capabilities are also beneficial to agriculture [191], particularly when tracking moving livestock. Livestock tracking is similar in function to the wildlife tracking detailed in Section VIII-G; however key differences exist for farmers monitoring owned livestock. It is often simpler for farmers to retrieve devices from owned livestock compared to doing so from wild animals. In addition, the areas normally inhabited by the livestock and occasionally even their movements are known in advance. Actuation capabilities can also be implemented for livestock; for example, delivering a mild shock when an animal leaves a certain perimeter, providing a low-cost replacement to electric fencing.

Elijah *et al.* [191] prioritize security for farming applications, proposing that rival enterprises could gain access to confidential information. We also note the concept of agro-terrorism, in which malicious forces aim to compromise the food supply. Any IoT components introduce a new method for accomplishing this, and networks must be sufficiently secure to avoid it.

Several studies have recommended LoRaWAN for the agricultural domain and provided results confirmatory of this recommendation. Kodali et al. [192] claim LoRaWAN has good obstacle penetration, while Liu *et al.* [182] recommend its use for a piggery system that requires indoor and through-wall communications. SigFox and NB-IoT have been shown to provide significant improvements in 'deep-indoor' obstacle penetration [96]. However, other studies [141]–[143], [193] have supported LoRaWAN's suitability for indoor or through-wall penetration. Previous studies [90], [124], [134], [135] also claim that D7AP has good obstacle penetration capabilities.

LoRaWAN is also recommended by Hirata *et al.* [194], Rachmani and Zulkifli [195], and Yim *et al.* [196] based on its communications range. However, LoRaWAN has one of the lowest communications ranges of the LPWANs discussed in this paper, especially in rural areas. Notably, Hirata *et al.* only required coverage of a single rice field while Kodali *et al.* defines long range as a ''few'' kilometers. Yim *et al.* claimed LoRaWAN could operate for up to 30 miles in rural areas, however this was proven false during experimentation. These results confirm LoRaWAN could encounter difficulty in very large farms.

While LoRaWAN's range could be insufficient for larger farms, its energy efficiency and low cost have been praised by agricultural studies. In fact, Hirata *et al.* [194] found their expectations regarding battery life were exceeded. Ikhsan *et al.* [197] claim LoRaWAN can facilitate real-time collection of livestock data, while Yim *et al.* [196] adjusted its configuration to maximize reliability.

For larger farms where a longer coverage is required, our assessment shows that NB-Fi is the most suitable solution. NB-Fi has high reported battery life, low cost, robust security, and a long communications range. However, it does not support mobility and its localization capabilities are unknown. LoRaWAN can be used if mobility is required, providing low cost, high structural scalability, and energy-efficiency. In fact, Hirata et al. found in [194] that expectations for LoRaWAN battery life were exceeded. Ikhsan *et al.* [197] also claim that LoRaWAN is capable of collecting livestock data in real-time. NB-IoT can also be used if a much longer communication range or more accurate localization is required, however, it is relatively expensive and can be unavailable in remote areas without cellular coverage. Alternatively, farmers can install additional LoRaWAN gateways or repeaters, and will not require permission to do so as it is their own land.

For short-range farming systems such as greenhouses, animal growing facilities, or small animal pens, D7AP or Weightless-P also provide acceptable solutions although their lower localization accuracy should be considered. Both provide mobility, robust security, and high data rates. D7AP is the superior choice if devices being physically small or having longer battery life is prioritized. Conversely, if range exceeding 1-2 km is required, Weightless-P is the better solution.

J. SMART STREETLIGHTING

Kuzlu *et al.* outline several ways in which sensor/actuator components can be applied to smart street lighting systems in [198]. This study observed that remotely activating, deactivating, and adjusting the luminosity of streetlights only requires a low data rate. These use cases were classified as 'basic control' and the authors recommended SigFox, LoRaWAN, Weightless-P or NB-IoT. Conversely advanced configuration, fault alarms, and power monitoring are said to require a 'medium' data rate. Weightless-P, NB-IoT, or LTE-M were recommended for these use cases.

Kuzlu *et al.* also proposed an *Emergency Response*(ER) use case where smart streetlights assist emergency services and law enforcement alongside assisting citizens in danger. A good example is outlined in [199] where threatened citizens can remotely maximize the luminosity of surrounding streetlights with a smartphone app. Unlike the previously discussed applications of smart streetlighting, ER use cases are critical systems.

Our assessment shows SigFox is unsuitable for the basic control as its load scalability is limited by heavy restrictions on downlink messaging. We also assess that Weightless-P is unsuitable in dense urban areas, considering its very short range in these deployments. In contrast, it is difficult to justify the extra cost of NB-IoT for basic controls unless its very long range is required, or ER systems are being implemented requiring its high load scalability. Similarly, the cost of broadband-like speed of LTE-M is difficult to justify for advanced controls considering its short range and high power consumption.

Zhao *et al.* propose a system in [200] capable of advanced control and remote monitoring, stating it requires high scalability and long range but only low data rate. After considering NB-IoT, LoRaWAN, and SigFox, they selected NB-IoT for its transmission range, scalability, and power consumption alongside 'moderate' cost.

Smart streetlight systems using LoRaWAN are proposed by Ramesh *et al.* in [199] and Bingöl *et al.* in [201]. Notably, Bingöl *et al.*'s system is capable of transmitting fault alarms, performance monitoring, and remotely adjusting brightness. This contrasts with Kuzlu *et al.* who did not mention LoRaWAN as a candidate for these 'advanced' applications. Qadir et al. [9] recommend SigFox, LoRaWAN, and NB-IoT for smart streetlights and state that wide coverage, security, and energy-efficiency are required while delay is tolerable. Again, we debate the suitability of SigFox for any remote configuration as it has very low load scalability as a consequence of heavy downlink restrictions.

Kuzlu *et al.* exclusively recommend LTE-M for ER applications; while LTE-M is definitely essential for multimedia transmission (e.g. CCTV cameras), NB-IoT has adequate speed and reliability for critical use cases while consuming less power and achieving significantly higher transmission range.

We assess that NB-Fi is the most suitable LPWAN for smart street lighting systems without ER functionality. NB-Fi meets all requirements and its lower data rate is tolerable. If NB-Fi is not deployed in the area LoRaWAN is a suitable alternative, providing higher speeds but shorter communications range. NB-IoT is also a good solution, exhibiting a very long range but higher energy consumption and lower structural scalability alongside increased cost. However, NB-IoT has significantly higher load scalability than LoRaWAN and NB-Fi due to lack of regulatory restrictions in the unlicensed spectrum. Additionally, Zhao *et al.* [200] justifiably stressed the importance of firmware updates for smart street lighting. NB-IoT's multicast capabilities are advantageous for firmware updates, alongside simultaneous control of many streetlights.

TABLE 8. Requirement analysis and Most suited LPWANs for various use cases.

Use Cases	Requirements								Most suitable LPWANs
	Energy efficiency	Long range	Scalability SS = Structural Scalability LS = Load Scalability	Low cost	Robustness (Obstacle Penetration, Interference Management)	Uplink Performance	Downlink Performance	Mobility Required?	
Meter Reading (No alarm or real-time functionality)	**High-** Replacing batteries in many meters would be impractical and costly to utility organizations.	**High –** Large urban areas are likely to be covered. Obstacle penetration should also be prioritized to ensure meters in deep-indoor or underground environments can communicate.	**High (SS) -** Almost all premises will have a connected meter, resulting in many devices proportional to urban range and density. **Low (LS) -** No more important than normal.	**High -** Due to the large number of meters, higher costs will quickly become impractical or unrealistic.	**High –** Meters are often placed in deep-indoor environments such as basements, or behind obstructive material such as concrete. In addition, close placement of meters can lead to significant inter-network management.	**Low -** Latency of up to a day is tolerated for standard meter readings [154].	**Low/None –** Latency of up to 15 minutes is tolerated for command messages changing rates [154]. If no commands are being used to change rates, downlink messaging is not required.	**No -** Meters remain fixed in one place.	NB-IoT, LoRaWAN, NB-Fi SigFox (requiring uplink data only)
Meter Reading (Real-time or alarm functionality)	See above.	**See above.**	**High (SS) –** Same as standard *meter reading* use case. **High (LS) -** Messages must be able to be sent at any time, and potentially large amounts of real-time or usage data may be sent.	**See above.**	**See above.**	**High –** Latency must not exceed one minute for alarms or five minutes for real-time monitoring messages [154].	**Varies –** See above.	**See above.**	NB-IoT
SCADA and Infrastructure Control	**Varies** If assets are connected to constant power supply, this is low. If not, this will be moderate in normal environments and high in hazardous industrial environments. Battery replacement should be minimized in hazardous environments to avoid dangerous situations.	**Varies-** Sommer et al. [157] state that industrial IoT networks are required to communicate for several tens to hundreds of meters, while Grabia et al. [124] provide a range of 0.5-1 km for *Industry 4.0* systems. These are met by all solutions discussed. However, if assets are deployed over an entire utility network or in remote environments, this will range from moderate to high.	**Low (SS) -** SCADA systems have a relatively small number of devices. **High (LS) -** SCADA systems are often critical, requiring real-time communications and the ability to communicate at any time.	**Low-** SCADA assets are generally considered 'critical' and more investment can be justified.	**Moderate/High –** Industrial systems are often deployed in signal hostile environments [157], including factories with abundant obstructive material such as concrete and areas with high electromagnetic interference. In these cases, we recommend *high* robustness.	**Moderate/High –** Data from critical systems must arrive in real-time. Otherwise, moderate data rate is acceptable.	**Moderate/High –** Commands should be delivered to actuators and executed in real-time for critical systems. Otherwise, moderate data rate is acceptable.	**No –** Industrial assets are unlikely to move.	NB-IoT (long range or critical systems) LoRaWAN (mid-range systems) Weightless-P, D7AP (short-range systems) EC-GSM (if GSM already used)
Transport	**Low -** Vehicles can provide a constant source of power to any attached sensors.	**High -** Vehicles may drive a long distance from base stations and into remote areas.	**High (SS) –** Inhabited areas will contain a large number of vehicles at potentially very high densities, especially in big cities. Phillip et al. **[158]** also observed that increasing structural scalability improved efficiency at autonomous intersections. **High (LS) –** Transport systems are often critical, with malfunction or delay risking human safety or public infrastructure. Systems may also be required to process large CAN BUS messages.	**Low -** Transceiver cost has much less impact when manufacturing or purchasing a vehicle. Vehicular systems must also be reliable and fast, which will always cost more to ensure.	**High –** Vehicles are likely to be obstructed by urban obstacles including buildings, tunnels, bridges, and other vehicles. The doppler effect has a significant impact on vehicular communications [159] and therefore robust strategies for handling it are recommended.	**High –** Regardless of criticality, all transport applications require very fast and reliable communications [9] [158]. High data rate may be the difference between life and death for a crash-avoidance system. In addition, vehicles may exchange complex geospatial data or media for analysis. Real-time interfacing with vehicle CAN Bus components will require speeds in the megabit range [161] [162].	**High –** Equal to uplink performance, for the same reasons. Data exchanged between cars will require both uplink and downlink exchanges.	**Yes –** Vehicles can potentially move at high speeds over very large areas. This requires robust base station/cell handover capabilities.	LTE-M (critical systems or CAN Bus integration) NB-IoT, LoRaWAN, or EC-GSM
Logistics	**High -** The large number of potential devices makes changing or recharging batteries impractical, and goods may be in transit or storage for long periods of time.	**High -** Goods may be moved long distances from base stations and stored in environments such as basements, containers, or secure warehouses.	**High (SS) -** Exact structural scalability requirements depend on the granularity of the system – for example, whether assets are tracked at the container, pallet, or individual item level. However, even at the container level, this is a potentially huge number of items. **Low (LS) -** No more important than normal.	**High -** The potentially large number of devices means higher-priced devices will be impractical to deploy.	**Low –** No more important than normal.	**Low -** It is unlikely very large amounts of data will be sent, and higher latency can be tolerated. Fore et al. [168] state that data sent from logistics sensors will likely be very small quantitative or discrete values.	**None –** Stock items are unlikely to have an actuation component.	**Yes –** Sensors must be able to communicate while goods are in transit. Goods can be transported over very long distances and are often transported at high speeds.	LoRaWAN, NB-IoT
Logistics (High risk stock)	**See above.**	**See above.**	**High (SS) –** Same as standard *logistics* use case. **High** (LS) - Systems must support real-time communication with sensor information sent and actuator commands received for environmental control received at any time.	**Moderate –** Organizations will be willing to invest additional funds in safety-critical sensors. However, the large potential number of sensors should still be considered, as high cost will make purchase impractical.	**Moderate –** Robustness should always be increased for critical systems to further guarantee reception.	**High –** Values outside safe thresholds should raise alarms, and these should be sent and received as soon as possible.	**See above.**	**Yes –** High-risk stock will also have higher requirements for regular communication while in transit.	NB-IoT
Retail	**Low -** POS systems are likely to be connected to mains or constant power sources. If not, they can be equipped with rechargeable batteries. A month or even week of battery life are considered good for rechargeable batteries in consumer electronics.	**Low/Moderate -** While distance is not a concern for a single 'brick and mortar' storefront, street vendors or market sellers will move between different locations. These locations can be rural or remote, far away from a base station.	**Moderate (SS) -** If all POS systems in an area are sharing a base station or common backhaul, a high number of devices will be served. **High/Moderate (LS) -** Large amounts of data may be sent, and timeouts are often unacceptable when processing financial or banking data. In many cases, timeouts will cause the transaction to be cancelled and 'roll back'.	**Low -** Most retailers will only purchase a relatively small number of POS systems, with boutique-sized businesses having one per store. Market sellers or street vendors will only require a single machine.	**Moderate –** Retailers are likely to operate in crowded environments with both human and urban obstructions. Increased robustness also decreases probability of timeout or transaction failure.	**High -** Large amounts of bank and inventory data must be sent, and financial institutions often cancel transactions after a relatively short timeout.	**High –** Aside from acknowledgement and return messages from financial institutions, inventory systems for larger enterprises will send regular stock updates. In addition, banks often send firmware updates to all machines to patch security issues. This is critical when handling financial data, and if possible, multicast communications should be employed.	**Yes –** Many vendors, especially market sellers or street vendors, travel between locations to sell their goods. Some vendors also operate in high-speed moving environments such as food carts on trains.	D7AP, LTE-M, NB-IoT
Environmental Monitoring (Non-critical)	**High -** Battery replacement should be minimized as sensors are often placed in very remote or hard-to-reach locations.	**High -** Sensors may be placed in locations very far away from base stations or in obstructed environments.	**High (SS) -** Could require deployment across very large areas including national parks. Large areas will, by nature, include a greater number of sensors. A greater number of sensors will also facilitate finer-grained measurement of environmental parameters [210]. **Low (LS) -** No more important than normal.	**Low -** No more important than normal.	**High –** Natural obstructions such as rocks, hills, and trees are likely to be present. Xue-Fen et al. [140] state outdoor areas are naturally prone to obstructions.	**Low –** No more important than normal. It is suggested in [9] that environmental monitoring systems should tolerate delays well. Delay tolerance often requires a network designed for low uplink performance.	**Moderate -** Abraham and Beard [177] prioritize remote updates and configuration for environmental sensors. This makes sense, as many environmental sensors such as soil moisture probes require regular calibration for a changing environment.	**No –** Sensors will be attached to environmental features that will have relatively little, if any, movement. Examples of this include soil, trees, rocks, riverbanks, and caves.	NB-Fi, LoRaWAN NB-IoT (very long range, if affordable)
Environmental Monitoring (Critical)	**See above.**	**See above.**	**High (SS) –** Same as standard *environmental monitoring* use case. **High/Moderate (LS) -** Devices in areas where sensed environmental values can rapidly change must be capable of sending alarm notifications at any given time, resulting in high prioritization. For example, sudden volcanic activity in a region threatening human lives and livestock. However, in situations such as those specified by [140] where sensed values are unlikely to rapidly change, this can be reduced to Moderate.	**High –** Many developing countries are most significantly affected by natural disasters [211] [180], and therefore sensors to monitor them can provide the most benefit and potentially prevent loss of life. For practical deployment in these countries, cost must be minimized.	**High –** Natural obstructions such as rocks, hills, and trees are likely to be present. In addition, sensors deployed in natural disaster zones will be relied on in very inclement conditions.	**High –** Requires speed as close to real-time as possible.	**High –** While the same logic applies as above, consequences for critical sensors being improperly calibrated are far more dire.	**See above.**	NB-IoT, LoRaWAN (Infrequently changing phenomena)
Wildlife Monitoring	**High –** Sensors attached to wildlife must be very small [183] [184], and therefore can only utilize very small and low-capacity batteries. To allow a practical lifetime, power consumption must be very low. In addition, batteries implanted in or attached to animals will be difficult (if not impossible) to retrieve.	**Varies –** Tracking animals in very remote locations, or those that migrate over long distances, will require a long communications range. However, some animal tracking systems (like detailed in [90]) only track animals around a given point. In these cases, only very short ranges are required.	**Moderate (SS) -** Higher structural scalability may be required for monitoring large herds of animals, or multiple herds over large areas. Ayele et al. [186] state that herds are compact and can encounter one another. **Varies (LS) -** While wildlife monitoring is often non-critical, critical use cases do exist such as monitoring endangered species or disease vectors.	**Moderate –** Sensors must be kept inexpensive if many animals are monitored. In addition, sensors are likely to be lost if attached to animals in remote areas. Sensors should be sufficiently inexpensive for this loss to be acceptable.	**High –** Areas uninhabited by humans or with low human populations will contain natural obstructions such as rocks and trees. If animals are located closely together in herds, the close proximity of simultaneously communicating sensors can introduce intra-network interference.	**Varies –** Criticality depends on why wildlife is being monitored. Monitoring endangered wildlife for threats or tracking disease vectors, for example, is far more critical than a scientific survey.	**None –** Actuation components on animals should be discouraged or prohibited for ethical reasons.	**Yes –** Animals regularly move, with some migrating over vast distances. Some animals also move very fast, and systems monitoring them should have good resistance to the doppler effect. Animal habitats are also unpredictable and subject to change.	LoRaWAN D7AP (Short range) NB-IoT (If necessary)

