Analyzing the Vulnerability of Wireless Sensor Networks to a Malicious Matched Protocol Attack

George D. O'Mahony
Dept. of Electrical and Electronic Engineering, University College Cork
Cork, Ireland
george.omahony@umail.ucc.ie

Philip J. Harris
United Technologies Research Center Ireland (UTRC-I)
Cork, Ireland
harrispj@utrc.utc.com

Colin C. Murphy
Dept. of Electrical and Electronic Engineering, University College Cork
Cork, Ireland
colinmurphy@ucc.ie

***Abstract*—Safety critical, Internet of Things (IoT) and space-based applications have recently begun to adopt wireless networks based on commercial off the shelf (COTS) devices and standardized protocols, which inherently establishes the security challenge of malicious intrusions. Malicious intrusions can cause severe consequences if undetected, including, complete denial of services. Particularly, any safety critical application requires all services to operate correctly, as any loss can be detrimental to safety and/or privacy. Therefore, in order for these safety critical services to remain operational and available, any and all intrusions need to be detected and mitigated. Whilst intrusion detection is not a new research area, new vulnerabilities in wireless networks, especially wireless sensor networks (WSNs), can be identified. In this paper, a specific vulnerability of WSNs is explored, termed here the matched protocol attack. This malicious attack uses protocol-specific structures to compromise a network using that protocol. Through attack exploration, this paper provides evidence that traditional spectral techniques are not sufficient to detect an intrusion using this style of attack. Furthermore, a ZigBee cluster head network, which co-exists with ISM band services, consisting of XBee COTS devices is utilized, along with a real time spectrum analyzer, to experimentally evaluate the effect of matched protocol interference on a realistic network model. Results of this evaluation are provided in terms of device errors and spectrum use. This malicious challenge is also examined through Monte-Carlo simulations. A potential detection technique, based on coarse inter-node distance measurements, which can theoretically be used to detect matched protocol interference and localize the origin of the source, is also suggested as a future progression of this work. Insights into how this attack style preys on some of the main security risks of any WSN (interoperability, device limitations and operation in hostile environments) are also provided.**

***Index Terms*—Attack, Co-existence, Detection, Distance, Inter-Node, Interference, Intrusion, IoT, Matched, Mitigation, PHY, Protocol, Security, Space, Spectrum, WSN and ZigBee.**

I. Introduction

As WSNs continue to become integrated in safety critical applications, adding the benefits of wireless technology in the process, new challenges in terms of security vulnerabilities and threat identification emerge. Safety critical WSN applications differ from traditional wireless networks (e.g. WiFi, Bluetooth) because of stricter security and availability requirements. The diverse range of safety critical WSN applications is extensive and includes space-based WSNs [1], the ever expanding IoT, wireless networked control systems (WNCS) [2], aerospace applications [3] and critical infrastructures [4]. Furthermore, Low Earth Orbit (LEO) satellites [5] and Unmanned Aerial Vehicles (UAVs) [6] can both use WSN components and act as components in existing WSN infrastructures. Consequently, network compromise, whether malicious or unintentional, in any of these applications could have significant consequences for privacy and/or safety. Therefore, the requirement for intrusion detection to allow countermeasures to be applied in a timely and accurate manner is of high importance and, significantly, DARPA's Wireless Network Defense project focuses on identifying and mitigating such intrusions [7].

WSNs, which consist of light weight devices used to sense the physical world, have unique security issues due to their design and use. WSN deployments and applications inherently require security levels higher than typical wireless networks, but, the devices in use and their need for interoperability hinder the use of complex or computationally intensive security protocols. Also, any propriety protocol in use can typically be reverse engineered by available tools, therefore, making the security and availability of the communication link essential for safety critical WSNs and requiring intrusion detection in the process. However, intrusion detection has become more difficult due to the expanding use of both the radio frequency (RF) spectrum and WSN applications. This leads to service co-existence issues for each WSN and adds a layer of complexity in the process. Intrusions/interference are the largest contributor to link and path problems in WSNs and resulting packet losses can lead to avalanche effects and potential network collapse [8]. Hence, the nature of WSNs and their expanding applications inherently requires intrusion detection as the first step in fixing a problem (intrusion) is knowing one exists.

