Interference and Intrusion in Wireless Sensor Networks

George D. O'Mahony, *Student Member, IEEE,* James T. Curran, *Member, IEEE,* Philip J. Harris and Colin C. Murphy

***Abstract*—Wireless sensor network (WSN) systems for safety-critical, space and internet of things applications have recently begun to adopt open standards and commercial-off-the-shelf equipment, and persistently face challenges of malicious intrusion and spectrum co-existence. These threats are explored through Monte-Carlo simulation and benchtop testing, including matched protocol interference and sophisticated, interactive intrusion attacks. The need for expanding intrusion detection via a more holistic approach, whilst simultaneously improving WSN security, is illustrated. Discussions on WSN security, vulnerabilities, and attacks are also provided.**

***Index Terms*—Co-existence, Detection, IDS, Interference, Intrusion, IoT, MAC, Mitigation, PHY, RF, Security, Space, Spectrum, Wireless and WSN.**

I. Introduction

The use of wireless sensor networks (WSNs) in safety critical applications, such as space-based WSNs [1] and the Internet of Things (IoT) [2], creates new challenges in terms of security and spectral coexistence. Unlike traditional wireless networks, (e.g. Bluetooth and WiFi,) the use of WSNs in safety critical applications imposes strict security and availability requirements on computationally constrained devices. A diverse range of these safety critical WSN applications exist, where robustness against harsh environments and maintaining low power operation need to be considered. These applications include, amongst others, wireless networked control systems [3], space applications, for example, in-orbit demonstration of an IEEE 802.15.4 protocol based WSN on the International Space Station [4] and space wireless local area networks [5]. Also, due to advances in the development of WSN architectures [6], Low Earth Orbit satellites can be used as WSN components [7] to receive aggregated packets from WSN relay nodes. Additionally, WSNs are being utilized in aerospace applications for aircraft control and health management systems [8] as a first step towards fly-by-wireless and increased monitoring capabilities. These WSNs are extensively used in traditional monitoring and control applications, such as, for example, environmental and surveillance [9]. Uniquely, arrays of nanosatellites are used in a WSN approach to enhance mobile communications through lower-cost, space-based mobile phone services [10]. In modern society, the emerging IoT [2], which leverages WSNs, is leading to the truly connected world and smart homes/businesses. Each of these infrastructures and applications require protection and attack detection, as any attack could have significant consequences for privacy and safety.

Security and availability of the communication link are essential for any safety-critical wireless system. These requirements are vital as WSNs develop into an indispensable component of modern technology. Simultaneously, spectrum coexistence issues emerge, for example, in the Industrial, Scientific and Medical (ISM) $2.4\ GHz$ radio frequency (RF) band. This is mainly due to (often changeable) large number of connected devices potentially running different protocols at the same frequency, location and time. These spectral issues add complexity to providing the necessary security and availability in WSNs, which are typically composed of multiple autonomous, low cost, resource-limited and low power sensor nodes running on a finite energy supply and an open interface protocol for interoperability between devices. Nodes gather data from their environment and often collaborate to transmit the sensed data to a centralized sink, cluster head or relay node. In general, WSNs need to share the frequency spectrum with multiple services and need to coexist with both similar and different protocols. WSNs are self-organizing, self-repairing and operate a dynamic topology, which brings both resilience to natural faults as well as a vulnerability to malicious attacks. Due to their design, application space and spectrum occupancy, a need for intrusion detection and security against both malicious and unintentional

At the time of writing, George O' Mahony and Dr. Colin C. Murphy are with the Department of Electrical and Electronic Engineering, School of Engineering, University College Cork, Cork, Ireland (email: george.omahony@umail.ucc.ie,colinmurphy@ucc.ie). Dr. James T. Curran was with the European Space Agency in Noordwijk, South Holland Province, Netherlands (email: jamestcurran@ieee.org). Dr. Philip J. Harris was with United Technologies Research Center Ireland, Cork, Ireland (email:harrispj@utrc.utc.com).

interference is warranted.

This article uses critical WSN applications as a case study to provide a review of WSN vulnerabilities, security and attacks, including co-existence intrusions. ZigBee is studied through Monte-Carlo simulations and benchtop experiments to highlight WSN security issues and the need for intrusion detection. An intrusion detection system (IDS) is used to identify the presence of intruders. Commercial-off-the-shelf (COTS) devices and standardized protocols are used due to the general trends towards the use of COTS components in commercial IoT networks and in space applications. Both areas, typically, favor high redundancy, high replenishment rates over custom-built components. Examples include the international space station [4], inter-satellite communication modules [1] and nanosatellite swarms [11]. WSNs are commonly deployed in environments where the spectrum changes rapidly due to the number of connected devices, demand, packet size or services in operation and changes in the physical environment due to varying fading levels, obstacles, path losses, and spurious interference. Beyond these non-malicious factors, critical WSN applications may incentivize malicious attackers to intentionally disrupt or compromise network operation. Presently, WSNs are highly susceptible to attacks, especially Denial of Service (DoS) [12] attacks and, as WSN operating environments become more diverse and attack techniques develop, security improvements are required. The challenges of system co-existence add even more complexity and need to be examined, as many modern WSN protocols adopt the same physical (PHY) and/or medium access control (MAC) layers [9]. This phenomenon is explored by investigating the IEEE 802.15.4 PHY and MAC layers, which are utilized by ZigBee and by various WSN protocols.