TABLE 8. *(Continued.)* **Requirement analysis and Most suited LPWANs for various use cases.**

Smart Buildings (Comfort, Building Integrity)	**High -** Building tenants will be unwilling to utilize systems that significantly increase their electricity consumption. Mekki et al. [7] also prioritize battery life for smart building use cases.	**Low-Moderate -** Low for relatively small or standard-sized buildings and moderate for large complexes or networks encompassing several properties.	**Moderate (SS) -** Highly integrated or large facilities may require a significant number of devices, which will be concentrated in a relatively small area. **Low (LS) -** No more important than normal.	**High -** Tenants are unlikely to invest in overly-expensive devices and usually strive to minimize expenditure. Like battery life, this is prioritized by Mekki et al. in [7].	**High –** Communications must be able to cover the entire indoor and outdoor area of one or more buildings, penetrating through signal-hostile materials such as concrete, glass, and metal.	**Low –** No more important than normal. Mekki et al. [7] states quality of service and frequent communications are not required, while Qadir et al [9]. imply the same by proposing that any LPWAN is suitable.	**Low –** The same constraints seen with uplink messaging will apply. Building Integrity actuators are unlikely to exist on an LPWAN scale, and comfort-related applications are non-essential.	**No –** Buildings and their sensors are very unlikely to move.	Weightless-P, D7AP (Higher Performance) LoRaWAN (Longer Range)
Smart Buildings (Safety/Security)	**Moderate -** While the same principles apply as above, additional power consumption is often deemed an acceptable exchange for extra safety.	**See above.**	**Moderate (SS) –** Same as standard *smart buildings* use case. **High (LS) -** devices must be able to send an unlimited number of alarms (such as fire alarms) and receive actuation commands to minimize potential loss and maximize human safety (such as activating sprinklers) at any given time.	Moderate **–** While the same principles apply as above, additional expenditure is often acceptable for critical use cases. In addition, safety and security fittings are often a landlord's responsibility.	See above,	**High –** Delay is completely unacceptable. Surveillance applications will also require sufficient speed to transmit video, sound, or image data.	**High –** Delay is, again, completely unacceptable. Many actuations for these use cases will be activating systems that can prevent loss of life or injury, such as fire sprinklers or security shutters.	See above.	NB-IoT LTE-M (surveillance) D7AP (Shorter Range)
Agriculture	**High –** Many sources have stated the importance of long battery life. Devices monitoring crops could potentially be required to operate through the entire crop's grow cycle, which can range between months and years. In addition, continually replacing batteries, particularly in remotely located devices, is very impractical to farmers.	**Varies -** Farms can be very large and located in remote areas far from base stations. An extreme example of this is the Anna Creek cattle station in Australia, which has a total area of 15,746 km^2. Previous literature [192] [194] has also emphasized the importance of long range communications to agriculture. However, some agricultural use cases also involve relatively small farms or indoor environments such as greenhouses and piggeries.	**High (SS) -** Billions of agricultural IoT devices are forecasted to be deployed in future **[191]** to support smart agriculture. **Low/Moderate (LS) –** Usually low, but sometimes measured values can rapidly change during severe weather or farm accidents.	**High –** Farms often operate under restricted budgets that can be further depleted by weather conditions such as drought. Devices located remotely or attached to animals are also more likely to be damaged, and lower cost per device will result in less net loss to the farm.	**Varies –** Depends on the farm's terrain. Relatively open or flat areas can be monitored, as can hilly, highly vegetated, or indoor environments. This can form a relationship with what is being cultivated, as certain plants or animals thrive only in certain types of terrain. In some cases, such as tree farming [196], the produce itself will directly form obstructions.	**Low-Moderate –** Agricultural use cases rarely endanger human life or significant environmental damage. However, significant financial loss can be incurred if information fails to arrive. Some sources [196] [197] also mention higher-performance data acquisition for agriculture.	**Low –** If actuation components are being employed for farming, they are often to prevent significant resource waste (such as water [192]) or control environmental variables for growth. However, some delay in the order of seconds can usually be tolerated.	**Varies –** Livestock monitoring will require mobility; however, tree or crop monitoring are extremely unlikely to.	NB-Fi (No mobility required) LoRaWAN (Mobility required) D7AP, Weightless-P (Mobility required, short-range) NB-IoT (only if cost-effective)
Smart Streetlighting	**High –**Many cities were motivated to introduce smart streetlights by the high energy consumption of standard systems. Therefore, any smart streetlights with high energy consumption would be counter-intuitive.	**High -** Streetlight systems are often distributed over wide areas, and sometimes sparsely.	**High (SS) -** Urban areas can have a very large number of streetlights. **Low (LS) -** Streetlights are unlikely to send large amounts of data on a frequent basis. Alarms indicating bulb burn-out are unlikely to require rapid 'follow' up messages.	**High -** Municipal authorities often operate with limited budget, and a large number of devices could be required to connect all streetlights.	**Moderate-High –** Streetlights are deployed in urban areas which are also home to several obstructions. Potential obstructions include buildings, infrastructure, and even citizens. Interference can also be introduced by other networks and signals present. Moderate robustness is required in medium or low-density urban areas, however high density areas will require additional capabilities.	**Low/Moderate -** Kuzlu et al. [198] state that monitoring streetlight performance values such as energy consumption requires a 'moderate' data rate. However, Zhao et al. [200] claim that streetlight performance monitoring only requires a low data rate. Ultimately, the speeds required will depend on how much data is being transmitted and the size of any variables. In all cases, none of this data is critical enough to require real-time speeds.	**Low/Moderate –** Kuzlu et al. also state 'basic' on/off and dimming control of streetlights only requires low data rates, while more advanced controls such as scheduling will require higher data rates. Again, Zhao et al. propose a remote control system they claim only requires 'low' data rates. We have determined this requires moderate speeds; while not critical to emergency response, streetlights are important to public safety and security. Therefore, any controls should have reasonably low delay.	**No –** Streetlights do not move.	NB-Fi, LoRaWAN NB-IoT (only if cost effective)
Smart Streetlighting (Emergency Management)	**Low/Moderate-** While net power consumption should still be smaller than that seen in older streetlight systems, more power consumption than normal is often considered acceptable for systems essential to public safety.	**See above.**	**High (SS) –** Same as standard *Smart Streetlighting* use case. **High (LS) -** Devices must have constant access to unrestricted communication to guarantee public safety.	**Moderate –** Municipal authorities and residents will accept higher expenditure for devices essential to public security. In addition, emergency management capabilities can be restricted to streetlights in dangerous areas.	**High –** Robustness should always be increased for critical systems to further guarantee reception.	**High –** Immediate threats to public safety should arrive immediately after detection.	**High –** If public safety is threatened, commands to implement a countermeasure should also arrive immediately.	**See above.**	NB-IoT LTE-M (surveillance)
Healthcare	**High -** Long battery life is prioritized in many existing studies. Frequently needing to charge devices limits patient independence and quality of life. Devices being powered off also introduces the risk of missing critical events.	**High -** User quality of life and independence should be maximized by allowing devices to operate over long distances and in various places. Devices being out of range also introduces the risk of critical events being missed.	**High (SS) -** Areas such as nursing homes and hospitals can concentrate a large number of people in a small space. As the human population grows and the average age increases, more people will be required to utilize healthcare devices. New wearable and medical sensors are also rapidly entering the marketplace. **High (LS) -** Healthcare systems are, by nature, critical. Alarms must arrive as close to immediately as possible and reception should be guaranteed.	**Moderate -** Sacrifices to cost-efficiency are somewhat acceptable for reliability and speed in healthcare. However, devices must still be affordable by patients or healthcare providers. Many people living with chronic health conditions are also economically disadvantaged.	**High –** Several sources [143] [193] have stated that healthcare systems must have robust indoor communications capabilities and obstacle penetration; in particular, [143] clarifies wearable sensors should be able to handle the obstruction of an attached human body.	**High –** Alarms indicating possible medical emergencies must arrive with healthcare personnel as soon as possible. Real-time communication is essential as time is of the essence in medical emergencies.	**None –** Currently, most healthcare applications discussed involve passively monitoring patient health indicators. Actuation could allow remote medical attention or resuscitation procedures in future; however, this is a complex legal and ethical issue.		NB-IoT, LoRaWAN (Periodic reports, long-term biometric monitoring) [206] [169]
Defense and Military	**High -** Many military devices will be deployed remote and potentially occupied/hostile areas. This makes regular battery replacement impractical. Devices may also be used for very long-term surveillance or intelligence gathering, requiring a significant amount of energy.	**High -** Devices may be placed in very remote environments or across large, hostile areas. Research performed by the U.S. Army [212] reinforces the need for long-distance communications.	**High (SS) -** A strategic planning meeting by the US Army concluded the Internet of Battle Things (IoBT) may be several orders of magnitude greater than any preceding network, with up to a million things per square kilometer possible [213]. **High (LS) -** Like healthcare systems, military systems are critical by nature due to the sheer importance of their data and the consequences of late or undelivered information.	**Low/Moderate –** U.S. Army research into IoT systems [212] emphasized low cost as a design principle. In addition, compromised devices should be 'disposable', meaning that their loss is acceptable [213]. For this to be truly workable, devices should have a relatively low cost. However, we have also classified this as 'Moderate' as military budgets could potentially allow more expenditure than normal.	**High –** Military networks will not only be deployed in harsh and potentially obstructed areas but will need to resist active attempts at jamming or other attacks by adversarial forces.	**High –** Information is critical to military command and monitoring of armed forces. Intelligence should arrive uncompromised as soon as possible.	**High –** Commands sent to personnel or military equipment should arrive uncompromised as soon as possible. Delay in military action could be catastrophic.	**Yes –** Systems tracking moving assets such as weapons, vehicles, and personnel should provide mobility. In these cases, very robust techniques will be required as military assets can move very fast. Most military assets will move at some stage, being relocated between deployments or campaigns.	LoRaWAN, (Localization required) Weightless-P, D7AP

For systems with ER functionality, we recommend LTE-M if transmitting image or video data is required, and NB-IoT in all other applications.

K. HEALTHCARE

Existing literature presents a wealth of information regarding the requirements of IoT healthcare systems. In this discussion, as with all others in this section, we will discuss those not summarized in Table 8. Privacy and security are prioritized in a wide range of works [202]–[205], demonstrating their high importance. Fernandez and Pallis outlined other non-functional requirements in [205] including stability, availability, extensibility, portability, and accessibility. Anand and Routray [204] also note that high-power radiation can potentially harm human tissue, and any healthcare sensors should seek to minimize this harm.

Localization capabilities can also provide significant benefit to healthcare, with example use cases including tracking vulnerable patients and locating them in emergencies. Valach and Macko state in [169] that LPWANs can potentially provide a low-power alternative to GPS for patient tracking.

Mdhaffar *et al.* [206] state LoRaWAN is a 'smooth' balance of security and cost for healthcare systems, alongside being very energy efficient. However, they also claim it is unsuitable for continuous real-time data, instead recommending it for periodic reports. A similar conclusion is drawn by Valach and Macko [169] when studying LPWANs for fall detection in elderly patients. Valach and Macko claim LoRaWAN is unsuitable for critical alarms but good for monitoring health indicators over time while highlighting its Doppler Effect resistance, scalability, low power consumption, and long range. Buyukakkaslar *et al.* provide a somewhat contrasting observation in [193], claiming LoRaWAN can be used for real-time applications if payloads and spreading factor are kept very small. We also note that LoRaWAN's

range is relatively short compared with other LPWANs discussed.

Petajajarvi *et al.* [143] also recommend LoRaWAN, however do so after observing good indoor through-wall communications. Petajajarvi tested a LoRa transceiver attached to a user's arm, proving LoRaWAN can communicate when directly obstructed by a human body. While these studies, among others [141], [142], prove LoRaWAN is good for indoor through-wall communications, Lauridsen et al. [96] have also shown SigFox and NB-IoT perform better over wide areas.

NB-IoT is recommended for healthcare systems by Anand and Routray ***[204]*** because of its low power consumption, low bandwidth, and previously mentioned safety to human tissue. The authors also state that the clever use of upper-layer protocols is required to give NB-IoT sufficient performance for real-time health monitoring. Yearp *et al.* [207] and Ayoub *et al.* [85] both recommend using D7AP for healthcare systems. However, D7AP's short range is insufficient for monitoring patients over a wide area.

We recommend that healthcare applications always endeavor to use NB-IoT as it offers high speeds, energy efficiency, excellent communications range, high reliability, and high load scalability. In addition, it has been shown to not harm human tissue. 3GPP Release 14 also introduced improved localization capabilities to NB-IoT through the *Observed Time Difference of Arrival*(OTDOA) technique [92], which technology group Rohde and Schwarz claim is capable of accuracy within 50 meters [170]. Improved localization also makes NB-IoT more attractive to healthcare.

