A Survey on Low Power Network Protocols for the Internet of Things and Wireless Sensor Networks

Peter Barker
Dr Mohammad Hammoudeh
peter.barker@stu.mmc.ac.uk
m.hammoudeh@mmu.ac.uk
Manchester Metropolitan University

ABSTRACT

Low power communication is becoming an increasingly critical factor in the design and implementation of large-scale Internet of Things (IoT) and Wireless Sensor Networks (WSN). Recently, new protocols have been introduced to help reduce such system's power can cost. This paper presents a survey of recent research on low power consumption networking for IoT and WSN systems, highlighting the move from battery life of hours or days to months and years Then the paper flags some Cyber Security vulnerabilities of specific IoT interest as well as identifying key areas for further work.

KEYWORDS

Wi-Fi, Internet of Things, IoT, SigFox LoRaWAN, Bluetooth Low Energy, BLE, Zigbee, Backfi, NFC, Neul, Thread, Battery Life, Z-Wave.

ACM Reference format:
Peter Barker and Dr Mohammad Hammoudeh. 2017. A Survey on Low Power Network Protocols for the Internet of Things and Wireless Sensor Networks. In *Proceedings of International Conference on Future Networks and Distributed Systems (ICFNDS) 2017, Cambridge, UK, July 19–20 2017 (ICFNDS),* 8 pages.

DOI:10.1145/3102304.3102348

1 INTRODUCTION

The very accessible and well written paper "Trends in Internet of Things Platforms" [**?**] paints a picture of a future where there are billions of Internet of Things (IoT) devices, more IoT devices, in fact, than Humans, and also outlines a number of areas where, it is argued, that current technology needs to change to enable that future vision.

For example, as questioned by Andersen [**?**], who wants to be changing IoT device batteries every few days? This issue, he argues, needs a step change from the current standard of Wi-Fi if the potential of IoT is to be fully realized, or putting it very simply, battery life needs to be measured in tens of months not a handful of days.

This survey paper intends to take up the "..some things need to change" challenge set out by Andersen [**?**] and summarize and organize recent research results in the low power consumption area to add understanding to recent work in this field. It should be stressed at this point that the focus of this paper is very much the network connectivity of the IoT sensor nodes at the edge of the network, specifically low power consumption protocols, rather than IoT network protocols elsewhere in the overall IoT architecture. More recently the authors [**?**] build on the theme of the absolute criticality of low power consumption for IoT devices introduced by [**?**] and state very succinctly "..battery is the most precious resource for things at the edge of the network"

The chosen scope of low power network protocols for IoT and WNS covers both papers discussing research relating to new low power protocols as well as innovations to older protocols. Research on older protocols has been included where those papers are intended to boost the low power credentials of that protocol and increase it's applicability for use with IoT sensor nodes.

It is important to note at this point that whilst the major topic for this paper is the power usage of various IoT network protocols, the discussions will also need to cover papers on related topics such as communications range, communication bandwidth and vulnerabilities. As wll be shown, in many cases the nature of a low power consumption design may introduce limitations with respect to these, and other, network protocol attributes.

In order to classify and organise this paper the following high level structure has been adopted for the main body of the paper.

Section 2 Local Area Networks (LAN) - Addressing protocols usually targeted at home automation, or industrial process control, with ranges typically around the 100m range.

Section 3 Wide Area Networks (WAN)- Covering protocols allowing communications over in the 3 to 30 kilometer Range.

ICFNDS, July 19–20 2017, Cambridge, UK

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM. . . $15.00
https://doi.org/10.1145/3102304.3102348

Section 4 Personal Area Networks (PAN)- There is potentially some overlap between LAN and PAN in that many LAN can operate at short ranges. For the purpose of this paper to avoid confusion we will define PAN protocols as having a maximum 1m range and cover them in this section.

Section 5 - Concludes the paper and presents ideas for further work.

Figure 1 provides additional detail about the network protocols covered under each section. It should be noted that there can be some overlap between the terms Wide, Local and Personal in the definitions of WAN, LAN and PAN, but this is the taxonomy that will be used for this paper.