This paper uses ZigBee [9] and a cluster head network model to identify and analyze an interference vulnerability in WSNs. The matched protocol attack uses a signal which matches network operation to cause packet loss and denial of service. Here, a ZigBee network of COTS XBee devices is attacked using a ZigBee signal. The XBee devices are used in

This work was supported in part by the Irish Research Council and United Technologies Research Center Ireland under the Enterprise Partnership Scheme Postgraduate scholarship EPSPG/2016/66.

experimental tests to analyze a working ZigBee network under both normal and matched protocol attack conditions. The use of COTS devices and standardized protocols is relevant given the general trend towards the use of COTS components in safety critical applications, for example, space applications favoring high replenishment rates over custom built components [10]. WSNs are highly susceptible to attacks, especially jamming attacks and as WSN operating environments become more diverse and attacking hardware is enhanced and becomes more available, the probability of new attacks being designed and new detection strategies being required increases. This work also shows that traditional spectral techniques require advancements and a more rounded approach to identify certain attacks, for example, the matched protocol attack, is essential.

The remainder of this paper is organized as follows: Section II outlines the adopted network and signal models. Section III describes general security vulnerabilities in WSNs. Section IV describes the general strategy for new attack plans and the matched protocol attack. Section V provides the experimental setup and results. Section VI outlines future developments of this work and Section VII concludes the paper.

II. Network and signal model

Network Model: The chosen network model is based on WSN applications, outlined in Section I, which typically use cluster-based networks as they can improve stability, reduce energy consumption and compress the amount of transmitted data. For example, cluster heads are used as relay nodes (RN) which aggregate data and forward to Nanosatellites [5], which act as the links between clusters. Furthermore, according to studies and predictions by Gartner Inc., outlined in [11], the IoT will likely include 26 billion installed units by 2020. It is likely that the cluster head approach will be adopted in many of these applications due to the advantages it brings to large networks, clearly highlighting the importance of the cluster approach to WSNs. A WSN contains cluster heads (specific node or a sensor node given extra responsibility and designation may be transferred between nodes), which are deployed to collect and analyze data, multiple sensor nodes and a sink. Here, all nodes are static and the cluster head model is achieved using three specific ZigBee node types. The responsibilities of the cluster head are carried out by the $coordinator$ (C) (only one of these nodes is used here), $relay\ nodes$ (RN) relay data generated from neighboring nodes to the coordinator, and the sensing $end\ device$ (E) nodes. The RN reduce the distance between an $end\ device$ and the $corrdinator$ by introducing an additional hop, while also trying to reduce any overloading of nodes.

Signal Model: ZigBee [9], is the chosen signal model as is it based on the IEEE 802.15.4 protocol, currently the de facto standard for WSNs and enables interoperability between different device manufacturers. The versatility and future uses of IEEE 802.15.4 are observed in its use on an In-orbit Demonstration (IoD) of a WSN on the International Space Station (ISS) [10]. ZigBee's relevant physical layer (PHY) parameters and packet structure are shown in Tables I and II, respectively.

TABLE I
IEEE 802.15.4 (ZigBee) PHY Parameters

Parameter:	**2.4 GHz PHY Value:**
Data Rate	250 kb/s
Symbol Rate	62.5 $ksymbols/s$
Chip Rate	2 $Mchips/s$
Chip Modulation	O-QPSK with half sine pulse shaping
Number of Channels	16
Channel Spacing	5 MHz
Channel Width	2 MHz

TABLE II
ZigBee Frame used in Signal Generation

Synchronization Header (SHR)		PHY Header (PHR)	PHY Service Data Unit (PSDU)	
Preamble	SFD	Length	Payload	CRC
4 Bytes	1 Byte	1 Byte	0-125 Bytes	2 Bytes

The 2.4 GHz band was selected and the 16 relevant channel centre frequencies are provided in (1), where the frequency range is $2.405 - 2483.5$ GHz, F_c is the centre frequency and i is the channel number. These frequencies operate in the unlicensed industrial scientific medical (ISM) frequency band and, consequently, coexist with various other protocols, for example, WiFi and Bluetooth. ZigBee uses the PHY and MAC layers from the IEEE802.15.4 protocol and adopts ZigBee specific network and application layers. The MAC layer uses carrier sense multiple access with collision avoidance (CSMA-CA) and the PHY layer uses direct sequence spread spectrum (DSSS) and offset quadrature phase shift keying (O-QPSK).

$$F_c = 2405 + 5(i-11)MHz,\ for\ i = 11, 12, ...26 \quad (1)$$

III. WSN Security Vulnerabilities

All WSN applications require security, particularly when the networks are designed for use in hostile environments and/or in military/aerospace/commercial/IoT applications, as WSNs are susceptible to various attacks. Securing WSNs to an appropriate level is more difficult when compared to other wireless/wired networks because WSNs have a number of unavoidable unique security challenges, which are highlighted in [12] and summarized below:

- Open Interface: Protocols are unavoidably known publicly due to the requirement for interoperability between devices and protocols. The wireless channel is open to anyone with suitable equipment, resulting in vulnerabilities to radio jamming, spoofing, eavesdropping etc.
- Device Resources: Typically devices are deployed and left unattended, operate on a constrained energy supply and, for reasons of cost, have low processing power, which all pose significant challenges for security and reliability.
- Hostile Environments: WSNs are regularly deployed without any fixed infrastructure, where it is difficult to have continued surveillance and operate under harsh environmental

conditions [13]. Legitimate nodes are potentially physically susceptible to being captured by attackers. Thus, a high probability exists of node secrets being discovered and/or nodes becoming malicious. Tamper proofing nodes is possible, but may not be appropriate for all types of networks/nodes.

- Topology [13]: The network topology constantly changes due to changes in the environment (e.g. people, weather, objects), the natural dynamic nature of WSNs, damage, or "death" of some network nodes.
- Hardware Availability: As hardware becomes increasingly available at more cost effective prices, potential attackers can prepare and develop attacks using real-world WSN hardware, which provides an increased chance of attacker success.

IV. Attack Approach

In terms of design and application, attackers are generally more agile, timely and less constrained (in terms of obeying protocols and laws) when compared to their industrial counterparts. This allows attackers to focus on creating only what they truly need and disregard all laws and rules relating to the use of hardware, RF spectrum etc. In terms of WSNs, attackers can take advantage of the security issues described in Section III to develop new or modified attack plans. The general attack strategy is provided in Fig. 1 [14], where the time-line is only a few weeks and the cost of attack relates to (2). Scalability refers to how deployable a specific attack is and the takeaway quantifies the gain achieved by using the attack. This approach, the availability of hardware and the extensive set of potential techniques means attack styles are hard to predict and have relatively short development time-lines.

This work focuses on the matched protocol attack, which uses the attack plan shown in Fig. 2, where the identifier may not necessarily need to identify the exact protocol in use but recognize enough to match the spectral identity and cause packet collisions. This learning based attack determines the signal and frame structures based on monitoring the spectrum and frequencies in use and eavesdropping on transmitted packets, e.g. a 2 MHz bandwidth at specific frequencies near $2.4GHz$ highlights the use of the IEEE802.15.4 protocol and the operating channel is determined using (1). Packet eavesdropping, received power levels and moving around a specific area where nodes are suspected to be located (higher power levels are expected in areas enclosing network nodes) can identify network operation. All of the acquired information is used in the attack plan and a specific matched protocol attack is implemented. The attack causes collisions by introducing interference which mimics legitimate network signals and the resulting packet loss can cause an avalanche of problems which effect all levels of the communication stack [8]. For example, extra traffic introduced by retransmissions and attack packets, can lead to link prediction fluctuations, path changes in routing protocols, applications buffering too many packets and certain nodes becoming unreachable, leading to, in extreme circumstances, a complete collapse of the network [8].

$$Attack\ Value = Scalability * Takeaway \quad (2)$$

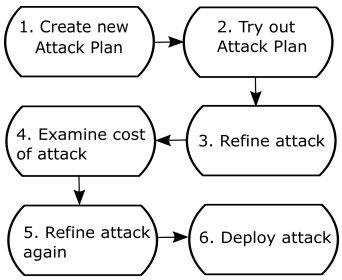


Fig. 1. Flowchart depicting a general attack creation strategy

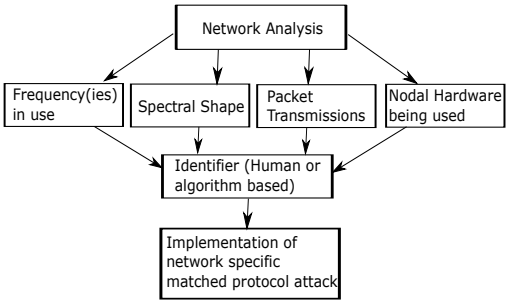


Fig. 2. Attack plan for the matched protocol attack.