If NB-IoT is unavailable, LoRaWAN is a potential alternative with speeds allowing real-time communications and has been recommended for healthcare applications in previous studies. However, LoRaWAN's shorter range could be problematic when monitoring patients over wide areas. LoRaWAN is also capable of localization, however this is only accurate to within 200 meters [169] in contrast to NB-IoT's 50 meters. Additionally, LoRaWAN's reduced load scalability limits its viability for critical healthcare systems and makes it difficult to practically achieve real-time communications.

L. DEFENSE AND MILITARY

Military organizations must have exclusive ownership of any network utilized and be able to rapidly deploy and disassemble as needed in any environment [208]. Three LPWANs discussed in this paper meet those requirements – LoRaWAN, Weightless-P, and D7AP.

All systems have mobility support, with LoRaWAN in particular having demonstrated excellent resistance to the Doppler effect [57]. LoRaWAN and Weightless-P increase reliability and interference management through spread-spectrum communications, while D7AP strives for the same results through its *BLAST* design principles [84] and additional use of PN9 data whitening [86]. LoRaWAN's spreading factor and bandwidth can also be adjusted [57], allowing control over the trade-offs between spreading factor, bandwidth, communication range, and data rate.

While all networks are capable of exchanging sensor data in real-time, the unlicensed frequency bands used are subject to duty cycling restrictions in civilian applications. Military networks must be fast, highly reliable, and have high load scalability - each of these requirements can be impacted by regulatory restrictions. Governments allowing military communications an exception from regulatory restrictions when using these bands will be helpful.

Military systems introduce the threat of electronic warfare from adversarial forces, with methods including jamming interception, and direction-finding [209]. In response, LPWANs must provide end-to-end security services. Experimentation by Sondrol *et al.* [208] showed that while LoRa frames can be intercepted, encryption prevented their specific contents from being determined. However, in the same study, the authors suggested conducting further research on the protocol's security from a military perspective. LoRaWAN and D7AP both utilize AES-128 encryption, while Weightless-P can utilize either AES-128 or AES-256. D7AP also provides additional security mechanisms through its *Stealth* concept as detailed in Section V.E.

As LoRa, LoRaWAN, Weightless-P, and D7AP are all open standards, users are capable of developing their own higher-level protocols. This has potentially huge benefit to military forces as closed-source alternatives can be developed to better fulfil military requirements. D7AP also has a history with the United States Department of Defense, giving it precedent for military use.

LoRaWAN should be used if localization capabilities [165] or longer communications range are prioritized, while Weightless-P and D7AP should alternatively be used if data rate is prioritized. D7AP has an even shorter range than Weightless-P, however, should be used if the extra range is not required. D7AP is a good choice due to its robust interference management and security.

M. SUMMARY

Our assessment has revealed that very few use cases have one prominent LPWAN suitable in all situations. Instead, a range of LPWANs are usually suitable and organizations will select the one most closely matching their individual requirements and situation. In many cases, the selection will be heavily influenced by regional availability and budget.

We can also observe that while some LPWANs have a distinct 'role' across several domains, others are suited to a wider variety of situations. LTE-M is exclusively capable of handling broadband-like and multimedia networking, while NB-IoT is recommended for all other critical systems. LTE solutions, D7AP, and Weightless-P are also capable of multicast communications. LTE-based solutions, D7AP, Weightless-P, or LoRaWAN must be used for any use cases requiring mobility. NB-IoT, LTE-M, LoRaWAN and SigFox provide the most accurate localization capabilities [165],

with NB-IoT's localization known to be more accurate than LoRaWAN [169].

LoRaWAN, NB-Fi, and NB-IoT are commonly recommended for non-critical use cases as they meet all LPWAN requirements adequately. NB-IoT is recommended when a very long range, high load scalability, or low latency are prioritized, and a higher budget is available. LoRaWAN is recommended when moderate data rate, low cost, and low power consumption are required while shorter range and lower load scalability can be tolerated. Finally, NB-Fi is recommended when lower data rate is tolerable but low power consumption, low cost, and long range are prioritized. In practice, LoRaWAN is often used as it is not restricted by regional availability.

Weightless-P, D7AP, EC-GSM, and SigFox are suited to a relatively small variety of use cases but perform well in their respective niches. Weightless-P performs very well at most LPWAN requirements but is hindered by its very short range in dense urban areas. However, its support for mobility and multicasting makes it a good choice for networks deployed in open areas or for shorter-range urban networks. D7AP fulfils a very similar niche to Weightless-P, providing relatively high performance and a robust suite of features while restricted to a short range. SigFox is an inexpensive and very low-powered solution for uplink-only sensors without high performance requirements such as basic utility meters or data loggers. EC-GSM is useful for deployment in areas where newer LTE networks are unavailable, or for integrating systems that use the legacy GSM/GPRS network.

IX. RESEARCH CHALLENGES

This section presents several future research challenges by examining the current state of LPWAN networks and inherent issues.

A. SCALABILITY

Following discussions in Section II.C and subsequent sections, increasing structural/horizontal scalability [14], [15] allows more devices to connect to each base station, and more base stations to be deployed throughout the network. This results in LPWANs meeting use cases where structural scalability was previously insufficient, and more devices were needed to meet requirements. An example of this can be observed in Section VIII, where NB-IoT was chosen for the healthcare domain but still fails to meet structural scalability requirements, especially when serving a large number of patients. Increasing structural scalability ensures NB-IoT comfortably fits the healthcare domain, potentially alongside others where it was previously unsuitable. Similarly, our choices for various use cases and their justification in Section VIII demonstrate how increasing load/vertical scalability allows an LPWAN to be suitable for a wider variety of use cases, especially for critical systems or those exchanging large amounts of data.

For licensed-spectrum networks not subjected to regulatory restrictions, increasing load scalability can be achieved through network design decisions as detailed in Section III. For unlicensed spectrum networks subjected to regulatory restrictions, this is achieved by both the decisions previously discussed and determining how to achieve the best performance within regulations. For example, implementing LBT/AFA in ETSI territories relaxes duty cycling restrictions. Section VII's ranking of Weightless-P above LoRaWAN for load scalability demonstrates this and adding LBT/AFA to LoRaWAN as discussed in [17] could improve its ranking.

Alongside load scalability, vertical scalability also considers an individual node's processing power or memory. Increasing this allows LPWANs to meet higher-performance use cases in situations where LPWANs have previously not been considered due to insufficient specifications. Many of these use cases can be classified as edge computing, where more processing is performed at each node instead of shared backend infrastructure. Edge computing eliminates the need for data to be transmitted over the network for processing, instead only transmitting relevant results. Utilizing edge computing leads to reductions in data transmission, operational expenditure, and use of backend resources. Reduced use of backend resources also saves capital expenditure on backend infrastructure.

Existing technologies or changes to design decisions may allow an increase in structural and load scalability, but most likely at the detriment of other design goals. For example, structural scalability can be increased by utilizing OFDMA multiple access to improve base station capacity. However, this requires a more complex and costly infrastructure. Trade-offs are also present when increasing vertical scalability, whether through design decisions or utilization of more powerful hardware.

Future research needs to focus on developing methods for increasing both horizontal and vertical scalability without detriment to the other scalability type and other LPWAN requirements such as device cost. Special interest would be to develop techniques that work across all protocols, rather any specific LPWAN. Potential topics include new or less expensive PHY layer techniques, reducing hardware expenses, and optimized hardware architecture to improve performance. Section VII.C also demonstrated that no LPWAN offers leading performance in both structural and load scalability – research should also apply these methods to achieve such a solution.

All types of scalability will naturally increase as technology advances and powerful hardware becomes less expensive. Section IX-C's research should focus on taking full advantage of this increased scalability.

B. FURTHER PERFORMANCE STUDIES

One of the most challenging aspects of this study was to obtain reliable technical data and performance metrics for each LPWAN. Relevant data is only available for a few popular LPWANs like LoRaWAN, SigFox and NB-IoT through the provider's technical specifications and some research,

while those for others are difficult to gather, as fewer reference materials are available for them. Another problem is the wide variation in specifications reported in various studies/sources. The other possibility is manufacturers purposefully keeping selected information confidential for their own business strategy.

Further research should be conducted to determine actual performance metrics for each LPWAN under different circumstances. Such research will provide more accurate values for each measure outlined in Table 6, as well as increasing confidence in these values. It is far better to utilize values obtained from real-world testing than those from specifications or technical documents.

It is likely that performance varies under different circumstances. Many LPWANs provide adjustable configuration for ADR mechanisms, spreading factors, modulation schemes and even carrier frequency. The performance will vary based on which of these are chosen, and testing must be carried out for possible configurations including variations in weather conditions. This not only provides concrete values under various scenarios but establishes a relationship between each configuration and performance, allowing greater planning for future LPWANs.

C. CATERING TO FUTURE NEEDS

Users will inevitably begin to demand new applications as LPWANs become more widespread, inventing ways of applying them to their personal lives or business processes. If LPWANs cannot meet increased expectations, this could lead to potential disenchantment and negatively impact the acceptance of LPWAN technology.

Future applications will push the boundaries of LPWANs by requiring higher performance and factors unique to new requirements. LPWANs may be applied in applications deep underground, underwater, or even in space. Existing applications will also evolve as society changes over time and expectations from LPWANs rise. For example, implanted biometric devices may become widespread and 'normal' for each person to have. This contrasts with their relative rarity at the time of writing. Future research must identify new and challenging applications for meeting user expectations, which may require developing a new LPWAN platform.

D. STANDARDIZATION

While organizations such as Weightless SIG, DASH7 Alliance, LoRa Alliance, and 3GPP have introduced a variety of full-featured LPWAN standards, intercommunication between networks using different standards is still highly difficult. Consequentially, developing a method for devices to easily communicate with those utilizing different standards provides an ongoing challenge with significant potential rewards.

Static Context Header Compression(SCHC) is a standard being drafted by the *Internet Engineering Task Force*(IETF) attempting to achieve the above goal by making UDP and IPv6 protocols accessible to LPWAN devices [214]. UDP and IPv6 will not only provide a common communication mechanism for devices on networks with different standards, but also connect easily with more 'typical' Internet endpoints. Historically, IPv6 has been unable to work effectively with LPWANs because of its large packet headers, and the fact that some LPWANs may not support message fragmentation. A lack of fragmentation quickly becomes impractical when IPv6's *Maximum Transmission Unit*(MTU) value is 1280 bytes.

As per the draft standard, SCHC creates an adaptation layer between IPv6 and the underlying LPWAN technology which is further divided into the compression and fragmentation sublayers. The compression layer compresses (or decompresses) an IPv6 packet's header to make it smaller (or bigger) than the original header to create the SCHC packet. An SCHC packet is then subject to fragmentation if its packet size exceeds MTU. SCHC also outlines security countermeasures to deal with malicious header compression that may result in incorrect packet reconstruction and thwart potential attacks to fragmentation.

IETF should continue research and development of the SCHC standard while maximizing compatibility with prominent LPWANs. Development should also be accompanied with efforts to ensure widespread support and implementation from standard holders and software vendors, as regardless of quality unused standards will fade into obscurity. Additional research should focus on standardization at the application layer, providing consistent schemata and formats for contextual data. For example, all devices measuring temperature should send data using the same scale and unit of measurement. This data format could be retroactively utilized by existing LPWANS through interfaces and translation mechanisms and built into networks developed in the future. Considerations should be given to future needs as outlined in the previous sub-section.

E. SECURITY

Section VIII identified several use cases where security and privacy are critical; however so far, there has been relatively little focus on the security for LPWANs in general. For example, unauthorized access to smart home controllers could be used to steal private information and actuate home appliances, causing severe distress and inconvenience to users. Even more worryingly, breaches to inter-vehicle communication or infrastructure control systems could easily cause loss of life and environmental damage. All of these put security as one of the most significant issues for LPWANs moving forward. Without adequate security, LPWANs will not be commercially viable.

Chacko and Job [215] identified five vulnerabilities inherent in LPWAN networks; *compromising devices*, *jamming attacks*, *replay attacks*, and *wormhole attacks*. *Compromising devices* involves physically intercepting the connection between device microcontroller and network transceiver, often by placing an additional component along with the data interface. These additional components are not only capable

of sending all exchanged data to an attacker, but also altering data to potentially disastrous consequences, especially when large-scale deployment will become commonplace as more IoT services emerge. *Jamming attacks* and *replay attacks* have been widely discussed in the fields of network security and wireless communications. Replay attacks are especially dangerous with SigFox networks if security follows the 'opt-in' model. *Wormhole attacks* are less widely-known and involve intercepting packets over the air and sending them to another receiver.

Several solutions have been proposed to mitigate these vulnerabilities. In [215], Chacko and Job provided a broad mitigation strategy for each of the five vulnerabilities stated above. Compromising devices can be mitigated by encrypting the interface (such as UART- Universal Asynchronous Receiver/Transmitter) between the device and the transceiver. Replay attacks can be mitigated in a similar fashion by encrypting over-the-air communications, however, it requires frame counters to be implemented. It is hard to prevent jamming; however, it can quickly be detected by a decrease in traffic over a frequency range. The probability of frequency jamming can be reduced by utilizing frequency-hopping techniques. Wormhole attack can be orchestrated using both a sniffer and a jammer and is more dangerous. Once packets are intercepted by the sniffer, a jammer is used to prevent them from arriving at their intended destination. Without a packet's arrival to destination, the message request will remain 'open' and valid. While wormhole attack is hard to detect in LPWANs, *packet leashes* [216] and *transmission time base mechanism* [217] are effective defense options.

A number of research works have been reported in the literature to improve security aspect of LPWANs. These include the development of a network intrusion detection system for LoRaWAN [218], a secure link establishment technique using LoRaWAN's variable MAC parameters [219], and investigation of utilizing blockchain architecture for low-power, resource-constrained IoT end-devices [220].

Any defense mechanism employed for LPWAN solutions must be considerate of hardware and bandwidth constraints, as increased security often requires additional bandwidth, storage, or processing power. It is insufficient to simply focus on devising stronger techniques, but instead the focus must be placed on developing techniques for the unique challenges of LPWANs. An additional research challenge is to develop security mechanisms for a wider range of LPWAN technologies.

F. EMERGING TRANSMISSION MEDIA

While all current LPWANs utilize the radio section of the spectrum, innovative technologies have emerged utilizing other sections; notably, the visible light spectrum with technologies such as Li-Fi. Because of larger bandwidth, utilizing the visible light spectrum allows for very fast data rates and enormous scalability. However, utilizing light as a transmission media introduces a unique set of challenges of its own. Because of these challenges, light-spectrum communications are currently unsuitable for LPWANs – they are more expensive, have a very short range and are unable to penetrate opaque obstacles.

Despite these challenges, potentially huge increases to speed and scalability make the light spectrum worth investigating as a transmission media in future LPWANs. Research challenges exist to reduce the cost of light-based techniques, increase range, and develop innovative methods for overcoming physical limitations of light. Examples of techniques to be investigated include the deployment of rapidly-rotating mirrors to refract light in the correct direction, beamforming light or developing less expensive light sensors.

X. CONCLUSION

With increasing deployment planned for IoT applications on a large scale, the need for efficient low power long range network technologies is growing fast. In this paper, we determined that all LPWAN technologies share six design goals, namely, energy efficiency, long range, scalability, low cost, interference management, and integration. Depending on the extent to which these goals are targeted, seven design decisions are made when developing LPWAN technologies which are unlicensed/licensed spectrum, operating frequency and bandwidth, modulation technique, channel access method, signal diversity technique, duplexity and business model. The impacts of these design choices on the meeting the design goals are discussed in detail, and one choice could help achieve one or multiple LPWAN goals while hindering others.