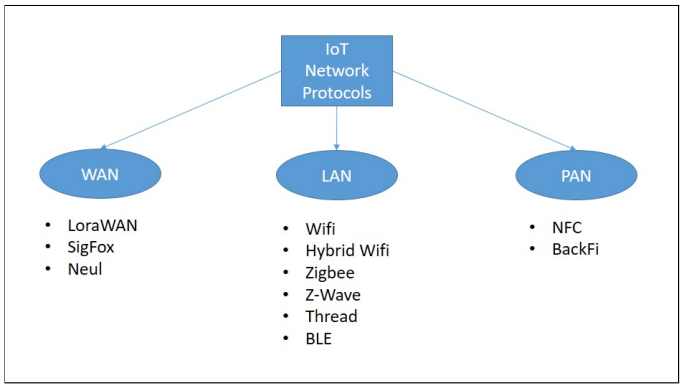

Figure 1: A Taxonomy for IoT sensor node Networks.

2 LOCAL AREA NETWORKS

2.1 Wi-Fi

Although Wi-Fi is one of the oldest technologies reviewed in the survey, with the original IEEE 802.11 standard having first been released in 1997, it will be discussed first in this paper for two reasons.

Firstly, to be able to have a meaningful review of low power consumption technologies and protocols we need to set some context and calibrate what we mean by high and low power consumption.

Secondly, although Wi-Fi in standard guise will be shown to be a power hungry protocol there is ongoing research into Wi-Fi that will be reviewed and summarised which boosts it's low power consumption credentials and makes it more applicable to IoT sensor node applications.

Since the Wi-Fi protocol is the baseline we will use to define a power hungry protocol; to be able to define this in an objective way we need some facts and figures. As articulated by Andersen [**?**] the best Wi-Fi modules typically consume 50mA to receive and 200mA to transmit. So as the research [**?**] shows, a 2xAA battery powered device would have exhausted its batteries within 2 days if all it did was to listen. Andersen [**?**] also suggests a 5-10 year battery life is what is required to make IoT devices commercially viable, so a 2 day battery life with conventional Wi-Fi is clearly way off the mark.

To add further context to the power hungry nature of the Wi-Fi protocol versus other elements of typical IoT sensor node technology the paper [**?**] goes on to compare the power requirements of the Cortex M0+ as found on the Arduino Zero which can sleep at 2uA and would give a theoretical 100 year life with the same 2xAA batteries.

2.2 Zigbee

Zigbee is an IEEE. 802.14.4 based protocol widely viewed as an important technology for the IoT [**?**]. The IEEE 802.15.4-2003 Zigbee specification was ratified on December 14, 2004, making it just slightly older than the generally accepted birth of the IoT in 2005 [**?**]. An early Zigbee paper [**?**], discussed here very briefly just for historical context, shows the industrial adoption of Zigbee and the low power, 2 year battery life. It was exactly these attributes which has made Zigbee very applicable both to it's early industrial context and also the current focus on IoT.

Recent research[**?**] presents a Zigbee implementation, the context being a cardiac unit in a hospital. In this case a one hop architecture rather than the mesh arrangement that is discussed by alternative research [**?**].

In the paper, [**?**] the authors aim to balance the duty cycle of Zigbee versus the need for the Zigbee connected cardiac sensors still to be able to report to base with an acceptable latency and throughput. So in simple terms balancing on one hand patient safety and the other energy efficiency.

Duty cycle is an important concept both for Zigbee and other low power consumption protocols. As we saw previously [**?**] WiFi has two modes, send and receive both of which expend a lot of energy in comparison to the CPU. Zigbee, amongst others, builds in this two state model and introduces a third configurable sleep mode. Increasing the time spent in the sleep mode decreases the duty cycle, saving power, after the reference [**?**].

Perhaps unsurprisingly the conclusions of the cardia unit research [**?**] are that the quality of service, or QoS (as measured by latency and throughput) is better with a high duty cycle but equally power consumption is better (ie lower) with a low duty cycle.

Disappointingly the cardiac unit researchers [**?**] don't make any comment in their conclusions about whether they believe that there is a sweet spot in the results. Such a sweet spot would be important to identify because both QoS and

power consumption are optimised. Also absent is comment about future research in this direction or how a sweet spot, if it exists, might be extended or improved by future work.