V. Matched Protocol Attack Analysis

A. Experimental Setup and Results

The vulnerability of WSNs to the matched protocol attack was experimentally tested using a ZigBee cluster head network of XBee COTS devices. The nodes were configured using DIGI's XCTU software, to form a network with one coordinator and four receiving nodes (ZigBee Routers), as shown in Fig. 3, which also supplies a snapshot of the hardware used. This self-organizing network operates a dynamic topology which brings resilience to natural faults as well as vulnerabilities to malicious attacks. The nodes were powered and controlled remotely using Raspberry Pi 2 and 3 devices utilizing the digi-xbee python library and dispersed sufficiently to provide a realistic deployment scenario. Each node records each of its transmitted packets in a $.txt$ file and the coordinator records and analyzes all received packets in a $.txt$ file in terms of received data, 64 bit source address and packet time-stamp. A programmable software defined radio (SDR), which can adapt to different protocols, was used as the attacking node to transmit ZigBee signals with either pseudo-random data or code words. A Tektronix real time spectrum analyzer (RTSA), using a ZigBee stubby antenna, monitored both the RF spectrum and the transmitted packets and allowed the effectiveness of the matched protocol attack to be verified. Both legitimate packets and attack packets were monitored using the Tektronix RTSA, visualized through the Tektronix Digital Phosphor technology (DPX) and are shown in Fig. 5(a) and Fig. 5(b) respectively. These spectral images are both OQPSK signals with an $\approx 2\ MHz$ bandwidth at $2.465\ GHz$ and have similar power levels, which demonstrates the difficultly in detecting

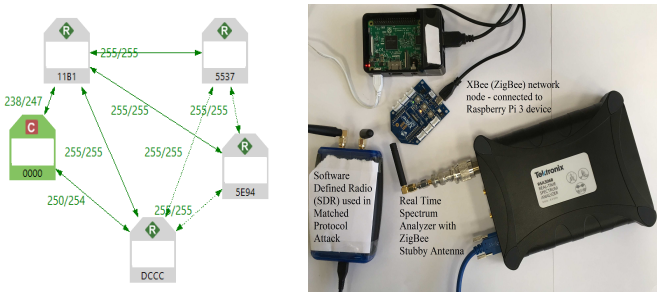


Fig. 3. XCTU produced network configuration, showing the coordinator and receiving nodes, which can talk directly to the coordinator or route through neighboring nodes. A snapshot of the actual hardware shows the real devices used.

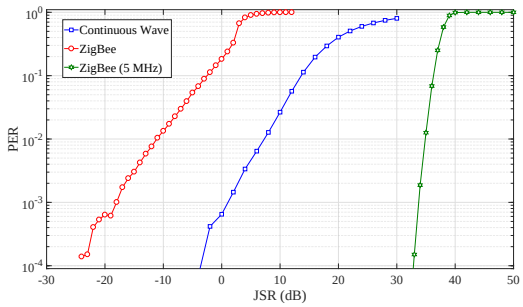
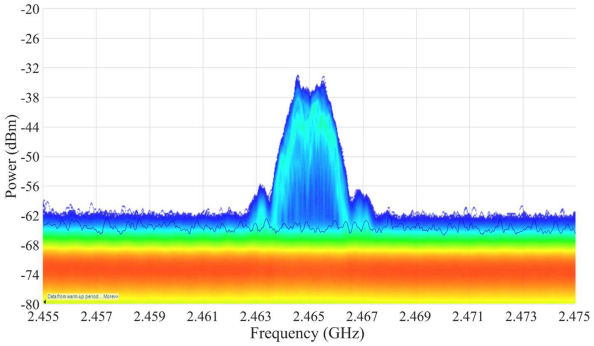


Fig. 4. Simulated PER for a ZigBee signal under both a matched protocol and CW attack using a matched filter receiver. An attack on an adjacent channel shows ZigBee's resilience to cross channel interference.

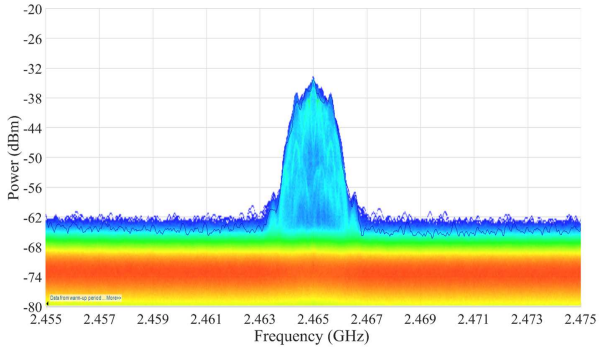
the matched protocol attack using traditional spectral methods, without causing undesirable false positives. Therefore, packets being lost and network services becoming unavailable cannot be directly associated with an attacker because the signals all appear to match normal network operations.