When examining each LPWAN's ability to match design goals, a clear trade-off became evident between power consumption, communications range, and data rate. Although that unlicensed-spectrum solutions are less expensive, more scalable, and consume less power, they are subject to duty-cycling restrictions that can hinder their suitability for critical applications. The results of this examination supported our assessment of LPWAN performance, through comprehensive analyses of technical specifications, reported results and observations from practical deployment, and the design decisions made in the respective LPWAN technology.

We also observed that very few use cases had a single, overwhelmingly suitable LPWAN – instead, multiple LPWANs are suitable and which one to select depends on the individual application's specific requirements and/or implementing organization. Each organization prioritizes LPWAN requirements differently across different applications. Organizations and individual applications are also restricted by LPWAN availability in the given area alongside available resources and budget. Considering these restrictions, selecting an LPWAN often has a degree of compromise.

This paper is valuable to consult which LPWANs are practical for a variety of industrial or research projects. The design goals presented here should be consulted to determine which are the most essential for a particular project. The comprehensive details of the technical specifications, strengths, and weaknesses of various LPWAN technologies

and their comparison with respect to the design goals and reported implementation in diverse applications in literature will equip readers with the necessary technical expertise. The use cases we discussed in this paper will assist readers with assessing available solutions, determining which one best meets their requirements, and making both informed decisions and balanced compromises. Based on our analysis of the available and emerging LPWAN technologies, we have identified a number of significant areas for future research. Scalability, security, and standardization are among the areas that need significant research for reliable operation and large-scale commercial deployment of IoT services.

ACRONYMS

3GPP	3rd Generation Partnership Project
ADR	Adaptive Data Rate
AES	Advanced Encryption Standard
AFA	Adaptive Frequency Agility
API	Application Programming Interface
ARQ	Hybrid Automatic Repeat Request
BER	Bit Error Rate
BLAST	Bursty, Light, Asynchronous, Stealth, Transitive
BPSK	Binary Phase Shift Keying
CDMA	Code-Division Multiple Access
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
CE	Coverage Enhancement
C-SS	Chirping Spread Spectrum
D7AActP	D7AP Action Protocol
D7AAdvP	D7AP Advertising Protocol
D7AP	DASH7 Adaptive Protocol
DBPSK	Differential Binary Phase Shift Keying
DoD	Department of Defence
DS-SS	Direct-Sequence Spread Spectrum
DL	Downlink
EC-GSM	Extended Coverage GSM
EPC	Evolved Packet Core
ETSI	European Telecommunication Standards Institute
FCC	Federal Communications Commission
FD	Full-Duplex
FDMA	Frequency Division Multiple Access
FEC	Forward Error Correction
FH-SS	Frequency-Hopping Spread Spectrum
GFSK	Gaussian Frequency Shift Keying
GMSK	Gaussian Minimum Shift Keying
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HARQ	Hybrid Automatic Repeat Request
HD	Half-Duplex
IoT	Internet of Things
IPv6	Internet Protocol version 6
ISM	Industrial, Scientific, and Medical
LBT	Listen Before Talk
LoRaWAN	Long-Range Wide Area Network
LTE	Long-Term Evolution
LTE-M	Long-Term Evolution for Machine
LPWANs	Low-Powered Wide-Area Networks
M2M	Machine-to-Machine
MAC	Medium Access Control
MD	Manufacturing-Driven
MTU	Maximum Transmission Unit
NB-IoT	Narrow Band IoT
NB-Fi	Narrow Band Fidelity
NS	Network Server
OFDMA	Orthogonal Frequency-Division Multiple Access
OTDOA	See TDOA
PRB	Physical Resource Block
QPSK	Quadrature Phase Shift Keying
R-FDMA	Random FDMA
RFID	Radio Frequency Identification
RSSI	Received Signal Strength Indicator
RX	Receiver
SCADA	Supervisory Control And Data Acquisition
SD	Subscriber-Driven
SINR	Signal-to-Interference-plus-Noise Ratio
SNR	Signal to Noise Ratio
TDOA	Time Difference of Arrival
TOA	Time of Arrival
TDD	Time-Division Duplex
TDMA	Time-Division Multiple Access
TX	Transmitter
UDP	User Datagram Protocol
UNB	Ultra-Narrowband
UE	User Equipment
UL	Uplink
TBS	Transport Block Size
XTEA	eXtended Tiny Encryption Algorithm

ACKNOWLEDGMENT

The authors would like to thank Mr. Iain McDougall of East Gippsland Water Corporation (EGW) for his constant support and valuable suggestions.

REFERENCES

[1] Statista. (2018). *Internet of Things (IoT) Connected Devices Installed Base Worldwide From 2015 to 2025 (in Billions)*. Statists. Accessed: May 6, 2018. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[2] L. Columbus. (Jan. 29 2017). *Internet of Things Market to Reach $267B By 2020*. Forbes, Accessed: May 6, 2018. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2017/01/29/internet-of-things-market-to-reach-267b-by-2020/#576cdc609bd6

[3] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 855–873, 2nd Quart., 2017.

[4] D. Ismail, M. Rahman, and A. Saifullah, "Low-power wide-area networks: Opportunities, challenges, and directions," in *Proc. Workshops ICDCN*, Varanasi, India, 2018, pp. 1–6.

[5] R. S. Sinha, Y. Wei, and S.-H. Hwang, "A survey on LPWA technology: LoRa and NB-IoT," *ICT Express*, vol. 3, no. 1, pp. 14–21, Mar. 2017.

[6] A. Lavric and V. Popa, "Internet of Things and LoRa low-power wide-area networks: A survey," in *Proc. Int. Symp. Signals, Circuits Syst. (ISSCS)*, Iasi, Romania, Jul. 2017, pp. 1–5.

[7] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Express*, vol. 5, no. 1, pp. 1–7, Mar. 2019.

[8] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) communication protocols: Review," in *Proc. 8th Int. Conf. Inf. Technol. (ICIT)*, Amman, Jordan, May 2017, pp. 685–690.
[9] Q. M. Qadir, T. A. Rashid, N. K. Al-Salihi, B. Ismael, A. A. Kist, and Z. Zhang, "Low power wide area networks: A survey of enabling technologies, applications and interoperability needs," *IEEE Access*, vol. 6, pp. 77454–77473, 2018.
[10] N. Poursafar, M. E. E. Alahi, and S. Mukhopadhyay, "Long-range wireless technologies for IoT applications: A review," in *Proc. 11th Int. Conf. Sens. Technol. (ICST)*, Sydney, NSW, Australia, Dec. 2017, pp. 1–6.
[11] J. Finnegan and S. Brown, *A Comparative Survey of LPWA Networking*. Maynooth, Ireland: Maynooth Univ. Department of Computer Science, 2018.
[12] W. Yang, M. Wang, J. Zhang, J. Zou, M. Hua, T. Xia, and X. You, "Narrowband wireless access for low-power massive Internet of Things: A bandwidth perspective," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 138–145, Jun. 2017.
[13] S. Tabbane. (Dec. 2017). *IoT Long Range Technologies: Standards*. Accessed: Jul. 16, 2018. [Online]. Available: https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2017/Nov_IOT/NBTC%E2%80%93ITU-IoT/IoT_standards.pdf
[14] A. B. Bondi, *Characteristics of Scalability and Their Impact on Performance*. Middletown, NJ, USA: AT&T Labs, 2000.
[15] A. Gupta, R. Christie, and P. R. Manjula, "Scalability in Internet of Things: Features, techniques and research challenges," *Int. J. Comput. Intell. Res.*, vol. 13, no. 7, pp. 1617–1627, 2017.
[16] D. Castells-Rufas, A. Galin-Pons, and J. Carrabina, *The Regulation of Unlicensed Sub-GHz bands: Are Stronger Restrictions Required for LPWAN-based IoT Success?* Ithaca, NY, USA: Cornell Univ., 2018.
[17] J. Ortin, M. Cesana, and A. Redondi, "Augmenting LoRaWAN performance with listen before talk," *IEEE Trans. Wireless Commun.*, vol. 18, no. 6, pp. 3113–3128, Jun. 2019.
[18] D. Zucchetto and A. Zanella, "Uncoordinated access schemes for the IoT: Approaches, regulations, and performance," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 48–54, 2017.
[19] M. Loy, R. Karingattil, and L. Williams. (May 2005). *ISM-Band and Short Range Device Regulatory Compliance Overview*. Accessed: Dec. 9, 2019. [Online]. Available: http://www.ti.com/lit/an/swra048/swra048.pdf
[20] Lora Alliance. (Nov. 2015). *LoRaWAN-What is It?* Accessed: Jun. 25, 2019. [Online]. Available: https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf
[21] S. Vijayakumaran. (Oct. 15 2013). *Comparison of Modulation Schemes*. Accessed: Jun. 27, 2018. [Online]. Available: https://www.ee.iitb.ac.in/~sarva/courses/EE703/2013/Slides/ComparisonOfModSchemes.pdf
[22] S. K. Rony, F. A. Mou, and M. M. Rahman, "Performance analysis of OFDM signal using BPSK and QPSK modulation techniques," *Amer. J. Eng. Res.*, vol. 6, no. 1, pp. 108–117, 2017.
[23] R. Pickholtz, L. Milstein, and D. Schilling, "Spread spectrum for mobile communications," *IEEE Trans. Veh. Technol.*, vol. 40, no. 2, pp. 313–322, May 1991.
[24] P. Prabakaran, "Tutorial on spread spectrum technology," *EETimes-Designlines Wireless Netw.*, May 2003. Accessed: Feb. 7, 2018. [Online]. Available: https://www.eetimes.com/document.asp?doc_id=1271899
[25] A. Singh, "Performance analysis of spread spectrum techniques," in *Proc. Conf. Adv. Commun. Control Syst.*, Mumbai, India, 2013, pp. 683–687.
[26] P. Zhang and H. Liu, "An ultra-wide band system with chirp spread spectrum transmission technique," in *Proc. 6th Int. Conf. ITS Telecommun.*, Chengdu, China, Jun. 2006, pp. 294–297.
[27] Semtech Corporation. (May 2015). *AN1200.22 LoRa Modulation Basics*. Accessed: Sep. 9, 2019. [Online]. Available: https://www.semtech.com/uploads/documents/an1200.22.pdf
[28] N. Vlajic. (2010). *Multiple Access (1)*. Accessed: Jan. 7, 2018. [Online]. Available: https://www.eecs.yorku.ca/course_archive/2010-11/F/3213/CSE3213_12_RandomAccess_1_F2010.pdf
[29] R. Rom and M. Sidi, *Multiple Access Protocols: Performance and Analysis*. Berlin, Germany: Springer, 1990.
[30] K. Benkic, "Proposed use of a CDMA technique in wireless sensor networks," in *Proc. 14th Int. Workshop Syst., Signals Image Process. 6th EURASIP Conf. Focused Speech Image Process., Multimedia Commun. Services*, Maribor, Slovenia, Jun. 2007, pp. 343–348.
[31] H. Yin and S. Alamouti, "OFDMA: A broadband wireless access technology," in *Proc. IEEE Sarnoff Symp.*, Princeton, NJ, USA, Mar. 2006, pp. 1–4.
[32] T. Xu and I. Darwazeh, "Spectrally efficient FDM: Spectrum saving technique for 5G?" in *Proc. 1st Int. Conf. 5G Ubiquitous Connectivity*, Akaslompolo, Finland, 2014, pp. 273–278.
[33] V. Almonacid and L. Franck, "An asynchronous high-throughput random access protocol for low power wide area networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, May 2017, pp. 1–6.
[34] SigFox. (2019). *SigFox Technology Overview*. Accessed: Aug. 25, 2019. [Online]. Available: https://www.sigfox.com/en/sigfox-iot-technology-overview
[35] SigFox. (Nov. 2918). *SigFox Device Cookbook: Communication Configuration*. Accessed: May 9, 2019. [Online]. Available: https://build.sigfox.com/sigfox-device-cookbook
[36] SigFox. (May 2017). *Sigfox Technical Overview*. Accessed: Jun. 6, 2018. [Online]. Available: https://www.disk91.com/wp-content/uploads/2017/05/4967675830228422064.pdf
[37] SigFox. (2018). *SigFox-Our Story*. Accessed: Jun. 6, 2018. [Online]. Available: https://www.sigfox.com/en/sigfox-story
[38] SigFox. (2019). *How to Become a SigFox Operator?* Accessed: Aug. 25, 2019. [Online]. Available: https://www.sigfox.com/en/coverage/become-so
[39] B. Ray. (May 31, 2018). *SigFox vs. LoRa: A Comparison Between Technologies & Business Models*. LinkLabs. Accessed: May 24, 2018. [Online]. Available: https://www.link-labs.com/blog/sigfox-vs-lora
[40] SigFox. (2019). *Radio Configuration*. Accessed: Aug. 25, 2019. [Online]. Available: https://build.sigfox.com/sigfox-radio-configurations-rc
[41] SigFox. (2019). *Downlink Information*. Accessed: Aug. 25, 2019. [Online]. Available: https://support.sigfox.com/docs/downlink-information
[42] SigFox. (2019). *Uplink/Downlink Messages*. Accessed: Aug. 25, 2019. [Online]. Available: https://build.sigfox.com/technical-quickstart
[43] H. Mroue, A. Nasser, S. Hamrioui, B. Parrein, E. Motta-Cruz, and G. Rouyer, "MAC layer-based evaluation of IoT technologies: LoRa, SigFox and NB-IoT," in *Proc. IEEE Middle East North Africa Commun. Conf. (MENACOMM)*, Jounieh, Lebanon, Apr. 2018, pp. 1–5.
[44] SigFox USA. (2019). *SigFox-Solutions*. Accessed: Aug. 25, 2019. [Online]. Available: https://www.sigfox.us/solutions/
[45] E. Pietrosemoli. (2017). *Wireless Standards for IoT: WiFi, BLE, SigFox, NB-IoT and LoRa*. Accessed: Jun. 25, 2019. [Online]. Available: http://wireless.ictp.it/school_2017/Slides/IoTWirelessStandards.pdf
[46] J. C. Zuniga. (Oct. 7, 2017). *SigFox Technology Overview for W3C WoT Group*. Accessed: Jun. 25, 2019. [Online]. Available: https://www.w3.org/2017/07/wot-f2f/slides/W3C_Sigfox_Technology.pdf
[47] SigFox. (2019). *Sigfox Global Network Key Features*. Accessed: Aug. 25, 2019. [Online]. Available: https://www.sigfox.com/en/sigfox-global-iot-network
[48] M. C. Padmavathy, "Performance evaluation of energy efficient modulation scheme and hop distance estimation for WSN," *Int. J. Commun. Netw. Inf. Secur.*, vol. 2, no. 1, pp. 44–49, 2010.
[49] Semtech. (2017). *LoRa Technology Whitepaper*. Accessed: Oct. 7, 2018. [Online]. Available: https://www.nnnco.com.au/wp-content/uploads/LoRa_technology_Whitepaper.pdf
[50] M. Barnela, "Digital modulation schemes employed in wireless communication: A literature review," *Int. J. Wired Wireless Commun.*, vol. 2, no. 2, pp. 15–21, 2014.
[51] R. Wireless, *A Comparison of UNB and Spread Spectrum Wireless Technologies as Used in LPWA M2M Applications*. West Sussex, U.K.: R. Wireless, 2015.
[52] Ben-Gurion University of the Negev. *Lecture 9: Spread Spectrum Modulation Technologies*. Accessed: Feb. 7, 2018. [Online]. Available: http://www.cse.bgu.ac.il/common/download.asp?FileName=Lecture_9new.pdf&AppID=2&MainID=408&SecID=3499&MinID=3
[53] N. Boudargham, J. B. Abdo, J. Demerjian, C. Guyeux, and A. Makhoul, "Investigating low level protocols for wireless body sensor networks," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Agadir, Morocco, Nov. 2016, pp. 1–6.
[54] J. D. C. Silva, J. Rodrigues, A. M. Alberti, and A. L. Aquino, "LoRaWAN—A low power WAN protocol for Internet of Things: A review and opportunities," in *Proc. Int. Multidiscipl. Conf. Comput. Energy Sci. (SpliTech)*, Split, Croatia, 2017, pp. 1–6.
[55] S. Devalal and A. Karthikeyan, "LoRa technology—An overview," in *Proc. 2nd Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, Coimbatore, India, Mar. 2018, pp. 284–290.