Research presented in the form of a demonstration system [**?**] showcases the potential to improve 802.15.4 compliant sensor devices from low power long battery life devices to light powered devices that don't require batteries at all. In this specific case research is focused on a prototype sensor node called Gecko. Gecko is a simple local temperature sensor. The research demonstrated that Gecko could work successfully under typical indoor office lighting. Once scavenged light had sufficiently charged the internal capacitors the Gecko node could send local temperature readings back to a base station. Connection rates up to several times a minute were possible, with the actual connection rate depending on prevailing light levels at the time.

Whilst the work presented by the Gecko researchers [**?**] is an interesting development in the area of IoT renewable energy there is additional work required before such a system could be commercialised, specifically in the areas of:-

Lifespan - capacitors have a finite life in terms of charge cycles, it's not clear from the research to date what the lifespan of the capacitor in the solar Gecko would be and whether it could match the 5-10 year lifetime challenge laid down by Andersen [**?**].

24x7 operation - the Gecko sensor worked on the basis of scavenging data and then sending a temperature reading. It didn't build up reserves of power. Whilst some IoT sensors may, by design, only need to work during daylight or office hours the majority are likely to require 24x7 operation, therefore requiring further development of the Gecko prototype to scavenge and store energy. Stored energy being used, for example, to facilitate 24x7 operation.

In contrast, alternative research [**?**] focuses on the vulnerabilities of low power sensor devices. In this case those present within Zigbee. This research showcases means by which a malicious attacker can inject Zigbee traffic onto the network. Such an injection can force unsuspecting sensor nodes to respond to spurious request and waste power responding. This results initially in battery life reduction from years to days and then post power depletion causes denial of service (DoS) impact. Figure 2 shows several Zigbee nodes arranged in single hop and multi hop configuration, in this case with the rogue node attacking the multi hop leg of the network. Although the work presented by the authors [**?**] is a thorough evaluation of Zigbee, the themes in this paper need to be further explored against the other IoT communications protocols as the attack vector is likely to be very applicable to other low power protocols.

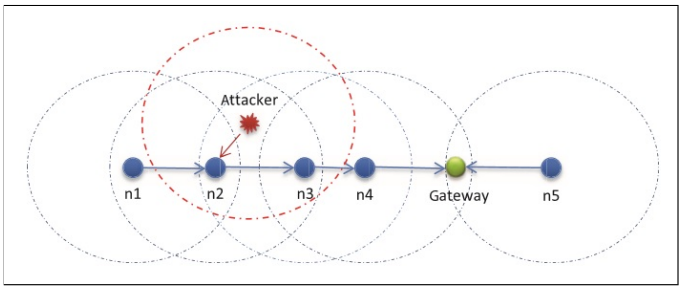

Figure 2: An Example Zigbee Ghost Attack [?]

2.3 Hybrid Zigbee Wifi

A recent research paper [**?**] introduces more innovative research aimed at improving Wi-Fi enabled sensor node life span. This research aims to demonstrate the effect of introducing a sleep state to Wi-Fi. The sleep state being achieved by turning off the communication module when not needed. This allows the duty cycle to be optimised to give the best balance of battery life, latency and throughput. More specifically the authors [**?**] present research relating to a sensor node that novelly runs two network protocols. Firstly, a Zigbee interface to control the sleep and wake pattern, or duty cycle, of the sensor node. Then, secondly, a Wi-Fi interface that actually transmits the sensors data payload.

Results from the research demonstrate an increase in battery life from that of Wi-Fi alone. Power consumption being improved by the ability of the hybrid system to tune the duty cycle balance battery life, throughput and latency. Although this is an interesting concept there is still more work in this area required to address three key areas.

Firstly, the resulting battery life from the hybrid system, whilst being reported as improved from Wi-Fi alone, was still only measured in tens of hours from a typical mobile phone battery capacity, still not sufficient for the majority of IoT applications.

Secondly, the prototype two protocol system inevitably adds cost and complexity over an equivalent single network protocol sensor node. This research hasn't bench marked their results against other single protocol systems, other than Wi-Fi, to see if their results justify this extra cost and complexity.

Finally, although the focus of this paper was to show an improvement in Wi-Fi, which they have achieved, a better comparison for this (or subsequent work) would have been to compare a pure Zigbee network with the hybrid network.

The key unanswered question left by the research is not whether Zigbee can improve Wi-Fi but rather what benefits a hybrid solution may have over pure Zigbee implementation.