Theoretically, the attack focuses on creating packet collisions, resulting in packet loss and node links collapsing causing nodes to become unreachable. Through network monitoring, attack packets can be transmitted when legitimate packets are expected, causing the packets to collide and increasing the probability of errors occurring and packets being lost or being so erroneous that retransmissions are necessary. The PER shown in (3) (N_{Bytes} denotes the number of bytes in the packet), shows that increasing the probability of error, P_e, increases the PER. Each consequential retransmission is costly and can have an avalanche effect in the network, leading to routing changes, links being unusable and certain nodes being unreachable. Clearly, this approach targets exposed security holes, as explained in Section III, to affect packets in the channel and to deny network services. Through publicly available protocols, signals and packets can be matched by the attack and are difficult to detect due to a lack of complex security algorithms and techniques in use. Additionally, suitable hardware is available at low cost and the applications which use WSN are attractive to potential attackers as they have a large takeaway, if successful, thus giving rise to a positive attack value using (2).

To provide initial evidence, Monte-Carlo simulations, based on a simple matched filter receiver, (Fig. 4) were executed for both matched protocol interference and continuous wave (CW) interference. The PER was calculated for a number of jammer-signal-noise ratios (JSR) for a matched protocol attack on the channel in use (ZigBee), on an adjacent channel (ZigBee-5 MHz) and for a CW attack on the channel in use (Continuous Wave). Fig. 4 shows the susceptibility of WSNs to a matched protocol attack, even at low JSR, while adjacent channels only have an effect at extremely high JSR. Additionally, Fig. 4 provides evidence that this intelligent attack is more effective compared to brute force jamming attacks like, CW. Interestingly, the use of cyclic redundancy codes in the ZigBee packet, Table II, would only identify errors



(a) Legitimate Packet



(b) Attack Packet

Fig. 5. DPX images showing both (a) a legitimately transmitted packet and (b) an attack packet on ZigBee channel no. 23 (2465 MHz)

and require retransmissions, leading to a successful attack.

$$Packet\ Error\ Rate\ (PER) = 1 - (1 - P_e)^{2 * N_{Bytes}} \quad (3)$$

To verify the above, a real WSN, based on XBee nodes, was set up and run under normal conditions and attack conditions. The Tektronix RTSA identified the channel in use, the spectral image of the legitimate signals/packets and the packet transmission period (approx. every 60s). In this testbed, which uses simple python code and XBee devices, a successful attack requires the coordinator to become unreachable by the individual nodes and in this case, using the digi-xbee library, an "Address Not Found" error occurs causing the python code

TABLE III
EXPERIMENTAL RESULTS: NORMAL OPERATION

Normal Operation	Test 1	Test 2	Test 3	Test 4	Test 5	Test 6
Test Length (Hours):	≈ 17	≈ 17	≈ 17	≈ 17	≈ 17	≈ 26
Total Packets Sent:	4100	4170	4084	4084	4135	6308
Packets Lost:	0	0	0	0	0	0

to throw an exception and fail. To validate this approach the testbed was tested under normal conditions for 6 distinctive periods as per Table III. The results in Table III show that the network ran without error during the 6 separate tests, in which over $26,500$ packets were transmitted, therefore, validating the code and setup. During the attacking tests, the attacking SDR ignored the CSMA/CA protocol in use and constantly injected packets into the channel at specific times and effectively became a learning based jammer with the spectral image of legitimate packets. This resulted in packet collisions and the coordinator (identified from network monitoring) becoming unreachable by network nodes. This caused each network node to throw an exception, resulting in code failure and a denial of network services. This error only occurred when the SDR attacker was present and caused the nodes to fail when trying to transmit a packet. These experiments demonstrated WSNs vulnerability to matched protocol interference, as the network was jammed with indistinguishable signals.

VI. FUTURE WORK

Future progressions of this work includes the analysis of inter-node distances, packet security measures and packet manipulation. Inter-node distances, denoted D_{a-b}, have potential in terms of attack detection and Ultra Wide-band devices are key for this concept to work as accurate distance measurements can be achieved. Furthermore, this concept can be developed to include the identification of channel properties due to the existence of a unique channel between two distinct static nodes. Therefore, these unique properties would be difficult for an attacker to replicate and so a detection strategy for matched protocol interference could emerge. The work can be expanded by delving into indoor positioning and WSN localization techniques. The analysis of security techniques used in WSN protocols and packets, and especially why they are used, will provide insights into how to improve WSN protocols in terms of security and design methodologies and allow for the best detection algorithm deployments. Finally, an interesting future development is to explore whether the matched protocol attack (and/or other attack techniques) can cause packet manipulation or network spoofing.