[56] U. Noreen, A. Bounceur, and L. Clavier, "A study of LoRa low power and wide area network technology," in *Proc. Int. Conf. Adv. Technol. Signal Image Process. (ATSIP)*, Fez, Morocco, May 2017, pp. 1–6.

[57] A. Lavric and A. I. Petrariu, "LoRaWAN communication protocol: The new era of IoT," in *Proc. Int. Conf. Develop. Appl. Syst. (DAS)*, Suceava, Romania, May 2018, pp. 74–77.

[58] *How to Qualify a LoRaWAN Device in Europe*, Semtech, Camarillo, CA, USA, 2018.

[59] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of LoRaWAN," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 34–40, Sep. 2017.

[60] LoRa Alliance Technical Commitee. (Nov. 10 2017). *LoRaWAN 1.1 Specification*. Accessed: Jun. 25, 2019. [Online]. Available: https://lora-alliance.org/sites/default/files/2018-04/lorawantm_specification_-v1.1.pdf

[61] W. Webb, "Standard's net gains," *Commun. Technol.*, vol. 8, no. 5, pp. 76–78, 2013.

[62] B. Ray. (Nov. 23, 2015). *What is Weightless?* Link Labs. Accessed: Jul. 17, 2018. [Online]. Available: https://www.link-labs.com/blog/what-is-weightless

[63] R. Quinnell. (Sep. 15, 2015), *Low Power Wide-Area Networking Alternatives for the IoT*. Accessed: Feb. 8, 2018. [Online]. Available: https://www.edn.com/Pdf/ViewPdf?contentItemId=4440343

[64] P. W. Webb. *Weightless: A Bespoke Technology for the IoT*. Cambridge, U.K.: Weightless SIG, 2013.

[65] R. Merritt. (Jan. 19, 2017). *IoT Network Reboots Its Efforts*. EE Times. Accessed: Jul. 17, 2017. [Online]. Available: https://www.eetimes.com/document.asp?doc_id=1331207&page_number=2

[66] C. McClelland. (Apr. 14, 2017). *So You Want to Use LPWAN for Your IoT Application, Now What? A Medium Corporation*. Accessed: Jul. 17, 2018. [Online]. Available: https://medium.com/iotforall/so-you-want-to-use-lpwan-for-your-iot-application-now-what-846cd9d14b30

[67] Weightless SIG. (Jul. 14, 2015). *Weightless-N Open Standard IoT Networks Deploy in Europe*. Accessed: Jul. 17, 2018. [Online]. Available: http://www.weightless.org/news/weightlessn-open-standard-iot-networks-deploy-in-europe

[68] A. Woolhouse. *Weightless-N Network Deployed Across London*. Weightless SIG. Accessed: Jul. 17, 2018. [Online]. Available: http://www.weightless.org/about/weightlessn-network-deployed-across-london

[69] K. Sweeney. (Sep. 25, 2017). *Weightless Tech now Shipping to Customers in 20 Countries. Business Weekly*. Accessed: Jul. 17, 2018. [Online]. Available: https://www.businessweekly.co.uk/news/hi-tech/weightless-tech-now-shipping-customers-20-countries

[70] Weightless SIG. *Weightless Specification*. Accessed: Jul. 17, 2018. [Online]. Available: http://www.weightless.org/about/weightless-specification

[71] S. O. Popescu and A. S. Gontean, "Performance comparison of the BPSK and QPSK modulation techniques on FPGA," in *Proc. IEEE 17th Int. Symp. Design Technol. Electron. Packag. (SIITME)*, Timisoara, Romania, Oct. 2011, pp. 257–260.

[72] S. S. Sarnin, N. Kadri, A. Mahyuni Mozi, N. A. Wahab, and N. F. Naim, "Performance analysis of BPSK and QPSK using error correcting code through AWGN," in *Proc. Int. Conf. Netw. Inf. Technol.*, Dhaka, Bangladesh, Jun. 2010, pp. 178–182.

[73] Ubiik. *Ultra Low Power*. Accessed: Feb. 8, 2018. [Online]. Available: https://www.ubiik.com/weightlessp-batterylife

[74] Ubiik. (2019). *Weightless*. Accessed: Jun. 25, 2019. [Online]. Available: https://www.ubiik.com/lpwan-technology

[75] Ubiik. *Long Range*. Accessed: Jun. 25, 2019. [Online]. Available: https://www.ubiik.com/range

[76] Ubiik. *Weightless vs LoRaWAN*. Accessed: Feb. 8, 2018. [Online]. Available: https://www.ubiik.com/embargo

[77] Ubiik. *LPWAN Comparison*. Accessed: Jul. 17, 2018. [Online]. Available: https://www.ubiik.com/lpwan-comparisons

[78] S. Universal. (Apr. 29, 2019). *The Importance of Weightless SIG*. Accessed: Aug. 26, 2019. [Online]. Available: https://www.sureuniversal.com/the-importance-of-the-weightless-sig/

[79] WAVIoT. (2018). *What is NB-Fi Protocol*. Accessed: Jul. 18, 2018. [Online]. Available: http://waviot.com/technology/what-is-nb-fi

[80] WAVIoT. (2018). *NB-Fi LPWA Network*. Accessed: Jul. 18, 2018. [Online]. Available: http://waviot.com/technology/waviot-lpwa-network

[81] A. Ikpehai, B. Adebisi, K. M. Rabie, K. Anoh, R. E. Ande, M. Hammoudeh, H. Gacanin, U. M. Mbanaso, "Low-power wide area network technologies for Internet-of-Things: A comparative review," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2225–2240, Apr. 2019.

[82] NB-Fi Alliance. (2018). *NB-Fi Alliance-Frequently Asked Questions*. Accessed: Jul. 18, 2018. [Online]. Available: https://nb-fi.org/en/

[83] WAVIoT. (Feb. 2018). *WAVIoT NB-Fi (V1) Transceiver Datasheet*. Accessed: Jun. 25, 2019. [Online]. Available: https://nb-fi.org/wp-content/uploads/2018/02/NB-Fi-Transceiver-specification-2.pdf

[84] M. Weyn, G. Ergeerts, R. Berkvens, B. Wojciechowski, and Y. Tabakov, "DASH7 alliance protocol 1.0: Low-power, mid-range sensor and actuator communication," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Tokyo, Japan, Oct. 2015, pp. 54–59.

[85] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, and J.-C. Prevotet, "Internet of mobile things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs standards and supported mobility," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1561–1581, 2nd Quart., 2019.

[86] *DASH7 Alliance Wireless Sensor and Actuator Network Protocol*, DASH7 Alliance, Brussels, Belgium, 2018.

[87] *Implementing Data Whitening and CRC Verification in Software in Kinetis KW01 Microcontrollers*, Freescale Semiconductor, Austin, TX, USA, 2015.

[88] X. Vilajosana, P. Tuset-Peiro, F. Vazquez-Gallego, J. Alonso-Zarate, and L. Alonso, "Standardized low-power wireless communication technologies for distributed sensing applications," *Sensors*, vol. 14, no. 2, pp. 2663–2682, Feb. 2014.

[89] G. Christiansen, *Data Whitening and Random TX Mode*. Dallas, TX, USA: Texas Instruments, 2010.

[90] G. Ergeerts, M. Nikodem, D. Subotic, T. Surmacz, B. Wojciechowski, P. De Meulenaere, and M. Weyn, "DASH7 alliance protocol in monitoring applications," in *Proc. 10th Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput. (3PGCIC)*, Krakow, Poland, Nov. 2015, pp. 623–628.

[91] A. D. Zayas and P. Merino, "The 3GPP NB-IoT system architecture for the Internet of Things," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Paris, France, May 2017, pp. 277–282.

[92] A. Hoglund, X. Lin, O. Liberg, A. Behravan, E. A. Yavuz, M. Van Der Zee, Y. Sui, T. Tirronen, A. Ratilainen, and D. Eriksson, "Overview of 3GPP release 14 enhanced NB-IoT," *IEEE Netw.*, vol. 31, no. 6, pp. 16–22, Nov./Dec. 2017.

[93] A. Hoglund, J. Bergman, X. Lin, O. Liberg, A. Ratilainen, H. S. Razaghi, T. Tirronen, and E. A. Yavuz, "Overview of 3GPP release 14 further enhanced MTC," *IEEE Commun. Standard Mag.*, vol. 2, no. 2, pp. 84–89, Jun. 2018.

[94] GSM Association. (Feb. 8, 2017). *NB-IoT Deployment Guide to Basic Feature set Requirements*. Accessed: Jul. 14, 2017. [Online]. Available: https://www.gsma.com/iot/wp-content/uploads/2017/08/CLP.28-v1.0.pdf

[95] R. Ratasuk, N. Mangalvedhe, D. Bhatoolaul, and A. Ghosh, "LTE-M evolution towards 5G massive MTC," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Singapore, Dec. 2017, pp. 1–6.

[96] M. Lauridsen, H. Nguyen, B. Vejlgaard, I. Z. Kovacs, P. Mogensen, and M. Sorensen, "Coverage comparison of GPRS, NB-IoT, LoRa, and SigFox in a 7800 km^2 Area," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Sydney, NSW, Australia, Jun. 2017, pp. 1–5.

[97] N. Networks. (2015). *LTE-M-Optimizing LTE for the Internet of Things-White Paper*. Accessed: Jul. 16, 2017. [Online]. Available: https://novotech.com/docs/default-source/default-document-library/lte-m-optimizing-lte-for-the-internet-of-things.pdf?sfvrsn=0

[98] A. Diaz-Zayas, C. A. Garcia-Perez, A. M. Recio-Perez, and P. Merino, "3GPP standards to deliver LTE connectivity for IoT," in *Proc. IEEE 1st Int. Conf. Internet Things Design Implement. (IoTDI)*, Berlin, Germany, Apr. 2016, pp. 283–288.

[99] S. Barros, J. Bazzo, O. Dos Reis Pereira, D. Carrillo, and J. Seki, "Evolution of long term narrowband-IoT," in *Proc. IEEE XXIV Int. Conf. Electron., Electr. Eng. Comput. (INTERCON)*, Cusco, Peru, Aug. 2017, pp. 1–4.

[100] Y.-P.-E. Wang, X. Lin, A. Adhikary, A. Grovlen, Y. Sui, Y. Blankenship, J. Bergman, and H. S. Razaghi, "A primer on 3GPP narrowband Internet of Things," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 117–123, Mar. 2017.

[101] R. Ratasuk, J. Tan, N. Mangalvedhe, M. H. Ng, and A. Ghosh, "Analysis of NB-IoT deployment in LTE guard-band," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Sydney, NSW, Australia, Jun. 2017, pp. 1–5.