2.4 Bluetooth Low Energy (BLE)

According to recent research [**?**] BLE '..is a expected to be incorporated into billions of devices in the next few years'. This is partly because the existing adoption of classic Bluetooth in many everyday devices makes the adoption of BLE more likely. Another key reason for adoption is that BLE has specifically designed with IoT in mind to provide low power short range connectivity.

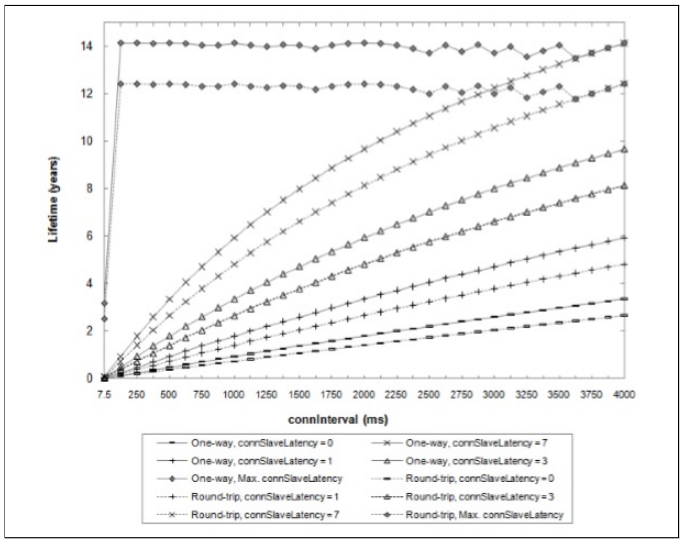

Figure 3: How BLE parameters impact battery life [?]

Research presented by [**?**] and visualised in Figure 3, has projected battery life to be in the range 2 days to 14 years with BLE. The battery life is predominantly controlled by the frequency of communication between the master and slave devices. This communication frequency can be set in a range between 7ms and 32s by means of a pair of parameters that can be configured on the slave and master devices. BLE is a single hop protocol. One master can have up to 5,917 slave nodes. So the pair of parameters essentially allows varying duty cycles across the many nodes potentially attached to a single master.

The architecture of BLE offers both pros and cons over other alternative protocols, dependent on use case in question. This was partially explored in the research [**?**] but more work is required across two broad categories:-

Firstly, for those IoT sensor devices where it makes sense to connect to a smart phone or other BLE enabled mobile device (eg personal fitness sensors). In this category, BLE will be a big improvement.

Secondly, there are use cases where lots of cheap sensors are deployed and it is not practical or desirable to require to link them via an expensive mobile smart device. The work presented in [**?**] is lacking detail for these mobile free use cases. Un-answered questions include how they would be architected, and how these use cases would compare, for example, to a Zigbee implementation in terms of key metrics such as power consumption and cost.

2.5 Thread

Thread is another very new IoT protocol it's supported by a number of heavyweight technology organisations such as Samsung [**?**]. In a similar way to Z-Wave it is a proprietary format and details and specifications are only available to members of threadgroup.org. Their web site claims that the protocol is battery friendly but there is no independent public research to confirm this, or comparative studies to confirm the strengths or weaknesses versus competing protocols. This protocol is mentioned in this survey for completeness and also do draw out that there are many emerging IoT protocols and little in the way comparative research.

2.6 Z-Wave

As noted in by recent research [**?**], Z-Wave is a proprietary protocol marketed by the Z-Wave Alliance, membership of this Alliance prevents open source research, As such there are few research publications concerning Z-Wave or it's low energy credentials.

Z-Wave is primarily used in the home automation market. The authors [**?**] articulate an architecture whereby sensors deployed in a home can be controlled either locally or globally. This is a similar model, at least superficially, to that of Zigbee presented elsewhere in this paper.

The Z-Wave Alliance includes more than 300 companies, therefore it can be assumed that this protocol gives adequate battery life for it's intended home automation purpose. But without public research on this point it can't be stated factually.

One of the few Z-Wave public papers [**?**] presents research on a number of vulnerabilities. These vulnerabilities are focused more around gaining control and access to the network, rather than the energy depletion and DoS attack described in the Zigbee section.

