Low Throughput Networks for the IoT: Lessons Learned From Industrial Implementations

George Margelis*, Robert Piechocki*, Dritan Kaleshi*,Paul Thomas†
*Communication Systems and Networks Research Group
MVB, School of Engineering
University of Bristol, UK
†University of Bristol Honorary Research Fellow
george.margelis@bristol.ac.uk

***Abstract*—The emerging Internet of Things (IoT) is getting closer to reality every day, with standards and protocols tailored to specific applications. Although some technologies follow a 'make once, fit all' approach, others are designed for specific applications such as smart-metering where the devices are often stationary with low jitter and throughput requirements. ETSI is already working towards a new standard for such applications, having specified a Specification Group to study what they call Low Throughput Networks (LTN) and propose a communications standard. In the meantime industrial solutions have entered the market such as, among others, Sigfox's and OnRamp Wireless technologies and LoRaWAN. Although this may lead to fragmentation of the IoT, they are worth examining to gain insights from their innovations and approaches to solving problems that are common in IoT technologies, and more specifically, security, energy management and resource constrains.**

This paper examines the wireless technologies of LoRaWan, Sigfox and OnRamp Wireless, the emerging leaders in IoT smart metering applications.These have so far not been studied in any peer-reviewed paper. Furthermore we discuss the suitability of Low Throughput Networks for certain applications and how the above technologies would work in such scenarios.

I. Introduction

The IoT is coming closer to realization with each day, propelled by advancements in embedded systems, wireless communications, sensors design, and machine intelligence. In the IoT, physical objects have virtual representations, they can be controlled remotely and may act as physical access points to internet services[1]. However the homogeneity needed for such a network is still missing, a consequence of lacking a wireless technology that is suitable for all possible application scenarios. Although the Internet was built on specific protocols, we should keep in mind that until the emergence of smart-phones the devices connected to the internet shared a large degree of traits, e.g. they were all stationary, with access to a power source and computational capabilities that allowed them to implement encryption processes that provided an acceptable level of security. Thus, agreeing to a de facto standard was a process that was more about market penetration and public adoption than from designing a communication protocol that was significantly better for a certain application than others.

However in the IoT, we are not afforded the luxury of assuming anything about the connected nodes. The protocol designer cannot predict the resources of all connected devices or of those that will be connected in the future. Thus designing a technology that will service all possible applications and connected hardware is significantly harder and subject to extensive research. Possible ways to implement the aforementioned functionality include implementation of virtualization layers [2], integration platforms [3] and the usage of mobile code and virtual machines[4]. A discussion of these however is out of the scope of this paper.

Until the emergence of such an all-encompassing solution, the industry has focused on creating solutions that cater to specific market segments. Currently the three domains where most research is focused is Vehicle-to-Vehicle communications (V2V), Continuous e-HealthCare and Smart Metering[5][6]. Each of these possess a different set of requirements and therefore necessitate different approaches.

From the aforementioned, Smart Metering is presently closer to mass implementation. Many systems currently in the market use cellular technologies [7] however due to the power requirements of cellular modems and the fact that these modems waste a significant amount of energy continuously listening, they lack the battery life that is deemed acceptable for large scale smart metering networks (that is, a battery life of years or even decades). Thus new wireless technologies have been proposed from emerging market leaders like Sigfox in Europe and OnRamp Wireless in the USA. Furthermore ETSI is currently in the process of specifying a new standard for what they refer to as Low Throughput Networks (LTN).

This paper discusses LTNs and examines the LTN implementations by Sigfox, OnRamp Wireless and the LoRa Alliance. To the best of our knowledge this is the first study of these technologies, which although proprietary, are likely to influence future open standards as both Sigfox and OnRamp Wireless are working closely with ETSI and IEEE respectively.

The structure of the paper is as follows: Section II defines LTNs and discusses their strengths and weaknesses. Section III and IV present the technologies behind OnRamp Wireless' LTN solution and the Sigfox network respectively, the innovations that they introduce and how they differ from older communication protocols. Section V examines LoRaWan and some potential vulnerabilities, and finally in Section VI we offer our conclusions from the analysis.