[102] Telesystem Innovations. (2010). *LTE in a Nutshell: The Physical Layer White Paper*. Accessed: Jul. 15, 2018. [Online]. Available: https://home.zhaw.ch/kunr/NTM1/literatur/LTE%20in%20a%20Nutshell%20-%20Physical%20Layer.pdf
[103] Cisco Systems. (2016). *Power Saving Mode (PSM) in UEs*. Accessed: Jul. 15, 2018. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21/MME/b_21_MME_Admin/b_21_MME_Admin_chapter_0111010.pdf
[104] T. Shalev. (Nov. 23, 2016). *Cellular IoT Power Saving Techniques: How Do The New Cat-M1 and Cat-NB1 Protocols Achieve Ultra-Low Energy Consumption?* Ceva. Accessed: Aug. 13, 2018. [Online]. Available: https://www.ceva-dsp.com/ourblog/cellular-iot-power-saving-techniques-how-do-the-new-cat-m1-and-cat-nb1-protocols-achieve-ultra-low-energy-consumption/
[105] N. Mangalvedhe, R. Ratasuk, and A. Ghosh, "NB-IoT deployment study for low power wide area cellular IoT," in *Proc. IEEE 27th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Valencia, Spain, Sep. 2016, pp. 1–6.
[106] O. Liberg, M. Sundberg, E. Wang, J. Bergman and J. Sachs, *Cellular Internet of Things: Technologies, Standards, and Performance*. Cambridge, MA, USA: Academic, 2017.
[107] A. Ratilainen. (Nov. 2016). *NB-IoT presentation for IETF LPWAN*. Accessed: Jul. 30, 2017. [Online]. Available: https://datatracker.ietf.org/meeting/97/materials/slides-97-lpwan-30-nb-iot-presentation-00
[108] Y. Li, X. Cheng, Y. Cao, D. Wang, and L. Yang, "Smart choice for the smart grid: Narrowband Internet of Things (NB-IoT)," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1505–1515, Jun. 2018.
[109] Ericsson. (Sep. 26, 2018). *Ericsson and Telstra Complete Ground-Breaking Long-Range NB-IoT Connection*. Accessed: Jun. 26, 2019. [Online]. Available: https://www.ericsson.com/en/press-releases/2018/9/ericsson-and-telstra-complete-ground-breaking-long-range-nb-iot-connection
[110] European Telecommunications Standards Institute. (Aug. 2, 2017). *ETSI Work on Standards for the IoT*. Accessed: Jul. 16, 2018. [Online]. Available: http://ec.europa.eu/information_society/newsroom/image/document/2017-7/20170208_etsi_work_on_iot_-_etsi_dg_luis_jorge_romero-v3_CD79F6B8-BBF5-50E2-33A4113893A0ABFA_42878.pdf
[111] M. Elsaadany and W. Hamouda, "The new enhancements in LTE—A Rel-13 for reliable machine type communications," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Montreal, QC, Canada, Oct. 2017, pp. 1–5.
[112] O. Liberg. (Aug. 24, 2017). *The Cellular Internet of Things*. 3GPP. Accessed: Jul. 16, 2018. [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1906-c_iot
[113] WAVIoT. (Jun. 6, 2016). *WAVIoT NB-Fi LPWAN Technology Products and Tech Description*. Accessed: Jul. 18, 2018. [Online]. Available: https://waviot.com/wp.pdf
[114] SigFox. (2019). *Radio Technology Keypoints*. Accessed: Aug. 26, 2019. [Online]. Available: https://www.sigfox.com/en/sigfox-iot-radio-technology
[115] J. Schlienz and D. Raddino. *Narrowband Internet of Things White Paper*. Accessed: Jul. 15, 2018. [Online]. Available: https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_application/application_notes/1ma266/1MA266_0e_NB_IoT.pdf
[116] H. Wang and A. O. Fapojuwo, "A survey of enabling technologies of low power and long range machine-to-machine communications," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2621–2639, 4th Quart., 2017.
[117] M. A. N. Sukar and M. Pal, "SC-FDMA & OFDMA in LTE physical layer," *Int. J. Eng. Trends Technol.*, vol. 12, no. 2, pp. 74–85, 2014.
[118] K. E. Nolan, W. Guibene, and M. Y. Kelly, "An evaluation of low power wide area network technologies for the Internet of Things," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Paphos, Cyprus, Sep. 2016, pp. 439–444.
[119] Y. Roth, L. Ros, J.-B. Dore, and V. Berg. (Oct. 7, 2017). *The Physical Layer for Low Power Wide Area Networks: A Study of Combined Modulation and Coding Associated with an Iterative Receiver*. Accessed: Jan. 2, 2019. [Online]. Available: https://hal.archives-ouvertes.fr/tel-01568794v2/file/170710_defence.pdf
[120] A. Alexiou, C. Bouras, V. Kokkinos, A. Papazois, and G. Tseliou, "Enhancing FEC application in LTE cellular networks," in *Proc. IFIP Wireless Days*, Venice, Italy, Oct. 2010, pp. 1–5.
[121] O. Liberg, M. Sundberg, E. Wang, J. Bergman and J. Sachs, *Cellular Internet of Things: Technologies, Standards and Performance*. Cambridge, MA, USA: Academic, 2017.
[122] WavIoT. *NB-Fi Transceiver*. Accessed: Feb. 8, 2018. [Online]. Available: http://waviot.com/product/uncategorized/nb-fi-transceiver
[123] S. Tabbane. (Oct. 17–19, 2018). *Session 5: NB-IoT Networks*. Accessed: Jun. 28, 2019. [Online]. Available: https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/ITU-ASP-CoE-Training-on-/Session5_NB_IoT%20networks%20web.pdf
[124] M. Grabia, T. Markowski, J. Mruczkiewicz, and K. Plec, "Design of a DASH7 low power wireless sensor network for Industry 4.0 applications," in *Proc. IEEE Int. Conf. RFID Technol. Appl. (RFID-TA)*, Warsaw, Poland, Sep. 2017, pp. 254–259.
[125] *LoRaWAN and Cellular IoT (NB-IoT, LTE-M)-How do they Complement Each Other?* Actility SA, Lannion, France, 2018.
[126] (2019). *NB-Fi Alliance*. Accessed: Aug. 26, 2019. [Online]. Available: https://nb-fi.org/en/
[127] *Evaluation of LTE-M Towards 5G IoT Requirements*, Sierra Wireless, Richmond, BC, Canada, Dec. 2017.
[128] D. M. Hernandez, G. Peralta, L. Manero, R. Gomez, J. Bilbao, and C. Zubia, "Energy and coverage study of LPWAN schemes for industry 4.0," in *Proc. IEEE Int. Workshop Electron., Control, Meas., Signals Their Appl. Mechatronics (ECMSM)*, Donostia-San Sebastian, Spain, May 2017, pp. 1–6.
[129] Radiocrafts. (Aug. 8, 2017). *[SIGFOX] What is the Battery Lifetime of a SIGFOX Device?* Accessed: Nov. 19, 2019. [Online]. Available: https://radiocrafts.com/kb/battery-lifetime-sigfox-device/
[130] SigFox Partner Network. *Modulus Two Monitor and Remote Controlling*. Accessed: Dec. 19, 2019. [Online]. Available: https://partners.sigfox.com/products/modulus-two
[131] M. Harttree. (Sep. 15, 2017). *Get 10 Years From 9 Volts: The Power of LoRaWAN*. Cisco Systems. Accessed: Dec. 19, 2019. [Online]. Available: https://blogs.cisco.com/government/get-10-years-from-9-volts-the-power-of-lorawan
[132] Weightless SIG. (Nov. 8, 2015). *Weightless-P Standard is Designed for High Performance, Low Power, 2-Way Communication for IoT*. Accessed: Apr. 12, 2018. [Online]. Available: http://www.weightless.org/news/weightlessp-standard-is-designed-for-high-performance-low-power-2way-communication-for-iot
[133] WAVIoT. *WAVIoT NB-Fi LPWAN Technology Products and Tech Description*. Accessed: Dec. 19, 2019. https://nb-fi.org/wp_WAVIoT.pdf
[134] D. Piromalis, K. Aravanitis, and N. Sigrimis, "DASH7 mode 2: A promising perspective for wireless agriculture," in *Proc. 4th IFAC Conf. Modeling Control Agricult., Horticulture*, Espoo, Finland, 2013, pp. 1–7.
[135] O. Cetinkaya and O. B. Akan, "A DASH7-based power metering system," in *Proc. 12th Annu. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, Jan. 2015, pp. 406–411.
[136] M. Arsalan, A. Umair, and V. K. Verma, "DASH7: Performance," *IOSR J. Electron. Commun. Eng.*, vol. 2, no. 5, pp. 8–11, 2012.
[137] G. Vos, J. Bergman, Y. Bitran, M. Beale, M. Cannon, R. Holden, Y. S. Chan, G. Vivier, R. Le Bras, T. Wakayama, R. Ratasuk, N. Okubo, N. Park, Y. Akimoto, S. Lee, S. Trope, and F. Mertz. (Dec. 2017). *Evaluation of LTE-M Towards 5G IoT Requirements*. Accessed: Dec. 19, 2019. [Online]. Available: https://pdfs.semanticscholar.org/8e48/d692e13868cf1e0910867be5edca55d52852.pdf
[138] CNXSoft. (Jan. 9, 2015). *Comparison Table of Low Power WAN Standards for Industrial Applications*. Accessed: Jul. 29, 2018. [Online]. Available: https://www.cnx-software.com/2015/09/21/comparison-table-of-low-power-wan-standards-for-industrial-applications/
[139] M. Lauridsen, I. Z. Kovacs, P. Mogensen, M. Sorensen, and S. Holst, "Coverage and capacity analysis of LTE-M and NB-IoT in a rural area," in *Proc. IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, Montreal, QC, Canada, Sep. 2016, pp. 1–5.
[140] W. Xue-fen, Y. Yi, and C. Jian, "Wireless sensor node with lightning and atmospheric pressure detection for severe convective weather warning networks," in *Proc. Int. Symp. Sens. Instrum. IoT Era (ISSI)*, Shanghai, China, Sep. 2018, pp. 1–6.
[141] L. H. Trinh, V. X. Bui, F. Ferrero, T. Q. K. Nguyen, and M. H. Le, "Signal propagation of LoRa technology using for smart building applications," in *Proc. IEEE Conf. Antenna Meas. Appl. (CAMA)*, Tsukuba, Japan, Dec. 2017, pp. 381–384.
[142] T. Ameloot, P. Van Torre, and H. Rogier, "LoRa indoor performance: An office environment case study," in *Proc. Int. Appl. Comput. Electromagn. Soc. Symp.-China (ACES)*, Beijing, China, Jul. 2018, pp. 1–2.

[143] J. Petajajarvi, K. Mikhaylov, M. Hamalainen, and J. Iinatti, "Evaluation of LoRa LPWAN technology for remote health and wellbeing monitoring," in *Proc. 10th Int. Symp. Med. Inf. Commun. Technol. (ISMICT)*, Worcester, MA, USA, Mar. 2016, pp. 1–5.

[144] The Things Network. (2019). *Building a global open LoRaWAN Network*. Accessed: Aug. 26, 2019. [Online]. Available: https://www.thethingsnetwork.org/

[145] SigFox. *SigFox Buy*. Accessed: Dec. 19, 2019. [Online]. Available: https://buy.sigfox.com/buy

[146] A. Woolhouse. (May 20, 2016). *Choosing LPWAN Technology for Lowest Cost*. IoT Business Newa. Accessed: Aug. 26, 2019. [Online]. Available: https://iotbusinessnews.com/2016/05/20/90290-choosing-lpwan-technology-lowest-cost/

[147] P. Sayer. (Sep. 26, 2017). *SigFox Shows 20-Cent IoT Wireless Module*. IT World. Accessed: Aug. 26, 2019. [Online]. Available: https://www.itworld.com/article/3226476/sigfox-shows-20-cent-iot-wireless-module.html

[148] The Things Network. (2019). *Network Architecture*. Accessed: Jan. 13, 2019. [Online]. Available: https://www.thethingsnetwork.org/docs/network/architecture.html

[149] The Things Network. (2019). *Technology Stack*. Accessed: Aug. 26, 2019. [Online]. Available: https://www.thethingsnetwork.org/tech-stack#section1

[150] The Things Network. (2019). *The Things Network Console*. Accessed: Aug. 26. 2019. [Online]. Available: https://www.thethingsnetwork.org/docs/network/console/

[151] LoRa Server. (2019). *LoRa Server, Open-Source LoRaWAN Network-Server*. Accessed: Aug. 26, 2019. [Online]. Available: https://www.loraserver.io/

[152] Telstra. (2019). *IoT Platform*. Accessed: Aug. 26, 2019. [Online]. Available: https://www.telstra.com.au/business-enterprise/solutions/internet-of-things/platforms-and-services/iot-platform

[153] Telstra. (2019). *Telstra IoT Network*. Accessed: Aug. 26, 2019. [Online]. Available: https://www.telstra.com.au/business-enterprise/solutions/internet-of-things/iot-coverage

[154] J. I. Laveyne, G. V. Eetvelde, and L. Vandevelde, "Application of LoRaWAN for smart metering: An experimental verification," *Int. J. Contemp. Energy*, vol. 4, no. 1, pp. 61–67, 2018.

[155] TCAA Limited. (Mar. 23, 2017). *Technical Primer-Current and Emerging SCADA Wireless Bearers*. Accessed: Jul. 29, 2019. [Online]. Available: https://tcca.info/documents/2018-march_technical_primer_current_and_emerging_scada_wireless_bearers.pdf/

[156] H. Saputra and Z. Zhao, "Long term key management architecture for SCADA systems," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Singapore, Feb. 2018, pp. 314–319.

[157] P. Sommer, Y. Maret, and D. Dzung, "Low-power wide-area networks for industrial sensing applications," in *Proc. IEEE Int. Conf. Ind. Internet (ICII)*, Seattle, WA, USA, Oct. 2018, pp. 23–32.

[158] B. V. Philip, T. Alpcan, J. Jin, and M. Palaniswami, "Distributed real-time IoT for autonomous vehicles," *IEEE Trans. Ind. Inf.*, vol. 15, no. 2, pp. 1131–1140, Feb. 2019.

[159] Y. Li, L. Yang, S. Han, X. Wang, and F.-Y. Wang, "When LPWAN meets ITS: Evaluation of low power wide area networks for V2X communications," in *Proc. 21st Int. Conf. Intell. Transp. Syst. (ITSC)*, Maui, HI, USA, Nov. 2018, pp. 473–478.

[160] A. Shaik, N. Bowen, J. Bole, G. Kunzi, D. Bruce, A. Abdelgawad, and K. Yelamarthi, "Smart car: An IoT based accident detection system," in *Proc. IEEE Global Conf. Internet Things (GCIoT)*, Alexandria, Egypt, Dec. 2018, pp. 1–5.

[161] A. M. Elshaer, M. M. Elrakaiby, and M. E. Harb, "Autonomous car implementation based on CAN bus protocol for IoT applications," in *Proc. 13th Int. Conf. Comput. Eng. Syst. (ICCES)*, Cairo, Egypt, Dec. 2018, pp. 275–278.

[162] National Instruments. (May 3, 2019). *Understanding CAN With Flexible Data-Rate (CAN FD)*. Accessed: Feb. 8, 2019. [Online]. Available: https://www.ni.com/en-au/innovations/white-papers/14/understanding-can-with-flexible-data-rate–can-fd-.html

[163] A. K. Pundir, J. D. Jagannath, and L. Ganapathy, "Improving supply chain visibility using IoT-Internet of Things," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Las Vegas, NV, USA, Jan. 2019, pp. 156–162.

[164] A. Pal and K. Kant, "IoT-based sensing and communications infrastructure for the fresh food supply chain," *Computer*, vol. 51, no. 2, pp. 76–80, Feb. 2018.

[165] P. Silva, V. Kaseva, and E. Lohan, "Wireless positioning in IoT: A look at current and future trends," *Sensors*, vol. 18, no. 8, p. 2470, Jul. 2018.

[166] A. Mohsin and S. S. Yellampalli, "IoT based cold chain logistics monitoring," in *Proc. IEEE Int. Conf. Power, Control, Signals Instrum. Eng. (ICPCSI)*, Chennai, India, Sep. 2017, pp. 1971–1974.

[167] S. Lu and X. Wang, "Toward an intelligent solution for perishable food cold chain management," in *Proc. 7th IEEE Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Beijing, China, Aug. 2016, pp. 852–856.

[168] V. Fore, A. Khanna, R. Tomar, and A. Mishra, "Intelligent supply chain management system," in *Proc. Int. Conf. Adv. Comput. Commun. Eng. (ICACCE)*, Durban, South Africa, 2016, pp. 296–302.

[169] A. Valach and D. Macko, "Exploration of the LoRa technology utilization possibilities in healthcare IoT devices," in *Proc. 16th Int. Conf. Emerg. eLearn. Technol. Appl. (ICETA)*, Stary Smokovec, Slovakia, Nov. 2018, pp. 623–628

[170] Rohde & Schwarz. (2019). *R&S CMWcards Simplifies Verifying Your NB-IoT OTDOA Positioning Design*. Accessed: Aug. 14, 2019. [Online]. Available: https://www.rohde-schwarz.com/au/applications/r-s-cmwcards-simplifies-verifying-your-nb-iot-otdoa-positioning-design-application-card_56279-596352.html

[171] SigFox. *Monarch*. Accessed: Dec. 19, 2019. [Online]. Available: https://build.sigfox.com/monarch

[172] A. Morris. (Jun. 6, 2019). *Orange Flags LTE-M Roaming With AT&T, KPN, and Swisscom*. SDX Central. Accessed: Dec. 19, 2019. [Online]. Available: https://www.sdxcentral.com/articles/news/orange-flags-lte-m-roaming-with-att-kpn-and-swisscom/2019/06/

[173] GSM Association. (Apr. 6, 2018). *GSMA Announces Completion of First European NB-IoT Roaming Trial*. Accessed: Dec. 19, 2019. [Online]. Available: https://www.gsma.com/newsroom/press-release/gsma-announces-completion-of-first-european-nb-iot-roaming-trial/

[174] K. Hill. (Oct. 23, 2019). *Vodafone Strikes NB-IoT Roaming Deal With AT&T, Opens US Iot Lab*. RCR Wireless News. Accessed: Dec. 19, 2019. [Online]. Available: https://www.rcrwireless.com/20191023/internet-of-things/vodafone-att-strike-nb-iot-roaming-deal

[175] Orange Business Services. (Feb. 23, 2018). *Successful International Roaming Test Between Orange and KPN LoRaWAN Networks With Actility Opens New Horizons for IoT Business Applications*. Accessed: Dec. 19, 2019. [Online]. Available: https://www.orange-business.com/en/press/international-lorawan-roaming-trial-success

[176] L. Anciaux. (Dec. 6, 2018). *LoRaWAN Roaming. State of Deployments, Business Needs and Alternatives*. IoT Factory. Accessed: Dec. 19, 2019. [Online]. Available: https://iotfactory.eu/lorawan-roaming-state-of-deployments-business-needs-and-alternatives/

[177] S. Abraham, J. Beard, and R. Manijacob, "Remote environmental monitoring using Internet of Things (IoT)," in *Proc. IEEE Global Humanitarian Technol. Conf. (GHTC)*, San Jose, CA, USA, Oct. 2017, pp. 1–6.

[178] S. Fang, L. Da Xu, Y. Zhu, J. Ahati, H. Pei, J. Yan, and Z. Liu, "An integrated system for regional environmental monitoring and management based on Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1596–1605, May 2014.