In researching these vulnerabilities, the paper also highlights one issue which is common to all sensor devices with low power reserves. Specifically, that there is a constant battle to balance added features and associated power usage versus battery life. In relation to Z-Wave, the platform supports the AES128 encryption standard, but its use is optional. Vendors may choose to compromise security for better battery life if they assess that the data is not sensitive to warrant the power overhead encryption. This paper [**?**] is an in depth discussion of this specific vulnerability in relation to this single protocol. More work is still required to assess the nature of rogue controllers or gateway attacks on other IoT protocols with similar architectures.

3 WIDE AREA NETWORKS

3.1 LoRaWAN

LoRaWAN is a new protocol its specification v1.0 was released in January 2015 by the Lora Alliance [**?**]. This new protocol has specifically been designed with power utilisation as a key requirement, as early as line two of the specification the Lora Alliance state that LoraWAN is optimized for battery powered end-devices.

Data rates on LoRAWAN can vary from 0.3 kbps to 50 kbps [**?**]. End devices can be configured with a data rate within this range to best balance their transfer needs and power saving requirements. Furthermore research [**?**] confirm the LoraWAN sensor battery life of 10-20 years. This is made possible by two key factors. Firstly, LoRAWAN endpoints being able to receive very weak signals via the network interface card (NIC) and secondly, the LoRaWAN design enforcing duty cycles of less than one percent. The typical LoRaWAN architecture is presented in Figure 4.

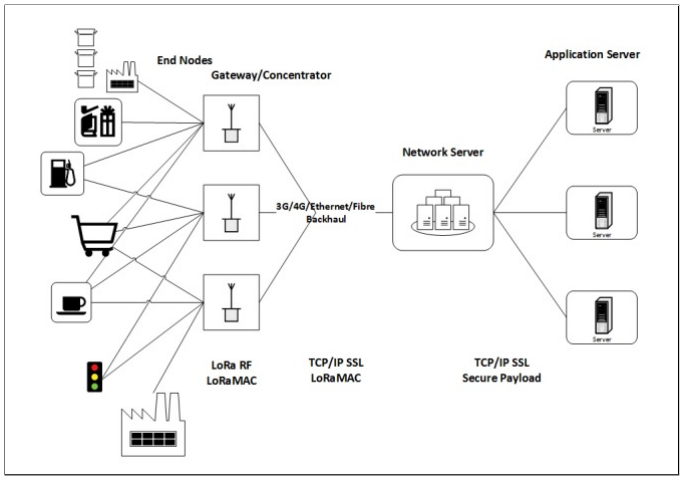

Figure 4: LoraWAN Network Architecture [?]

According recent research [**?**], LoRaWAN, and SigFox, which will be discussed in Section 3.2, differ from the other protocols reviewed in this paper in the key respect that their working range can be measured in tens of Kilometers. As such they are termed low power wide area (LPWA) networks. Such LPWA networks are projected to capture up to 55% of the IoT network market.

Figure 5 shows the 1300 square km coverage achieved experimentally in Ireland and demonstrates the ability of LPWA networks to cover large areas with few base stations. Although work presented in [**?**] is a good general evaluation of the potential of LPWA the researchers do not take the opportunity to evaluate the real world lifespan of LPWA sensor node batteries in the same way that they evaluate both the range and coverage.

Figure 5: Coverage from a single LPWA base Station [?]

	RF Mesh	LoRaWAN
Topology	Mesh	Star
Maximum data rate	10-100 kbps	50kbps
Average Latency	700ms	1s
Maximum Terminals	10,000	15,000
Cost Per Terminal	$0.50	$0.07
IoT Maturity	In Development	In Positioning
Endpoint Mobility	Restricted	Possible

Table 1: LoraWan Vs Mesh network attributes [?]

Additional recent research [**?**] evaluates LoraWAN against an 802.15.4 based grid network of the type used for smart meters in homes. With the key aim of comparing the key attributes of the mesh network against LoRAWAN. Table 1 summarises these key attributes.

Although the paper is generally a good in depth review of many attributes it lacks a comparison of the lifespan of the mesh node against the LoRaWan node. Although both protocols are IoT friendly and offer battery lifespan measured in years the LoRAWAN nodes potentially had a significant advantage in this respect that was not explored.