978-1-5090-0366-2/15/$31.00 ©2015 IEEE

II. Low Throughput Networks

In the past, conventional communication protocols evolved to offer higher data rates with each generation, trying to cater to the needs of human users that were using bandwidth-heavy applications like video streaming or large file downloads. In the IoT though, the senders and receivers of data are machines that, depending on the application, may not require high uplink or downlink speeds, since they communicate sparingly and transmit only a few kBs. Considering the fact that high data rates bring with them large power consumption, with power being a resource highly constrained in IoT devices, we can reach the conclusion that it is worth examining the possibility that for certain applications, lower data rates are not only better, but actually ideal.

Furthermore, IoT networks are expected to be large scale networks, with nodes numbering in the thousands and ranges of many tens of kilometres. While that can be achieved in a variety of ways (mesh networks for example), there is an opportunity here for new wireless protocols that are optimized for large distances and low-data rates. Although one could argue that General Packet Radio Service (GPRS) transmissions could be sufficient for this kind of communications (and indeed certain implementations of smart metering rely on these [8]) they rely on outdated 2G networks that are not optimized specifically for IoT applications. Furthermore, as LTE networks become more widely deployed, cellular providers switch off GSM networks to reduce operating costs [9].

These low data rate and high range networks referred by some as Low Throughput Networks, are designed with some specific characteristics in mind that set them apart from other IoT-type networks based on IEEE 802.15.4 or other similar technologies. More specifically:

- Data transmissions have a range of tens of kilometres (with distances up to 40km where Line Of Sight is available).
- LTN communication protocols should be designed to enhance battery-lifetime as much as possible. For example LTNs can be mono-directional to avoid spending power during listening. Without the ability to listen-before-transmitting, there is no need to use hardware or code to realize back-off algorithms. However, care must be taken to implement advanced signal processing that provides effective protection against interference and possible collisions. Another method of increasing battery-life is by reducing the overhead in each transmitted frame, as fewer bits means shorter transmissions and therefore less power consumption.
- Hardware must also be as power-efficient as possible with a target battery-life of several years, since changing the battery of these devices might be infeasible.
- Finally, since the applications require low throughput and might be tolerant to delays and jitter, requirements in respect to the aforementioned can be more relaxed, especially if that can lead to enhancing the previous points.

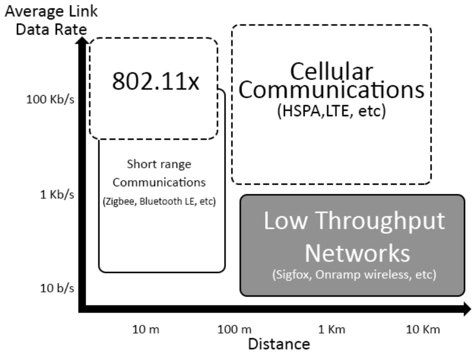

Fig. 1. Although in the past demand led to communication protocols designed for higher data rates,the needs of an IoT system create a new market space, where we are interested in long range and low data rate communications.

In other words, LTNs are suited for applications that require transfers of a few kb over large distances at low speeds in the most power-efficient way possible. Hence they are unsuited for continuous telemetry, or any kind of continuous monitoring and logging, (e.g. patient life signs monitoring or traffic shaping, as has been documented in the past [12]). Furthermore, critical infrastructure applications should be considered carefully, as certain technologies may be more suited than others (for example LTNs without downlink capabilities could pose significant security risks in the long term, since the end-points might use outdated security features that cannot be updated). LTNs are best suited for periodical metering or monitoring applications, e.g. parking management, atmospheric monitoring, water and power metering, self service bike rentals or out-of-area object tracking. Another potential use would be as redundancy to other ways of communication, complementing them by reducing listening time for example, and thus increasing battery time or signalling outages of the primary communication method. They can also be used as an additional source of contextual information for adaptive security systems as the one described in [10].

ETSI has already created a specification group to study and publish a standard for LTNs. In [11], case studies and application suitability are discussed in more detail. Similarly, start-ups have already starting to implement LTNs with proprietary technologies and some of the most promising are the ones offered by OnRamp Wireless, Sigfox and the LoRa Alliance. Furthermore these are currently the only technologies on the market that satisfy all of the aforementioned requirements to be characterized as LTN, and have yet to be examined in any peer-reviewed paper. Although some aspects of these are proprietary, we believe that they are worth studying as both Sigfox and Onramp Wireless are working with standard bodies (Sigfox with ETSI and Onramp Wireless with IEEE) and thus future open standards for LTN can bear similarities with these technologies.