VII. CONCLUSION

This paper described a matched protocol attack and how WSNs are vulnerable to it due to the use of network specific packets and signals. The detection of such an attack requires using information outside of the normal spectral and routing layer techniques. This implies that traditional interference detection schemes might be inadequate, as intruder signals may now be indistinguishable from legitimate signals. Therefore, intrusion detection requires more than monitoring the spectrum or routing layer as the whole WSN process requires attention. This paper clearly highlighted the need for intrusion detection and how WSN security is becoming critical. The attack style was described and experimentally tested and simulated and general WSN security vulnerabilities were identified. Therefore, a methodology is now required which designs protocols with attackers in mind, leading to the entire protocol stack and hardware used being designed to detect and mitigate attacks.

ACKNOWLEDGMENT

The authors would like to thank both Dr. James T. Curran for his contribution in developing the signal model and Monte-Carlo simulations and Dr. Kevin McCarthy for his guidance and insight with respect to the experimental set up.

REFERENCES

[1] T. Vladimirova, C. P. Bridges, J. R. Paul, S. A. Malik, and M. N. Sweeting, "Space-based wireless sensor networks: Design issues," *IEEE Aerospace Conference*, pp. 1–14, 2010.

[2] P. Park, S. C. Ergen, C. Fischione, C. Lu, and K. H. Johansson, "Wireless Network Design for Control Systems: A Survey," *IEEE Communiations Surveys and Tutorials*, vol. 20, no. 2, pp. 978–1013, 2018.

[3] R. K. Yedavalli and R. K. Belapurkar, "Application of wireless sensor networks to aircraft control and health management systems," *Journal of Control Theory and Applications*, vol. 9, no. 1, pp. 28–33, 2011.

[4] L. Buttyán, D. Gessner, A. Hessler, and P. Langendoerfer, "Application of wireless sensor networks in critical infrastructure protection: challenges and design options [Security and Privacy in Emerging Wireless Networks]," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 44–49, 2010.

[5] A. Addaim, A. Kherras, and Z. Guennoun, "Design of WSN with Relay Nodes Connected Directly with a LEO Nanosatellite," *International Journal of Computer and Communication Engineering*, vol. 3, no. 5, pp. 310–316, 2014.

[6] M. A. M. Marinho, E. P. De Freitas, J. P. C. Lustosa Da Costa, A. L. F. De Almeida, and R. T. De Sousa, "Using cooperative MIMO techniques and UAV relay networks to support connectivity in sparse Wireless Sensor Networks," *International Conference on Computing, Management and Telecommunications, ComManTel*, pp. 49–54, 2013.

[7] T. Woodward, "DARPA - Wireless Network Defense." [Online]. Available: https://www.darpa.mil/program/wireless-network-defense

[8] A. Förster, *Introduction to wireless sensor networks*, 2016.

[9] ZigBee Alliance, "ZigBee Specification. ZigBee document 053474r20," Tech. Rep., 2012. [Online]. Available: http://www.zigbee.org/

[10] H. J. Beestermöller, J. Sebald, M. C. Sinnreich, H. J. Borchers, M. Schneider, H. Luttmann, and V. Schmid, "Wireless-Sensor Networks in Space Technology Demonstration on ISS," in *Dresdner Sensor-Symposium*, 2015, pp. 99–102.

[11] I. Gartner, "C. STAMFORD. (2016) Gartner says by 2020, more than half of major new business processes and systems will incorporate some element of the internet of things." [Online]. Available: https://www.gartner.com/newsroom/id/3185623

[12] Y. Zhou, Y. Fang, and Y. Zhang, "Securing Wireless Sensor Networks: A Survey," *IEEE Communications Surveys*, vol. 10, no. 3, pp. 6–28, 2008.

[13] A. P. Abidoye and I. C. Obagbuwa, "DDoS attacks in WSNs: detection and countermeasures," *IET Wireless Sensor Systems*, vol. 8, no. 2, pp. 52–59, 2018. [Online]. Available: http://digital-library.theiet.org/content/journals/10.1049/iet-wss.2017.0029

[14] G. Bullard, "Securing the Digital EcoSytem – A war we're losing." Public Lecture at: The Future of Security Seminar, Univeristy College Cork, 09th May 2018.