The remainder of this article is organized as follows: Section II gives a brief description of related work, section III outlines the signal model used as a case study and section IV provides adopted assumptions. Section V summaries security in WSNs, section VI describes various WSN attacks and section VII discusses specific attacks using Monte-Carlo simulations and benchtop tests. Finally, section VIII provides future directions for enhancing WSN IDS design and security and section IX concludes this article.

II. Related Work

Interference and intrusion detection is not a new area in wireless communication systems, but it is an area which requires expansion and enhancements to match the current trend of WSNs. Security for WSNs is the most relevant work which relates to this article and includes investigating applied security techniques [9], threats to WSNs [13], how to secure WSNs [14] and existing security issues in WSN protocols [15]. Additionally, related work includes research into WSN attacks, where [16] provides a brief overview of attacks and detection methods and [17], [18] focus on jamming attacks and associated detection measures only. Flexible and reliable software-defined reactive jamming is shown to be feasible in [19], which provides attack deployment evidence for the previous descriptive studies. Denial of service attacks are outlined in [12], which also states that security is the linchpin of good sensor network design and detection can aide deployments. Research on intrusion detection and IDSs includes using traditional techniques such as analyzing the received signal strength or packet delivery rate [20] and machine learning algorithms developed specifically for detecting intrusions on WSNs [21]. These machine learning techniques use features such as packet collision ratio, delivery waiting time and power consumption rate, to name but a few. Detailed surveys on intrusion detection in WSNs, the main concepts, and the vital areas can be found in [22], [23]. However, this type of research is not confined to WSNs as it is a current research topic across wireless networks, in general, including Global Positioning System signals [24], WiFi signals [25] and the coexistence of wireless systems [26]. This article provides its contribution by summarizing WSN security, vulnerabilities, interference and intrusion attacks and detection methods. In contrast, the literature above, typically, focuses on a specific type of attack and the associated detection process. Hereafter, critical WSN applications and an adopted WSN protocol are used as a case study to provide a review of WSN vulnerabilities, security and attacks, including co-existence intrusion. Notably, this article discusses WSN attacks in terms of both the unlawful transmitter and the non-compliant spectrum user. Whilst existing research focuses on malicious spectral intrusions in terms of jamming attacks, this paper highlights the idea of using coexisting signals as malicious intruders. This paper's contribution is expanded by highlighting the need to focus on WSN jamming for IoT penetration testing and deployment security.

III. Signal Model

Here, the IEEE 802.15.4 based wireless protocol for low rate wireless personal area networks (LR-WPAN), ZigBee, is the chosen signal model, since, currently, it is the de-facto standard for WSNs (as almost all available commercial and research sensor nodes are equipped with ZigBee transceiver chips [27]). The operating topology is either star, mesh or peer-to-peer and, in each case, is

self-organizing, self-repairing, dynamic and can exploit clustering approaches [15]. Cluster heads are, typically, used as relay nodes which aggregate and forward data to a centralized sink. An example is using nanosatellites as relay nodes (cluster head), allowing access to remote areas by using the nanosatellites as links between each cluster and centralized sink [7]. ZigBee is constructed using the PHY and MAC from IEEE 802.15.4 and uses a protocol-specific network layer, application support sublayer and application object layer [28]. Relevant PHY parameters are shown in Table I and three different frequency bands are supported: a 2.4 GHz band (16 channels), a 915 MHz band (10 channels) and an 868 MHz band (1 channel). Here, the 2.4 GHz band is selected and the 16 available 2 MHz wide channels, which range from 2400→2483.5 MHz and have an inter-channel gap of 3 MHz, have center frequencies as per (1), where F_c and i are the center frequency and channel number, respectively.

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

These frequencies are transmitted in the unlicensed ISM frequency band and must coexist with various signals including Bluetooth, numerous LR-WPAN, wireless local area networks and wireless metropolitan area networks. Due to the unlicensed operation, global availability and relatively long-range, the ISM frequency band is the first choice for wireless LAN solutions. To gain access to the wireless channel, ZigBee uses carrier sense multiple access with collision avoidance (CSMA/CA).