III. OnRamp Wireless

On-Ramp Wireless was founded in 2008 and their network is one of the younger technologies in the field. In September

2015, it was renamed Ingenu. It adopts a star networking topology with access points acting as coordinators of end points. The system favours uplink transmissions (device to network), but also supports downlink features.

The endpoints communicate with the base stations with a proprietary multiple access scheme named Random Phase Multiple Access Direct Sequence Spread Spectrum (RPMA-DSSS) [14] which is their main point of differentiation from their competitors. RPMA is only used for the uplink, while downlink makes use of conventional CDMA.

RPMA, a variation of CDMA, can lead to better Signal to Interference Ratio (SINR) compared to CDMA but also to potential security vulnerabilities. RPMA differs from CDMA in two ways: Firstly, all the nodes make use of the same Gold code to spread the bits before transmitting[14]. Secondly the transmissions are not synchronized, but start with a random delay. This is illustrated in Figure 2.

The transmission slot is divided into $\frac{8192}{2^k}$ subslots, where k is the employed spreading factor. The transmitter then selects a subslot to transmit and adds a random delay to the transmission. As we can see, every transmission in CDMA sees interference from the other transmitters for the whole duration of the transmission. However in RPMA because of the random delay of each transmission the interference seen by any transmitter is less than it would be in CDMA and the low auto-correlation properties of the Gold Codes allow correct decoding of the transmissions as long as two transmissions don't arrive at the exact same moment. We have simulated the behaviour of the system based on patents that OnRamp has been granted [13], [14], and these simulations show that in this way we can have significant better BER performance, as can be seen in Figure 3.

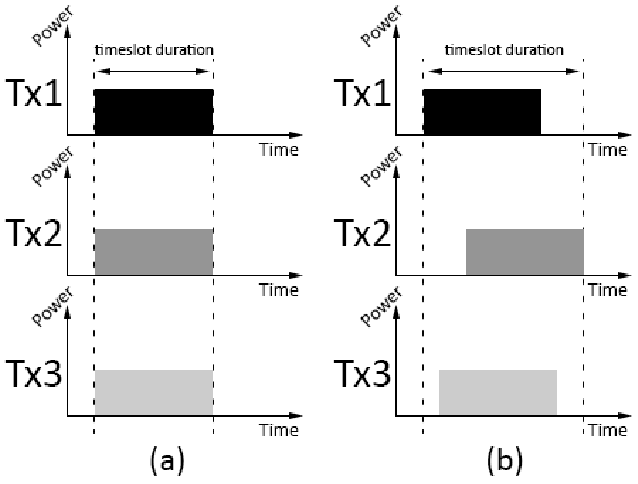

Fig. 2. Comparing CDMA and RPMA transmission strategies. CDMA allows smaller timeslot durations which can lead to better channel utilization, however RPMA can lead to better SINR as there are times where there is no interference from other transmitters.

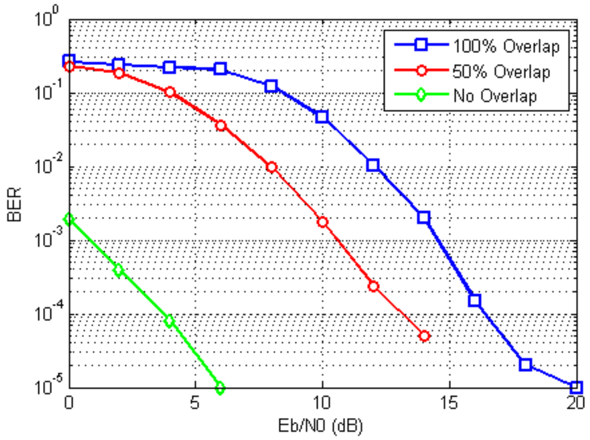

Fig. 3. Comparison of performance of RPMA in a Rayleigh Channel for the case where transmissions overlap completely, where there is 50% overlap and where there is no overlap at all.

The receiver employs brute force at despreading, that is to say it despreads all the received waveforms for all possible arrival times. To reduce the time needed to demodulate through brute force, the receiver incorporates demodulators working in parallel. In effect there is a trade-off here between cost and performance, as the hardware needed for the demodulation in the receiver is increased significantly. However, the receivers have the benefit of being few thanks to their range, and connected to a power source, and thus the price in cost and power consumption associated with the expanded hardware can be easily paid. This is a trend that is common in IoT networks that employ a star network topology, and will be seen later again in section IV. The recovered data are CRC checked, and those that pass the check are forwarded to the MAC layer. As long as no two frames arrive within one chip of another, the frames will demodulate successfully.