[179] E. A. Kadir, A. Efendi, and S. L. Rosa, "Application of LoRa WAN sensor and IoT for environmental monitoring in Riau province Indonesia," in *Proc. 5th Int. Conf. Electr. Eng., Comput. Sci. Inform. (EECSI)*, Malang, Indonesia, Oct. 2018, pp. 1–5.

[180] N. H. A. Rahman, Y. Yamada, M. H. Husni, and N. H. A. Aziz, "Analysis of propagation link for remote weather monitoring system through LoRa gateway," in *Proc. 2nd Int. Conf. Telematics Future Gener. Netw. (TAFGEN)*, Kuching, Malaysia, Jul. 2018, pp. 55–60.

[181] H. Wang, Y. Wei, H. Zhu, Y. Liu, C. K. Wu, and K. Fung Tsang, "NB–IoT based tree health monitoring system," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Melbourne, Australia, Feb. 2019.

[182] X. Liu, T. Yang, and B. Yan, "Internet of Things for wildlife monitoring," in *Proc. IEEE/CIC Int. Conf. Commun. China-Workshops (CIC/ICCC)*, Shenzen, China, Nov. 2015, pp. 62–65.

[183] M. Schadhauser, J. Robert, and A. Heuberger, "Concept for an adaptive low power wide area (LPWA) bat communication network," in *Proc. Eur. Conf. Smart Objects, Syst. Technol. Smart (SysTech)*, Duisburg, Germany, 2016, pp. 1–9.

[184] J. Wotherspoon, R. Wolhuter, and T. Niesler, "Choosing an integrated radio-frequency module for a wildlife monitoring wireless sensor network," in *Proc. IEEE AFRICON*, Cape Town, South Africa, Sep. 2017.

[185] E. D. Ayele, N. Meratnia, and P. J. Havinga, "MANER: Managed data dissemination scheme for LoRa IoT enabled wildlife monitoring system (WMS)," in *Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Paris, France, Feb. 2018, pp. 1–7.

[186] E. D. Ayele, K. Das, N. Meratnia, and P. J. Havinga, "Leveraging BLE and LoRa in IoT network for wildlife monitoring system (WMS)," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Singapore, Feb. 2018, pp. 342–348.

[187] N. Havard, S. Mcgrath, C. Flanagan, and C. Macnamee, "Smart building based on Internet of Things technology," in *Proc. 12th Int. Conf. Sens. Technol. (ICST)*, Limerick, Ireland, Dec. 2018, pp. 342–348.

[188] X. Chen, J. Chen, Y. Wu, L. Qian, L. Huang, Z. Shi, and L. Meng, "Design of indoor temperature monitoring system based on narrowband Internet of Things," in *Proc. 24th Asia–Pacific Conf. Commun. (APCC)*, Ningbo, China, Nov. 2018, pp. 604–609.

[189] J. Wang, J. Su, and R. Hua, "Design of a smart independent smoke sense system based on NB-IoT technology," in *Proc. Int. Conf. Intell. Transp., Big Data Smart City (ICITBS)*, Changsha, China, Jan. 2019, pp. 397–400.

[190] C. Yoon, M. Huh, S.-G. Kang, J. Park, and C. Lee, "Implement smart farm with IoT technology," in *Proc. 20th Int. Conf. Adv. Commun. Technol. (ICACT)*, Chuncheon-si Gangwon-do, Korea, Feb. 2018, pp. 749–752.

[191] O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow, and M. N. Hindia, "An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3758–3773, Oct. 2018.

[192] R. K. Kodali, S. Yerroju, and S. Sahu, "Smart farm monitoring using LoRa enabled IoT," in *Proc. 2nd Int. Conf. Green Comput. Internet Things (ICGCIoT)*, Bangalore, India, Aug. 2018.

[193] M. T. Buyukakkaslar, M. A. Erturk, M. A. Aydin, and L. Vollero, "LoRaWAN as an e-health communication technology," in *Proc. IEEE 41st Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Turin, Italy, Jul. 2017, pp. 391–394.

[194] T. Hirata, K. Terada, M. Toyota, Y. Takada, K. Matsumoto, and M. S. Tanaka, "Proposal of a power saving network for rice fields using LoRa," in *Proc. IEEE 6th Global Conf. Consum. Electron. (GCCE)*, Nagoya, Japan, Oct. 2017, pp. 1–4.

[195] A. F. Rachmani and F. Y. Zulkifli, "Design of IoT monitoring system based on LoRa technology for starfruit plantation," in *Proc. IEEE Region 10 Conf. (TENCON)*, Jeju, South Korea, Oct. 2018, pp. 1241–1245.

[196] D. Yim, J. Chung, Y. Cho, H. Song, D. Jin, S. Kim, S. Ko, A. Smith, and A. Riegsecke, "An experimental LoRa performance evaluation in tree farm," in *Proc. IEEE Sensors Appl. Symp. (SAS)*, Seoul, South Korea, Mar. 2018, pp. 1–6.

[197] M. G. Ikhsan, M. Y. A. Saputro, D. A. Arji, R. Harwahyu, and R. F. Sari, "Mobile LoRa gateway for smart livestock monitoring system," in *Proc. IEEE Int. Conf. Internet Things Intell. Syst. (IOTAIS)*, Bali, Indonesia, Nov. 2018, pp. 46–51.

[198] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, "Assessment of communication technologies supporting smart streetlighting applications," in *Proc. IEEE Int. Smart Cities Conf. (ISC2)*, Kansas City, MO, USA, Sep. 2018, pp. 1–7.

[199] R. Ramesh, S. Acharya, V. Rajaraman, A. Babu, A. Joglekar, A. Sharma, B. Amrutur, and P. Namekar, "Interoperable middleware for smartcities streetlighting on LoRaWAN as a case study," in *Proc. 11th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Bengaluru, India, Jan. 2019, pp. 550–552.

[200] L. Zhao, Q. Gao, R. Wang, N. Fang, Z. Jin, N. Wan, and L. Xu, "Intelligent street light system based on NB-IoT and energy-saving algorithm," in *Proc. 3rd Int. Conf. Smart Sustain. Technol. (SpliTech)*, Split, Croatia, 2018, pp. 1–6.

[201] E. Bingol, M. Kuzlu, and M. Pipattanasompom, "A LoRa-based smart streetlighting system for smart cities," in *Proc. 7th Int. Istanbul Smart Grids Cities Congr. Fair (ICSG)*, Istanbul, Turkey, Apr. 2019, pp. 66–70.

[202] A. T. Thakar and S. Pandya, "Survey of IoT enables healthcare devices," in *Proc. Int. Conf. Comput. Methodol. Commun. (ICCMC)*, Erode, India, Jul. 2017.

[203] S. Sonune, D. Kalbande, A. Yeole, and S. Oak, "Issues in IoT healthcare platforms: A critical study and review," in *Proc. Int. Conf. Intell. Comput. Control (I2C2)*, Coimbatore, India, Jun. 2017, pp. 1–5.

[204] S. Anand and S. K. Routray, "Issues and challenges in healthcare narrowband IoT," in *Proc. Int. Conf. Inventive Commun. Comput. Technol. (ICICCT)*, Coimbatore, India, Mar. 2017, pp. 486–489.

[205] F. Fernandez and G. C. Pallis, "Opportunities and challenges of the Internet of Things for healthcare: Systems engineering perspective," in *Proc. 4th Int. Conf. Wireless Mobile Commun. Healthcare-Transforming Healthcare Through Innov. Mobile Wireless Technol. (MOBIHEALTH)*, Athens, Greece, 2014, pp. 263–266.

[206] A. Mdhaffar, T. Chaari, K. Larbi, M. Jmaiel, and B. Freisleben, "IoT-based health monitoring via LoRaWAN," in *Proc. IEEE 17th Int. Conf. Smart Technol. (EUROCON)*, Ohrid, Macedonia, Jul. 2017, pp. 519–524.

[207] A. Yearp, D. Newell, P. Davies, R. Wade, and R. Sahandi, "Wireless remote patient monitoring system: Effects of interference," in *Proc. 10th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, Fukuoka, Japan, Jul. 2016, pp. 367–370.

[208] T. Sondrol, B. Jalaian, and N. Suri, "Investigating LoRa for the Internet of battlefield things: A cyber perspective," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Los Angeles, CA, USA, Oct. 2018, pp. 749–756.

[209] M. P. Đurišic, Z. Tafa, G. Dimić, and V. Milutinović, "A survey of military applications of wireless sensor networks," in *Proc. Medit. Conf. Embedded Comput. (MECO)*, Bar, Montenegro, 2012, pp. 196–199.

[210] C. Xiaojun, L. Xianpeng, and X. Peng, "IOT-based air pollution monitoring and forecasting system," in *Proc. Int. Conf. Comput. Comput. Sci. (ICCCS)*, Noida, India, Jan. 2015, pp. 257–260.

[211] B. Sudantha, E. Warusavitharana, G. Ratnayake, P. Mahanama, M. Cannata, and D. Strigaro, "Building an open-source environmental monitoring system—A review of state-of-the-art and directions for future research," in *Proc. 3rd Int. Conf. Inf. Technol. Res. (ICITR)*, Moratuwa, Sri Lanka, Dec. 2018, pp. 1–9.

[212] B. Jalaian, T. Gregory, N. Suri, S. Russell, L. Sadler, and M. Lee, "Evaluating LoRaWAN-based IoT devices for the tactical military environment," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Singapore, Feb. 2018.

[213] A. Kott, A. Swami, and B. J. West, "The Internet of battle things," *Computer*, vol. 49, no. 12, pp. 70–75, Dec. 2016.

[214] A. Minaburo, Acklio, L. Toutain, IMT-Atlantique, C. Gomez, U. P. D. Catalunya, D. Barthel, O. Labs, and Z. Zuniga, *Static Context Header Compression (SCHC) and Fragmentation for LPWAN, Application to UDP/IPv6*, document Internet-Draft draft-ietf-lpwan-ipv6-static-context-hc-21, SigFox, May 2019. Accessed: Dec. 18, 2019. [Online]. Available: https://tools.ietf.org/html/draft-ietf-lpwan-ipv6-static-context-hc-24

[215] S. Chacko and D. Job, "Security mechanisms and Vulnerabilities in LPWAN," in *Proc. IOP Conf. Ser., Mater. Sci. Eng.*, Jakarta, Indonesia, 2018, Art. no. 012027.

[216] Y.-C. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in *Proc. IEEE 32nd Annu. Joint Conf. IEEE Comput. Commun. Societies (INFOCOM)*, San Francisco, CA, USA, Mar. 2004, pp. 1976–1986.

[217] V. K. Raju and K. V. Kumar, "A simple and efficient mechanism to detect and avoid wormhole attacks in mobile ad hoc networks," in *Proc. Int. Conf. Comput. Sci.*, Phagwara, India, Sep. 2012, pp. 271–275.

[218] S. M. Danish, A. Nasir, H. K. Qureshi, A. B. Ashfaq, S. Mumtaz, and J. Rodriguez, "Network intrusion detection system for jamming attack in LoRaWAN join procedure," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kansas City, MO, USA, May 2018.

[219] J. Kim and J. Song, "A secure device-to-device link establishment scheme for LoRaWAN," *IEEE Sensors J.*, vol. 18, no. 5, pp. 2153–2160, Mar. 2018.

[220] K. R. Özyılmaz and A. Yurdakul, "Work-in-progress: Integrating low-power IoT devices to a blockchain-based infrastructure," in *Proc. Int. Conf. Embedded Softw. (EMSOFT)*, Seoul, South Korea, 2017, pp. 1–2.

[221] Sigfox Corner. (Sep. 11, 2016). *Sigfox Offers IoT Connectivity From $US3.00 Per Device*. Accessed: Aug. 26, 2019. [Online]. Available: https://www.iotaustralia.org.au/2016/11/09/iotnewsglobal/sigfox-ultra-low-cost-iot-connectivity/.

[222] J. C. Zuniga and B. Ponsard. (Jul. 2016). *SIGFOX System Description*. Accessed: Jul. 29, 2018. [Online]. Available: https://www.ietf.org/proceedings/96/slides/slides-96-lpwan-10.pdf

[223] DK Electronics. (Sep. 8, 2018). *Semtech Corporation SX1276IMLTRT*. Accessed: Oct. 8, 2018. [Online]. Available: https://www.digikey.com/product-detail/en/semtech-corporation/SX1276IMLTRT/SX1276IMLTRTCT-ND/4259551

[224] DK Electronics. (Sep. 8, 2018). *Microchip Technology ATA8520D-GHQW*. Accessed: Oct. 8, 2018. [Online]. Available: https://www.digikey.com.au/product-detail/en/microchip-technology/ATA8520D-GHQW/1611-ATA8520D-GHQWCT-ND/6831846

[225] O. S. Campillo and I. Demirkol, "Security issues in Internet of Things," M.S. thesis, Tech. Univ. Catalonia, TelecomBCN, Barcelona, Spain, 2017. [Online]. Available: https://upcommons.upc.edu/handle/2117/109290

[226] Ubiik. (Jan. 9, 2016). *Weightless-P LPWAN SDK Launches at CTIA*. Accessed: Jan. 15, 2019. [Online]. Available: http://www.weightless.org/news/weightlessp-lpwan-sdk-launches-at-ctia

[227] M. O. Farooq and D. Pesch, "Analyzing LoRa: A use case perspective," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Singapore, Feb. 2018, pp. 355–360.

[228] M. Saravanan, A. Das, and V. Iyer, "Smart water grid management using LPWAN IoT technology," in *Proc. Global Internet Things Summit (GIoTS)*, Geneva, Switzerland, Jun. 2017, pp. 1–6.

[229] E.-M. Oproiu, M. Iordache, C. Patachia, C. Costea, and I. Marghescu, "Development and implementation of a smart city use case in a 5G mobile network's operator," in *Proc. 25th Telecommun. Forum (TELFOR)*, Belgrade, Serbia, Nov. 2017, pp. 1–4.

[230] M. B. Soudan, H. M. Al Rifaie, T. M. Asmar, and S. Majzoub, "Smart home energy management system: An exploration of IoT use cases," in *Proc. Adv. Sci. Eng. Technol. Int. Conf. (ASET)*, Abu Dhabi, United Arab Emirates, Feb. 2018.

[231] S. E. Khateeb, "IoT architecture a gateway for smart cities in Arab world," in *Proc. 15th Learn. Technol. Conf. (L&T)*, Jeddah, Saudi Arabia, Feb. 2018.

[232] *Weightless-P System Specification*, Weightless SIG, Cambridge, U.K., 2015.

[233] A. M. Manoharan and V. Rathinasabapathy, "Smart water quality monitoring and metering using Lora for smart villages," in *Proc. 2nd Int. Conf. Smart Grid Smart Cities (ICSGSC)*, Kuala Lumpur, Malaysia, Aug. 2018.

[234] G. Wibisono, S. G. Permata, A. Awaludin, and P. Suhasfan, "Development of advanced metering infrastructure based on LoRa WAN in PLN Bali toward Bali Eco smart grid," in *Proc. Saudi Arabia Smart Grid (SASG)*, Jeddah, Saudi Arabia, Dec. 2017.

[235] F. Facchini, G. M. Vitetta, A. Losi, and F. Ruscelli, "On the performance of 169 MHz WM–Bus and 868 MHz LoRa technologies in smart metering applications," in *Proc. IEEE 3rd Int. Forum Res. Technol. Soc. Ind. (RTSI)*, Modena, Italy, Sep. 2017.

[236] M. Chen, Y. Miao, Y. Hao, and K. Hwang, "Narrow band Internet of Things," *IEEE Access*, vol. 5, pp. 20557–20577, 2017.