Table I
ZIGBEE PHY PARAMETERS

Parameter:	**2.4 GHz PHY Value:**	
Number of Channels	16	
Channel Spacing / Width	5 MHz	2 MHz
Data — Symbol Rate	250 kb/s	62.5 $ksymbols/s$
Chip Rate	2 $Mchips/s$	
Modulation	O-QPSK	
Pulse Shaping	Half Sine/Normal Raised Cosine	
Spreading	DSSS	
Maximum Packet Length	133 bytes	

Table II
ZIGBEE PHY FRAME

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

Prior to transmitting a packet, devices perform a clear channel assessment to ensure the channel is available. This technique is particularly vulnerable to DoS attacks and spectrum-sharing difficulties.

ZigBee uses direct sequence spread spectrum (DSSS) to split each outgoing byte into two 4-bit symbols, four most significant bits and four least significant bits. Each symbol is spread to a 32-bit pseudo-noise sequence from a predefined mapping table. Chip sequences are encoded using offset quadrature phase shift keying (O-QPSK) with half-sine/normal raised cosine pulse shaping. Matlab simulations, using random payload bits, produced the example in-phase and quadrature phase (IQ) data in Fig. 1a and associated IQ diagram, which illustrates the constant envelope nature of the signal, in Fig. 1b. The equivalent energy-per-bit (E_b) can be calculated using the period over which one byte is broadcast (T_{Byte}) and (2), where C is the signal power in Watts.

$$E_b = \frac{T_{Byte} * C}{8} \ J/bit \quad (2)$$

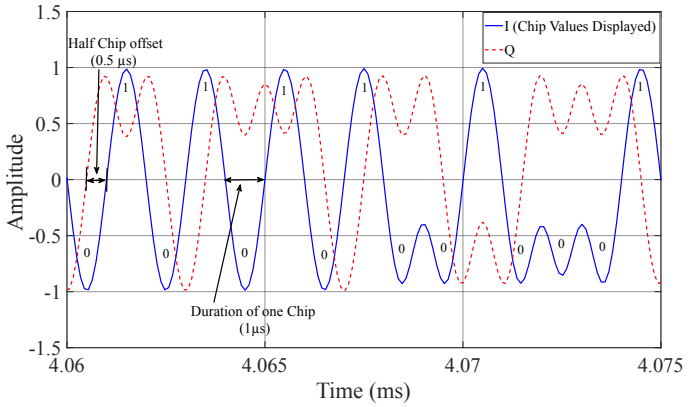
The packet error rate (PER) for a ZigBee signal in a zero mean additive white Gaussian noise (AWGN) channel was calculated to illustrate normal operation (Fig. 2). A range of energy-per-bit-to-noise ratios (E_b/N_0) were applied using a ZigBee frame (Table II) with a randomized payload. The predicted PER was calculated using the probability of receiving an incorrect symbol (P_e), given 16 unique DSSS pseudo-noise codes and an AWGN channel. Assuming a matched filter receiver, the symbol error probability can be expressed as (3), where σ (4) is the variance, $\mathrm{erf}()$ is the error function and L is the number of codes. The corresponding PER is estimated using (5), where N_{Bytes} is the number of bytes per packet.

$$P_e = 1 - \int_{-\infty}^{\infty} \frac{e^{-\frac{(-1+y)^2}{2\sigma^2}}}{\sqrt{2\pi}\sigma} \left(\frac{1}{2} + \frac{1}{2} \mathrm{erf}\left[\frac{y}{\sqrt{2}\sigma} \right] \right)^{L-1} dy \quad (3)$$

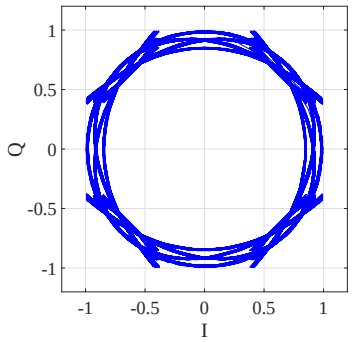
$$\sigma = \sqrt{\frac{1}{2E_b N_o}} \quad (4)$$

$$PER = 1 - (1 - P_e)^{2*N_{Bytes}} \quad (5)$$

The results express the PER for received packets across an AWGN channel for normal operating conditions. However, as will be discussed later, other considerations, including miss-routing of packets, erroneous transmissions or attacks, may occur. The predicted and simulated results begin to differ as the PER reduces because the mathematical model assumes the pseudo-



(a) Simulated ZigBee O-QPSK modulated IQ data, with the IQ chip offset and chip duration labelled