The drawback is that, while in CDMA the uplink timeslot can be as short as the time it takes to transmit a frame, in RPMA the timeslot must allow extra time for the time delay of each transmission. As can be seen in Figure 4 our work shows that if the length of the timeslot is such that the transmissions overlap, the performance is comparable with CDMA. Hence by extending the timeslot, although we gain in SINR we lose in data rate. However in an IoT application that can be an acceptable compromise, since the data to be transferred is only a few kb in size.

The fact that all the nodes make use of the same spreading code during uplink may be a security vulnerability. It is not difficult to imagine a scenario where a malicious node joins the network only to get access to the Gold code. With access to the Gold code an attacker could perform a series of passive attacks including eavesdropping or traffic analysis.

During downlink the system employs conventional CDMA where the signals intended for every node are spread first with a different Gold code, then combined and broadcast. The Gold code is generated based on the MAC address of each node, and one of the first tasks a node performs when joining the network is to communicate that MAC address to the base station. Through jamming or powering off, one could force a node to continuously attempt to join the network. An eavesdropper grabbing the setting-up messages could eventually generate the correct gold code to send messages to that node.

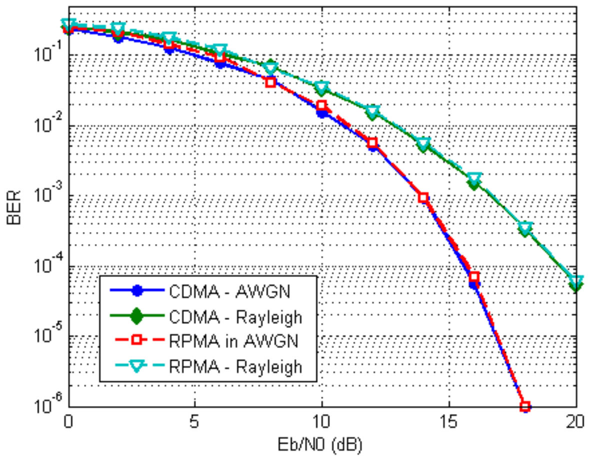

Fig. 4. Comparison of performance of the RPMA and CDMA schemes in conditions where overlapping is close to 100%. We can see that performance is similar.

IV. Sigfox

Sigfox is one of the emerging leaders in LTNs and one of the main contributors of ETSI's efforts to create a relevant standard. Sigfox's approach is a variation of the cellular network that is used by mobile phones, but instead of trying to offer services targeted to humans that require high bandwidth, low jitter and high throughput, tailored to services for devices. Hence, the advantages of the cellular network (long range, ubiquity, easier to set up than managing smaller-range networks) are combined with lower power consumption, and lower cost. Transmissions are Ultra Narrow Band (UNB) with each signal having a bandwidth of 100Hz. Because of the ultra narrow spectral occupation, the noise contribution is very low (around 150 dBm at T = 290 K), thus the system has the ability to successfully demodulate an extremely low received power signal (-142 dBm)[15].

To avoid licensing costs and ensure long range propagation the 868MHz frequency band is used. The spectrum is divided in 400 channels of 100Hz, starting at 868.180MHz for channel 0 and ending at 868.220 MHz for channel 400. Channels 181-219 are reserved and not used. This is visualised in figure 5. However it should be noted that although there is an option to send messages through specific channels (for details, refer to [18]), the transmitters in normal function do not choose from this predefined set. Rather the the carrier frequencies can take any value in the aforementioned allocated spectrum.

Each message is transmitted by default three times [17] although this can be modified. This serves two purposes: Firstly, since downlink transmissions are rare, there is no acknowledgement functionality, and thus retransmissions are a way to ensure that the message will have a better chance of reaching the base station. Hence, we can configure the system to retransmit the message more or less times depending on the importance of the payload. Secondly, each transmission is broadcasted in a different frequency. Thus effects of fading are diminished. In essence Sigfox is employing in this way both time and frequency diversity.

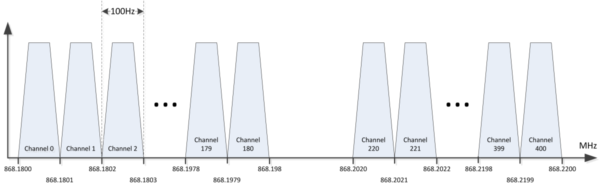

Fig. 5. Channels have a fixed 100 Hz bandwidth, starting at 868.180 MHz for channel 0, ending at 868.198 Mhz for channel 180, restarting at 868.202 MHz for channel 220 and ending at 868.220 MHz for channel 400.