[237] Ubiik. (Mar. 14, 2017). *Ubiik Launches Weightless-P Kit*. Accessed: Jul. 30, 2019. [Online]. Available: http://www.weightless.org/news/ubiik-launches-weightlessp-kit

[238] A. Srinivasan, "IoT cloud based real time automobile monitoring system," in *Proc. 3rd IEEE Int. Conf. Intell. Transp. Eng. (ICITE)*, Singapore, Sep. 2018, pp. 231–235.

[239] N. S. Rajput, Mukesh, A. Mishra, A. Sisodia, and I. Makarov, "A novel autonomous taxi model for smart cities," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Singapore, Feb. 2018, pp. 625–628.

[240] D. Kwon, S. Park, S. Baek, R. K. Malaiya, G. Yoon, and J.-T. Ryu, "A study on development of the blind spot detection system for the IoT-based smart connected car," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Las Vegas, NV, USA, Jan. 2018, pp. 1–4.

[241] Y.-S. Chou, Y.-C. Mo, J.-P. Su, W.-J. Chang, L.-B. Chen, J.-J. Tang, and C.-T. Yu, "i-Car system: A LoRa-based low power wide area networks vehicle diagnostic system for driving safety," in *Proc. Int. Conf. Appl. Syst. Innov. (ICASI)*, Sapporo, Japan, May 2017, pp. 781–791.

[242] Y. U. Devi and M. S. S. Rukmini, "IoT in connected vehicles: Challenges and issues—A review," in *Proc. Int. Conf. Signal Process., Commun., Power Embedded Syst. (SCOPES)*, Paralakhemundi, India, Oct. 2016, pp. 1864–1867.

[243] Y. Li, S. Han, L. Yang, F.-Y. Wang, and H. Zhang, "LoRa on the move: Performance evaluation of LoRa in V2X communications," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Changshu, China, Jun. 2018, pp. 1107–1111.

[244] S. Mahmood, R. Hasan, A. Ullah, and K. U. Sarker, "SMART security alert system for monitoring and controlling container transportation," in *Proc. 4th MEC Int. Conf. Big Data Smart City (ICBDSC)*, Muscat, Oman, Jan. 2019, pp. 1–5.

[245] G. Qiaolun and G. Tiegang, "R/M integrated supply Chain based on IoT," in *Proc. 14th IEEE Int. Conf. Comput. Sci. Eng.*, Dalian, China, Aug. 2011, pp. 290–294.

[246] S. Uddin and A. A. A. A. Sharif, "Integrating Internet of Things with maintenance spare parts' supply chain," in *Proc. 5th Int. Conf. Electron. Devices, Syst. Appl. (ICEDSA)*, Ras Al Khaimah, United Arab Emirates, Dec. 2016, pp. 1–4.

[247] S. Jianli, "Design and implementation of LOT-based logistics management system," in *Proc. IEEE Symp. Elect. Electron. Eng. (EEESYM)*, Kuala Lumpur, Malaysia, 2012, pp. 603–606.

[248] Y. Gu and T. Jing, "The IOT research in supply chain management of fresh agricultural products," in *Proc. 2nd Int. Conf. Artif. Intell., Manage. Sci. Electron. Commerce (AIMSEC)*, Dengleng, China, Aug. 2011, pp. 7382–7385.

[249] A. A. and R. G., "Earthquake early warning system by IOT using Wireless sensor networks," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Chennai, India, Mar. 2016, pp. 1201–1205.

[250] D. Purkovic, L. Coates, M. Honsch, D. Lumbeck, and F. Schmidt, "Smart river monitoring and early flood detection system in Japan developed with the EnOcean long range sensor technology," in *Proc. 2nd Int. Colloq. Smart Grid Metrol. (SMAGRIMET)*, Split, Croatia, Apr. 2019, pp. 1–6.

[251] H. Mulani and A. Gawade, "Environmental monitoring in IoT," in *Proc. Int. Conf. Current Trends Comput., Electr., Electron. Commun. (CTCEEC)*, Mysore, India, Sep. 2017, pp. 198–206.

[252] R. P. Hudhajanto, N. Fahmi, E. Prayitno, and Rosmida, "Real-time monitoring for environmental through wireless sensor network technology," in *Proc. Int. Conf. Appl. Eng. (ICAE)*, Batam, Indonesia, Oct. 2018, pp. 1–5.

[253] F. Wu, C. Rudiger, J.-M. Redoute, and M. R. Yuce, "Live demonstration: An IoT platform for environmental monitoring using self-powered sensors," in *Proc. IEEE SENSORS*, New Delhi, India, Oct. 2018, p. 1.

[254] D. Punniamoorthy, V. S. Kamadal, B. Srujana Yadav, and V. Reddy, "Wireless sensor networks for effective environmental tracking system using IoT and sensors," in *Proc. 2nd Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC)I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC)*, Palladam, India, Aug. 2018, pp. 66–69.

[255] K. Gopavanitha and S. Nagaraju, "A low cost system for real time water quality monitoring and controlling using IoT," in *Proc. Int. Conf. Energy, Commun., Data Anal. Soft Comput. (ICECDS)*, Chennai, India, Aug. 2017, pp. 3227–3229.

[256] N. R. Moparthi, C. Mukesh, and P. V. Sagar, "Water quality monitoring system using IOT," in *Proc. 4th Int. Conf. Adv. Electr., Electron., Inf., Commun. Bio-Inform. (AEEICB)*, Chennai, India, Feb. 2018, pp. 1–5.

[257] S. H. Kim, J. M. Jeong, M. T. Hwang, and C. S. Kang, "Development of an IoT-based atmospheric environment monitoring system," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Jeju, South Korea, Oct. 2017, pp. 861–863.

[258] B. Gonzalez. (Jan. 7, 2019). Internet Speed Requirements for Video Streaming. Lifewire. Accessed: Aug. 9, 2019. [Online]. Available: https://www.lifewire.com/internet-speed-requirements-for-movie-viewing-1847401.

[259] Netflix. *Internet Connection Speed Recommendations*. Accessed: Aug. 9, 2019. [Online]. Available: https://help.netflix.com/en/node/306

[260] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[261] J. Colistra, "The evolving architecture of smart cities," in *Proc. IEEE Int. Smart Cities Conf. (ISC)*, Kansas City, MO, USA, Sep. 2018, pp. 1–8.

[262] H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-Khah, and P. Siano, "Iot-based smart cities: A survey," in *Proc. IEEE 16th Int. Conf. Environ. Elect. Eng. (EEEIC)*, Florence, Italy, Jun. 2016, pp. 1–6.

[263] S. Chen, G. Xiong, J. Xu, S. Han, F.-Y. Wang, and K. Wang, "The smart street lighting system based on NB-IoT," in *Proc. Chin. Autom. Congr. (CAC)*, Xi'an, China, Nov. 2018, pp. 1196–1200.

[264] X. Liu and C. Huo, "Research on remote measurement and control system of piggery environment based on LoRa," in *Proc. Chin. Autom. Congr. (CAC)*, Jinan, China, Oct. 2017, pp. 7016–7019.

[265] Williams Cattle Company. (2018). *Anna Creek Station*. Accessed: Aug. 21, 2019. [Online]. Available: https://www.williamscattlecompany.com.au/anna-creek

[266] Telstra. (2019). *SIM Subscription Management*. Accessed: Aug. 26, 2019. [Online]. Available: https://www.telstra.com.au/business-enterprise/solutions/internet-of-things/platforms-and-services/sim-subscription-management

[267] WAVIoT. *Comparison of LPWAN Technologies*. Accessed: Aug. 14, 2019. [Online]. Available: https://waviot.com/technology/waviot-lpwan-technology-comparison

[268] G. Smithson. *Introduction to Digital Modulation Schemes*. Accessed: Jun. 29, 2018. [Online]. Available: https://pdfs.semanticscholar.org/670b/9419745dad27a7767a40267bd685f82067b1.pdf?_ga=2.238537216.1028105973.1530244400-428288019.1530244400

[269] L. Riche. (2012). *The Performance of High-Order Quadrature Amplitude Modulation Schemes for Broadband Wireless Communication Systems*. Accessed: Jun. 29, 2018. [Online]. Available: https://pdfs.semanticscholar.org/627d/dfebd0804228d7a8dc864247b8650d2f2b91.pdf
[270] T. F. Wong. (Oct. 8, 2000). *Introduction to Spread Spectrum Communications*. Accessed: Feb. 7, 2018. [Online]. Available: http://wireless.ece.ufl.edu/twong/Notes/CDMA/ch2.pdf
[271] B. Reynders and S. Pollin, "Chirp spread spectrum as a modulation technique for long range communication," in *Proc. Symp. Commun. Veh. Technol. (SCVT)*, Mons, Belgium, Nov. 2016, pp. 1–5.
[272] C. Andren, "A comparison of frequency hopping and direct sequence spread spectrum modulation for IEEE 802.11 Applications at 2.4GHz," in *Proc. Harris Semicond.*, Palm Bay, Florida, 1997, pp. 1–8.
[273] L. De Nardis. (2008). *TDMA, FDMA, and CDMA*. Accessed: Jan. 7, 2018. [Online]. Available: http://acts.ing.uniroma1.it/courses/comelet/Slides/20071217_TEL_lecture_2.pdf
[274] K. Witrisal. (May 12, 2010). *Orthogonal Frequency Division Multiplexing (OFDM): Concept and System-Modelling*. Accessed: Feb. 7, 2018. [Online]. Available: https://pdfs.semanticscholar.org/presentation/1f51/84a16735b3dff3045378ed79ce8f3bff69a4.pdf
[275] G. Povey, "Frequency and time division duplex techniques for CDMA cellular radio," in *Proc. IEEE 3rd Int. Symp. Spread Spectr. Techn. Appl. (ISSSTA)*, Oulu, Finland, Dec. 2002, pp. 309–313.
[276] A. A. Bhatji. (Dec. 14, 2004). *TDMA and CDMA in Mobile Communications*. Accessed: Aug. 9, 2019. [Online]. Available: https://fsu.digital.flvc.org/islandora/object/fsu:175931/datastream/PDF/view
[277] N. Vlajic. (2010). Analog transmission of digital data: ASK, FSK, PSK, QAM. Stanford University. Accessed: Sep. 9, 2019. [Online]. Available: https://www.eecs.yorku.ca/course_archive/2010-11/F/3213/CSE3213_07_ShiftKeying_F2010.pdf
[278] R. Berkvens, B. Bellekens, and M. Weyn, "Signal strength indoor localization using a single DASH7 message," in *Proc. Int. Conf. Indoor Positioning Indoor Navigat. (IPIN)*, Sapporo, Japan, Sep. 2017, pp. 1–7.
[279] M. Weyn, G. Ergeerts, L. Wante, C. Vercauteren, and P. Hellinckx, "Survey of the DASH7 alliance protocol for 433 MHz wireless sensor communication," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 12, Dec. 2013, Art. no. 870430.

BEN BUURMAN received the BIT&S degree from Monash University, Churchill, Australia, in 2016, and the M.Comp. degree from Federation University Australia, Churchill, in 2019, where he is currently pursuing the Doctor of Philosophy (Ph.D.) degree, investigating how wireless sensor network (WSN) technology can be used to provide accurate soil moisture measurements over unprecedentedly large areas at a reduced cost.

He developed the world's first Internet of Things (IoT) wastewater monitoring system during his M.Comp. For this achievement, he was awarded the Dean's Award for Best Thesis at the University. His research interests include the Internet of Things (IoT), low-powered wide-area networks (LPWANs), control and telemetry systems, and software engineering. He currently endeavours to apply these interests to agriculture, smart cities, utility management, and environmental conservation. He has been involved in the IT industry, since 2013. In that time, he has worked with a wide variety of organizations, including utility providers, federal government organizations, and not-for-profits. While working for these organizations, he has both led and been involved with research and development for enterprise-scale software systems, web services, high-security databases, and the IoT-based telemetry and control systems.

JOARDER KAMRUZZAMAN (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical and electronic engineering from the Bangladesh University of Engineering and Technology, Dhaka, and the Ph.D. degree in information systems engineering from the Muroran Institute of Technology, Hokkaido, Japan.

He is currently a Professor with the School of Science, Engineering and Information Technology, Federation University Australia. His research interests include distributed computing, the Internet of Things, machine learning, and cybersecurity. He has published over 250 peer-reviewed publications, which include 70 journal articles, over 160 conferences, 11 book chapters, and two edited reference books. He is a recipient of the Best Paper Award in four international conferences: ICICS'15, Singapore; APCC'14, Thailand; IEEE WCNC'10, Sydney, Australia; and in the IEEE-ICNNSP'03, Nanjing, China. His publications are cited 2683 times and have H-index 23, g-index 40, and i-10 index 63. He has received nearly A$2.3m competitive research funding, including prestigious Australian Research Council (ARC) Grant and large Collaborative Research Centre (CRC) Grant, and has successfully supervised 21 Ph.D.'s and eight masters' to completion. He was the founding Program Co-Chair of the First International Symposium on Dependability in Sensor, Cloud, and Big Data Systems and Applications (DependSys), China, in 2015. He has served 32 conferences in leadership capacities, including Program Co-Chair, Publicity Chair, Track Chair, and Session Chairs. Since 2012, he has been an Editor of the *Journal of Network and Computer Applications* (Elsevier), and had served as the Lead Guest of the *Journal Future Generation Computer Systems* (Elsevier) and a Guest Editor of the *Journal of Networks*.

GOUR KARMAKAR (Member, IEEE) received the B.Sc.Eng. degree in computer science and engineering from the Bangladesh University of Engineering and Technology, in 1993, and the master's and Ph.D. degrees in information technology from the Faculty of Information Technology, Monash University, in 1999 and 2003, respectively.

He was a Senior Lecturer at Monash University, Australia. He is currently a Senior Lecturer with the School of Science, Engineering, and Information Technology, Federation University Australia. He has published 137 peer-reviewed research publications, including 27 journal articles, and supervised 13 Ph.D. and three Masters by research students. He received five best paper awards from major international peer-reviewed conferences. His research has been funded by industry and government organizations, including the Australian Research Council (ARC) Linkage Project Grant. His research interests include intelligent systems using the Internet of Things, multimedia signal processing, data analytics, and simulation modeling.

SYED ISLAM (Fellow, IEEE) received the B.Sc. degree in electrical engineering from the Bangladesh University of Engineering and Technology, Bangladesh, in 1979, and the M.Sc. and Ph.D. degrees in electrical power engineering from the King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia, in 1983 and 1988, respectively.

He has been a Visiting Professor with the Shanghai University of Electrical Power, China. He is currently the Dean of the School of Science Engineering and Information Technology, Federation University Australia, Australia. He received the Dean's medallion for research at Curtin University, in 1999. He has published more than 300 technical articles in his area of expertise. His research interests include condition monitoring of transformers, wind energy conversion, and smart power systems. He is a member of the Steering Committee of the Australian Power Institute and a member of the WA EESA Board. He is a Fellow of the Engineers Australia, a Fellow of the IET, and a Chartered Engineer in U.K. He received the IEEE T Burke Haye's Faculty Recognition Award, in 2000. He received the Curtin University Inaugural Award for Research Development, in 2012. He received the Sir John Madsen Medal, in 2011 and 2014, for the Best Electrical Engineering Paper in Australia. He is a Founding Editor of the IEEE TRANSACTION ON SUSTAINABLE ENERGY and an Associate Editor of the *IET Renewable Power Generation*. He was the Guest Editor-in-Chief of the IEEE TRANSACTION ON SUSTAINABLE ENERGY special issue on Variable Power Generation Integration into Grid. He has been a keynote speaker and invited speaker at many international workshops and conferences.