3.2 SigFox

LPWA Sigfox is a similar technology to LoraWAN, [**?**] As can be seen in Figure 6, Sigfox employs a very similar network architecture. As summarised in Table 2, the key technical difference identified between the two protocols is that Sigfox is primarily a downlink protocol rather than the uplink and downlink design of LoRaWAN. Because there is no provision for acknowledgement messages in SigFox [**?**] each message is transmitted three times at different frequencies.

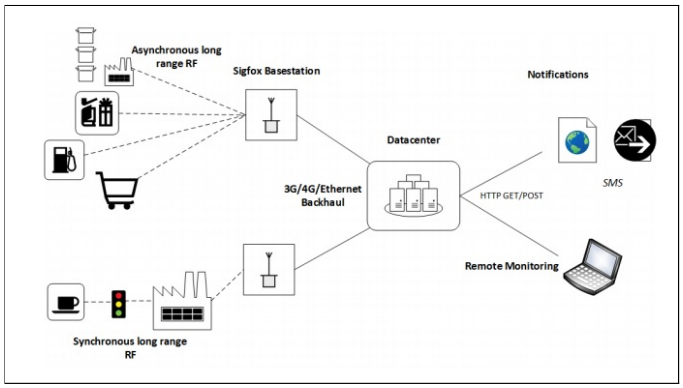

Figure 6: SigFox Network Architecture [?]

LPWA Features	LoRa	SigFox
Symmetrical Technology	Y	Y
Uplink	Data	Data
Downlink	Data +ACK	ACK
Payload Size (bytes)	19-250	12
Protocol Overhead (bytes)	12	26
TX power	13 dBm	14 dBm
TX consumption	28mA	45mA
RX consumption	10.5mA	10mA
AES 128 Encryption	Y	Y
Open Standard	Y	N
Sensitivity dBm	-137	-129

Table 2: SigFox Vs LoraWAN key attributes [?]

As already noted, the work presented by the authors [**?**] is a good introduction to LPWA networks and that research is complemented by additional research [**?**], but both sets of authors miss the opportunity to evaluate the real world, rather than theoretical, battery life for LPWA sensors communicating via either Sigfox or LoRaWAN. They also fail to perform more of a head-to-head comparison of SigFox versus LoRAWAN. For example the 25km range test articulated [**?**] was a SigFox only test.

3.3 Neul

Neul is another IoT WAN technology, included here for completeness. Various articles can be found about its commercial adoption, for example a collaboration between BT and Neul to deploy an IoT network in the UK. No public research materials were found to be available for this survey.

4 PERSONAL AREA NETWORKS

4.1 BackFi

To enhance the low power credentials of Wi-Fi researchers from Stanford [**?**] introduce the concept of BackFi which works in a similar manner to a RFID reader and RFID tag as, for example, you might see a vet using to identify a chipped pet. More specifically, a BackFi IoT device would operate in an environment with existing Wi-Fi by receiving a signal from an wireless Access Point that was intended for another standard Wi-Fi client. Then backscattering the Wi-Fi transmission with its own IoT data modulated on the backscatter signal. To enable this the Stanford researchers work was focused in three key areas.

Firstly, a low power IoT sensor that can detect, modulate and backscatter Wi-Fi signals. Secondly, a novel Wi-Fi access point design that allows receipt of Backscatter signals at the same time as ongoing transmissions. Thirdly, a means to demodulate and decode the backscatter from the IoT sensor whilst also preserving 95% fidelity of the standard WiFi traffic.

With these innovations the Stanford team achieved communications of 5Mbps at a range of 1m and 1Mbps at a range of 5m. Reporting up to three orders of magnitude improvement over prior research cited in their paper, and confirming that the IoT sensor required negligible power.

Although this research showcases interesting developments and the Backfi throughput compares very well to other low power consumption protocols the current level of maturity, and the basic premise, of the backscatter model pose a few challenges that are likely to limit its usefulness.

The range of communication showcased in the paper was 1m to 5m from a Wi-Fi AP. If the IoT sensor is so close to a source of mains power (the AP) then arguably the better solution for the IoT device would be mains power.

Backscatter by it's nature has a reliance on other ambient WiFi traffic - a time critical IoT sensor, say a smoke detector, may suffer delay in delivering sensor data in the absence of WiFi traffic to backscatter.

The power usage stated in this paper could be made more objective, rather than simply stating that negligible power was used. For example a projected lifespan from a typical battery would be more meaningful for the majority of readers.