One might wonder how the channel frequency is communicated between end-points and base station. Other protocols rely on a pre-agreed frequency hopping sequence or use a pseudo-random generator with a common seed value and precise timing. However Sigfox does neither. Instead they configure the base station to scan the spectrum listening at every channel and use signal processing algorithms to retrieve the message. The nodes transmit randomly in a frequency that is bounded by the limits of the channels seen in figure 5.In practice, the randomness in frequency domain is easy to implement: each node has its own transmission frequency, defined by the node components (electrical components and oscillator jitter), that varies naturally (depending on different parameters such as temperature and age of the device). The network as a whole has no a priori knowledge of the frequency that the node will use. Thus, factory constraints are relaxed, and the network is not sensitive to temperature variations and other environmental parameters that can affect the carrier. This channel accessing scheme, named Random Frequency Division Multiple Access (R-FDMA), detailed further in [15] leads to cheaper components, an important concern for IoT modems, and solves the problem of the high sensitivity of the system to the transmitter's oscillator's precision. In R-FDMA, there is no channel pre-transmission sensing, which saves energy that would be used to sense the medium.

Sigfox's frame structure is currently not publicly available. However using USRPs we have analysed Sigfox packets and discovered that even though Sigfox does not encrypt the transmitted payload (encryption of the payload is left to the customer, to be done in the application layer), that payload is scrambled. The information needed to unscramble the bits at the receiver is contained in a sync-word that follows the preamble (and is considered by Sigfox actually as part of the preamble). Thus instead of using certain bits as flags to define type of scrambling, payload size etc, they assign certain bit-words to each case. Both the transmitter and the receiver have some association tables stored that are used to translate the bit-word to the necessary information to retrieve the data [16]. This can lead to a reduction of the packet size.

To make this a bit more clear, assume that the sync word that follows the preamble has a length of SW$_{s}$=32 bits. Usually the exact value of these 32 bits is specified beforehand and remains standard. Furthermore let's assume that there are 4 different ways to scramble the payload, requiring SC$_{x}$2 bits to denote those 4 ways. We require PL$_{s}$2 more bits to denote the payload size. Let us also assume that information about the version of the protocol used is also contained within each frame (as some of Sigfox's patents mention).To future-proof the system, we suppose that there is provision for 4 protocol versions, that would need another PV$_{s}$2 bits to be represented. We would then need:

$$SW_s + SC_x + PL_s + PV_s = 32 + 2 + 2 + 2 = 38\ bits$$

The above 38 bits can be used to denote a maximum of 2^{38} different states, but because the sync word is constant, they end up representing only 64 combinations of payload size, scrambling pattern and protocol version. However we can incorporate SC$_{x}$, PL$_{s}$ and PV$_{s}$ in SW$_{s}$. That leads to 64 different sync words that can be made to be prefix-free codewords, and thus easily identified in the base-station. This way, we only need $SW_s = 32$ bits.

Thus we achieve a decrease of 15% of the aforementioned bits in exchange of increased computational complexity to decode the message. However since the base stations have more than enough computational capabilities to handle the task we can easily pay that cost.

The rest of the frame is made up from the payload that can be up to 12 bytes, 4 bytes that express a unique device ID, that is used as a sender address, a 2 byte CRC field and a hash of variable length. The hash is generated from a secret key that each end-point has stored and is used to authenticate (but not encrypt) the payload at the receiver.

Sigfox typically limits the amount of messages that can be send uplink to 6 per hour . Downlink transmissions are supported but for a much shorter range and are not real time, as they happen only after an uplink transmission occurs, to reduce the time the end-points spend listening.

Security wise, Sigfox is mostly interested in guarding against attacks on the integrity of the network, employing sequencing, message scrambling and anti-replay techniques. Security of the payload is left to the customer. It is the customer's responsibility to structure and encrypt the payload, as Sigfox is acting only as a transport channel pushing the data towards the customer's IT system. Hence security can vary and depends strongly on the implementation, and thus can be vulnerable to some attack vectors. Each end-point must be registered on-line to be allowed to use the network. However, the fact that the secret key remains constant, could be a security risk, as an attacker with knowledge of the key could forge messages that would be considered legitimate from the network and forwarded on higher layers.

The limit of uplink transmissions can be exploited by an attacker in a number of ways. For instance an attacker could force a node, by continuous triggering, to send enough messages for the node to be blacklisted, and thus cut it off from the network temporarily. As Sigfox nodes can act as gateways for LANs to connect to the Sigfox network [18] blacklisting a node that acts as a gateway could lead to a black-hole or sinkhole attack, or could just cut off the LAN from the Sigfox network altogether. This attack is based not on the technology itself, but rather on the business model applied by Sigfox, and could be mitigated if there was no artificial limit to the number of uplink transmissions.

V. LoRaWAN

LoRaWAN is a Low Power Wide Area Network (LPWAN) specification intended for IoT-type devices in regional, national or global network. It is frequency agnostic, being able to be applied in 433, 868 or 915 MHz ISM bands depending on the region it is being deployed. In Europe, it employs either GFSK or the proprietary LoRa modulation scheme, which employs a version of Chirp Spread Spectrum (CSS) with a channel bandwidth of 125KHz. The payload can range from 2 to 255 bytes.

The network follows a hierarchical star based topology, with devices being either end-points, gateways or the network server. Data rates can range from 0.3Kbps up to 50Kbps when channel aggregation is employed. The end-points are further divided in 3 types: Devices where downlink occurs only after an uplink transmission, devices where downlink occurs in scheduled time slots and devices that continuously listen for downlink transmissions. Power consumption is proportional to the time devices spend listening, and therefore the correct configuration of an end-point depends of the longevity expectations of the device as well as expectations for real-time downlink capabilities.

Activation of the devices can happen in two ways:

- Over-The-Air: The end-point device sends a join request containing an address that identifies the owner of the device, and an address that identifies uniquely the end-point. It also includes a nonce which is used to generate a Network Session Key and an Application Session key, with which the end-point will encrypt messages after it joins the network. The base station responds with a join accept message that contains an end-device address, another nonce, a network identifier and the channels that the end-point can use.
- Activation by Personalization: The end-device already contains the necessary information to join the LoRa network, including the Network and Application Session Keys and so the process of join request-join accept messages is bypassed.

The above processes contain potential vulnerabilities. For example the nonce used in the Over-The-Air method can, according to the specification [19], *"... be extracted by using a sequence of RSSI measurements"*. Although that can be random, it will not be uniformly random and thus degrades the encryption outcome. To make matters worse, if an end-device becomes stationary for a sufficient amount of time, the seed pool becomes even smaller. Furthermore, if the channel can be modelled as Rician, the RSSI measurements will deviate slowly, again impacting the seed pool. It should also be noted that the join request is not encrypted in any way, and thus a potential eavesdropper could gain information about the topology of the network.

In activation by personalization, the creation of the Network and Application keys is not detailed in any way, which could lead to lacking security depending on the robustness of the implementations. Last but not least, the downlink frames do not contain a CRC of the payload, and can be vulnerable to integrity attacks.

VI. Conclusions

In this paper we have discussed the emergence of a new type of wireless networks, whose range extends to tens of kilometres, their nodes have a battery life of several years and are meant to communicate small packets of data when the requirements for jitter, delay and throughput are more relaxed. Although these networks are not suitable for applications where constant communication is required, or for any kind of application where the aforementioned factors have strict requirements, they are suited for scenarios similar to smart-metering, or as redundancy for other more complex systems. Although efforts to create an open standard for these kind of networks are on-going, the actual implementations so far rely mostly on proprietary technologies that have not been studied or reviewed previously.

This paper is the first to examine the novel channel accessing scheme patented by OnRamp Wireless, Random Phase Multiple Access. Our simulations, based on the patents that OnRamp has been granted, show that performance is similar to traditional CDMA when comparable spreading factors are employed. However, the trade-off between data-rates and SINR that was discussed in section III can be optimized per application case to provide tangible benefits. Furthermore the asynchronicity inherent in the system can act as an extra security measure, although a determined attacker could implement similar parallel demodulators in FPGAs. Finally it can also increase battery life since strict timing is not necessary.

Furthermore we assessed Sigfox's technology, and examined their approach to typical IoT challenges, with R-FDMA helping reduce the overall component costs, and the incorporation of flag-bits in the sync word that can reduce the length of frames. These lead to a more battery-efficient and cheap technology, both important characteristics for IoT wireless technologies.