4.2 Near Field Communications (NFC)

Recent research [**?**] presents a demonstration of an NFC enabled sensor. NFC is the communications protocol that most users are familiar with though use of contact-less card payments. In contrast to typical card payment implementations, this demonstrations [**?**] presents an innovative use of an NFC enabled sensor node. In this specific case a temperature sensor. In operation the sensor node stores temperature readings in non volatile memory until such time as can be harvested by an NFC equipped smart-phone or similar device. In addition to being a novel use of the NFC protocol, the paper also showcases the low power attributes of the NFC protocol by making the sensor node battery-less.

As shown in Figure 7, rather than battery power the sensor node relies on two alternative data sources. Firstly solar power from a built in solar panel and secondly, data scavenged from the NFC harvesting device.

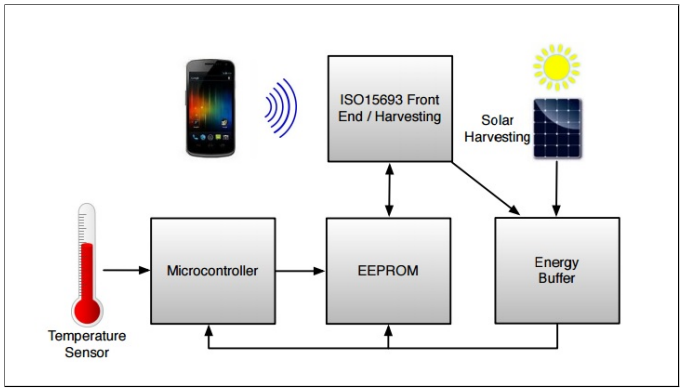

Figure 7: A NFC Enabled Sensor [?]

This NFC enabled sensor with its dual power sources is more flexible than the solar sensor node discussed in the Zigbee section. Further work is required to determine the life span of the energy buffer in this prototype as it cycles through multiple charge and discharge cycles. This prototype clearly has one major drawback that will limit its adoption to many use cases. Which is that, although the sensor can continue to gather data in isolation, it is unable to send it's payload without the visit of a harvesting device.

This design limitation could also be an advantage in some cases because as the research [**?**] states it allows disconnected deployment locations to be considered. This allows some service where always connected networks may be difficult to maintain. For example it would be easy to image use cases as diverse as for instance.

An NFC temperature sensor node at the top of a mountain. Such a sensor would gather data in isolation until harvested, either by a team interested in the data or harvesting could even be crowd-sourced to align with the ethos of many new mobile applications. Or, a covert sensor node, built into an everyday object, or hidden, for example a border security device could gather data secretly until harvested by someone (or something) that knew it's identify and location.

5 CONCLUSIONS

. This survey paper was triggered by Andersen's 'Battery life needs to be measured in months or years' [**?**] statement, specifically in relation to low power consumption network protocols for IoT Sensor nodes. On the basis of this survey in early 2017 it is fair to say that, although only circa 12 months have passed, an accurate response to Anderesn [**?**] would be 'A lot of things are changing'. Particularly across three key topics.

Firstly - With recent networking advances battery life for IoT sensor nodes can now be measured in years rather than days.

Secondly - Surveyed papers include networking solutions that are ready to be implemented now as well as novel research ideas that may be commercialised in due course after further enhancements. Demonstrating a healthy pipeline of research.

Thirdly - Low Power consumption protocols are available across the PAN, LAN and WAN network categories, so there are likely to be a range of options for any given IoT sensor node use-case.

But it is not all good news. The emerging ability to run IoT sensor nodes on tiny power reserves for periods of years presents a number of Cyber Security weaknesses that are of particular concern to IoT sensor networks.

Energy Depletions or, so called, Ghost attacks, causing faster than expected energy drain, and resulting in DoS impact once sensor node power is depleted. Man in the middle attacks are not new, but as we have reviewed in this paper, they may become a real threat to IoT sensors. For IoT sensor design there is a constant battle to maximise battery life on one hand versus, for example, higher data throughput operation or additional security and encryption on the other hand. Where battery life is prioritised over security then the level of risk is clearly increased.

As a final observation, although there are a wide range of new low power protocols there is very little comparative research to help guide the selection process. The proprietary nature of some protocols and the newness of others are clearly significant factors.

6 FUTURE WORK

Several areas are suggested as worthy of further investigation and future work.

Security vulnerabilities. This survey paper highlighted specific vulnerabilities against individual protocols. The vulnerabilities would seem to be very generic in nature and potentially applicable to all IoT nodes, regardless of network protocol used. Of all the protocols surveyed in this paper LoraWAN would appear to be one with the greatest potential for future research work given that. It is a WAN protocol that's expected to account for 55% of the IoT network market, and uniquely amongst the WAN solutions surveyed it is largely open source and open research based. To reinforce this last point a quick search using the term 'LoRaWAN vulnerabilities' in the MMU library does not return any active research in these areas, or indeed any work on LoRaWAN vulnerabilities in general.

Cross Protocol comparative studies. The proprietary nature and speed of development in this area of technology means that there are very few head to head studies. This is particularly true in the area of energy efficiency of competing IoT communications protocols. Given the billions of IoT devices predicted, even small power efficiency gains by using the most energy efficient protocol will save many millions of batteries and give associated environmental benefits.

IoT Management tools. With billions of IoT devices predicted the various IoT protocols and frequencies are going to be servicing lots of traffic with lots of potential for collisions and interference and other unwanted issues. As a result the authors believe that there exists a need for a tool similar in concept to the Wi-Fi Pineapple but an alternative that works with a range of IoT protocols, across the range of frequencies employed, rather than just standard Wi-Fi. The Raspberry Pi IoT platform already has LoRA, Zigbee and BLE network modules available and would make a good choice for some initial proof-of-concept research in this space.

REFERENCES

[1] Andersen, M. Trends in internet of things platforms. *XRDS: Crossroads, The ACM Magazine for Students 22*, 2 (2015), 40–43.

[2] AsiaNews. United states: Samsung and legrand team up to deliver world's first thread-enabled iot light switch, 2016.

[3] Bharadia, D., Joshi, K., Kotaru, M., and Katti, S. Backfi: High throughput wifi backscatter. *ACM SIGCOMM Computer Communication Review 45*, 4 (2015), 283–296.

[4] Cao, X., Shila, D. M., Cheng, Y., Yang, Z., Zhou, Y., and Chen, J. Ghost-in-zigbee: Energy depletion attack on zigbee-based wireless networks. *IEEE Internet of Things Journal 3*, 5 (2016), 816–829.

[5] Filho, H. G. S., Filho, J. P., and Moreli, V. L. The adequacy of lorawan on smart grids: A comparison with rf mesh technology. IEEE, pp. 1–6.

[6] Fuller, J. D., and Ramsey, B. W. Rogue z-wave controllers: A persistent attack channel. 734–741.

[7] Gomez, C., Oller, J., and Paradells, J. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors 12*, 9 (2012), 11734–11753.

[8] Gummeson, J., Zhang, P., Ganesan, D., and Priyantha, N. Demo: Nfc-based sensor data caching. 501–502.

[9] LoRaAlliance. Lorawan specification, v1.0.

[10] Margelis, G., Piechocki, R., Kaleshi, D., and Thomas, P. Low throughput networks for the iot: Lessons learned from industrial implementations. IEEE, pp. 181–186.

[11] Nolan, K. E., Guibene, W., and Kelly, M. Y. An evaluation of low power wide area network technologies for the internet of things. 439–444.

[12] Pathak, S., Kumar, M., Kumar, B., and Mohan, A. Energy optimization of zigbee based wban for patient monitoring. *Procedia Computer Science 70* (2015), 414–420.

[13] Qin, H., and Zhang, W. Zigbee-assisted power saving for more efficient and sustainable ad hoc networks. *IEEE Transactions on Wireless Communications 12*, 12 (2013), 6180–6193.

[14] Shi, W., Cao, J., Zhang, Q., Li, Y., and Xu, L. Edge computing: Vision and challenges. *IEEE Internet of Things Journal 3*, 5 (2016), 637–646.

[15] Yerva, L., Bansal, A., Campbell, B., Dutta, P., and Schmid, T. Demo: An ieee 802.15.4-compatible, battery-free, energy-harvesting sensor node. 389–390.

[16] Zheng, L. Zigbee wireless sensor network in industrial applications. IEEE, pp. 1067–1070.