Last, we introduce the LoRa network protocol and present potential vulnerabilities in the activation process of the endpoints as well as others that stem from the lack of a CRC field in downlink frames.

LoRaWAN, RPMA and Sigfox's technologies are partially closed technologies and thus hard to examine, however we believe our work can act as a starting point for further in-depth analysis. Moreover through our analysis we gain insights about how they tackle IoT challenges that when implemented in the design of open standards can lead to solutions that bolster IoT deployment and adoption.

Acknowledgment

This work was supported by the Engineering and Physical Sciences Research Council [EP/I028153/1] and the University of Bristol.

References

[1] F. Mattern and C. Floerkemeier, *From the Internet of Computers to the Internet of Things*, in *From Active Data Management to Event-Based Systems and More*, vol. 6462, K. Sachs, I. Petrov, and P. Guerrero, Eds. Springer, 2010, pp. 242-259.

[2] A. De Gante, M. Aslan, and A. Matrawy, *Smart wireless sensor network management based on software-defined networking*, in 2014 27th Biennial Symposium on Communications (QBSC), 2014, pp. 7175.

[3] A. J. Jara, M. A. Zamora-Izquierdo, and A. F. Skarmeta, *Interconnection Framework for mHealth and Remote Monitoring Based on the Internet of Things,* IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, pp. 4765, Sep. 2013.

[4] C.-L. Fok, G. Roman, and C. Lu, *Mobile agent middleware for sensor networks: an application case study*, in Fourth International Symposium on Information Processing in Sensor Networks, 2005. IPSN 2005, 2005, pp. 382387.

[5] J. Stankovic, *Research Directions for the Internet of Things*, IEEE Internet Things J., vol. 1, no. 1, pp. 3-9, Feb. 2014.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, *Internet of Things (IoT): A vision, architectural elements, and future directions*, Future Generation Computer Systems, vol. 29, no. 7, pp. 16451660, Sep. 2013.

[7] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, *Smart Grid Technologies: Communication Technologies and Standards*, IEEE Transactions on Industrial Informatics, vol. 7, no. 4, pp. 529539, Nov. 2011.

[8] Telefnica Innovation Hub, *Telefnica set to enable UK smart meter services*, [Online], Available: http://blog.digital.telefonica.com/?press-release=telefonica-uk-smart-meter-programme Accessed: 26-May-2015

[9] M. Wright, *Its time to say goodbye old friend, Telstra Exchange,* [Online], Available: https://exchange.telstra.com.au/2014/07/23/its-time-to-say-goodbye-old-friend/ Accessed: 26-May-2015

[10] J. L. H. Ramos, J. B. Bernabe, and A. F. Skarmeta, *Managing Context Information for Adaptive Security in IoT Environments*, in 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2015, pp. 676681.

[11] ETSI, *GS LTN 003:Low Throughput Networks (LTN)- Protocols and Interfaces* , [Online], Available: http://www.etsi.org Accessed: 05-May-2015.

[12] Jara, Antonio J., et al. *"Evaluation of Bluetooth Low Energy Capabilities for Tele-mobile Monitoring in Home-care."* J. UCS 19.9 1219-1241. 2013

[13] T. Myers, *Random Phase Multiple Access Communication Interface System And Method*, U.S. Patent 7,782,926 B2, August 24 2010.

[14] T. J. Myers, D. T. Werner, K. C. Sinsuan, J. R. Wilson, S. L. Reuland, P. M. Singler, and M. J. Huovila, *Light monitoring system using a random phase multiple access system*, U.S. Patent 8,477,830, July 02 2013.

[15] Do, Minh-Tien and Goursaud, Claire and Gorce, Jean-Marie, *Interference Modelling and Analysis of Random FDMA schemes in Ultra Narrowband Networks*, The Tenth Advanced International Conference on Telecommunications, AICT 2014, pp. 132–137.

[16] M. Vertes, C. ARTIGUE, and N. CHALBOS, *Method for transmitting useful information between two terminals and method for generating an association table used in the context of the transmission*, WO2014053769 A3, 03-Jul-2014.

[17] Sigfox, *Sigfox - One network a billion dreams*, Whitepaper.

[18] Telecom Design *TD1208 Reference Manual*, 2015 pp 38-41.

[19] N. Sornin (Semtech), M. Luis (Semtech), T. Eirich (IBM), T. Kramp (IBM)and O.Hersent (Actility) *LoRaWAN Specification V1.0*, January 2015