(b) IQ diagram for the transmitted ZigBee signal

Figure 1. Visual representation of transmitted ZigBee signal

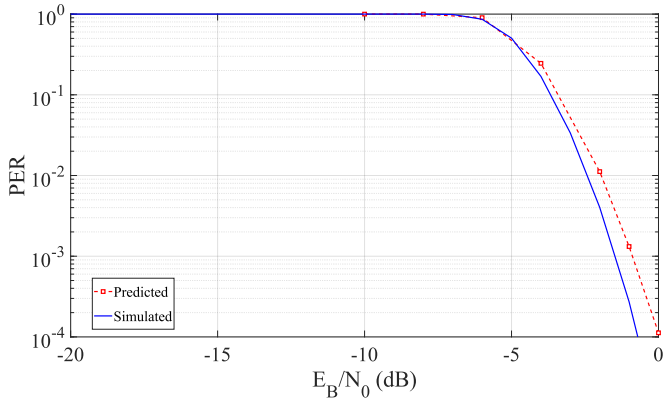


Figure 2. Predicted and simulated PER for a ZigBee signal over a range of energy-per-bit to noise ratios

noise codes are orthogonal but, in reality, there is a non-zero cross correlation.

IV. Operating Assumptions

Based on the literature, certain operating assumptions are made, which focus on IDSs and how wireless networks react to an intrusion. Traditional wireless network operation, typically transmitted packets, and attack methods were examined and the assumptions adopted herein are as follows:

1) A reliable routing protocol is used and a packet can always reach the base station, and other nodes, when no attacks are present [20].
2) Basic jamming hardware in use may be similar to network nodes [20], but notably does not have to adhere to any standards, guidelines or rules.
3) Attackers can use advanced hardware (e.g. software defined radios, computers) without adhering to standards, guidelines or rules. [29]
4) The attacker can place/seize one or more basic sensing nodes in the network [20]. These basic sensing nodes have limited resources and energy supplies, which hinder the use of complex security algorithms. Control nodes contain more advanced hardware and, as a result, are more difficult to seize.
5) Nodes at the edge of a jammed region can receive messages from "jammed" nodes and relay alarms to the controller and/or base station [30].
6) Intelligent jammers can monitor the network and determine the protocols being used [31].
7) Nodes can be deployed in environments where the possibility of being captured exists [16]. Captured (malicious) nodes can be used to implement attacks on the network and can gain access to sensitive data. An example includes a black hole attack [32], which "pulls in" network traffic by listening to route requests and replying that it has the shortest path. The node can, potentially, alter, reject or replay received packets. Section VI discusses other attack strategies for malicious nodes.

Application specific assumptions also exist, for example, encryption and/or a key management system for data privacy may be of high importance in some applications, while other systems might implement origin authentication and data integrity but not encryption. Certain applications may not use any mitigation strategies, while critical applications may use DSSS, frequency hopping spread spectrum or a frame check sequence to fortify against external interference. Consequently, an application's environment and the prevailing external factors will govern operating conditions.

V. Security in Wireless Sensor Networks

WSN applications require security, particularly when the networks are designed for use in hostile environ-

ments, military, aerospace, commercial or IoT applications [23]. Compared to other wireless networks, securing WSNs to an appropriate level is challenging as, typically, WSNs have certain unavoidable challenges [9], which form a unique combination of vulnerabilities:

1) Open Interface: Normally, protocols are unavoidably known publicly due to the requirement for interoperability between devices and protocols. Wireless channels are open to anyone with suitable equipment, enabling specific WSN attacks and access to transmitted signals.
2) Device Resources: Typically, devices are deployed, left unattended, must operate on a finite energy supply and, for reasons of cost, have low processing power, memory, physical storage, and speed. Generally, these constraints hinder the use of conventional security methods.
3) Operating Environments: Regularly, WSNs are deployed without any fixed infrastructure in hostile or remote environments, where it is difficult to have continued surveillance. Often, deployed legitimate network nodes become physically available to attackers and are susceptible to being captured. Therefore, a sufficiently high probability of node secrets being discovered and/or nodes being made malicious may prevail, thereby obliging countermeasure(s). Tamper proofing nodes is possible, but may not be appropriate/available for all types of networks/nodes due to, for example, cost restrictions.
4) Topology: WSN topologies can be dynamic and so changes are expected due to variations in the channel/environment (e.g. fading levels, obstacles, path losses, spurious interference, etc.), which may lead to the "death" of network nodes and topology reconfiguration.
5) Hardware Availability: Reconfigurable hardware, suitable for attacking networks, is becoming increasingly available/accessible to a wider set of users/potential malicious actors, who can readily design and deploy more computationally expensive attacks [29].
6) Deployment Diversification: As WSN applications continue to expand, the range of operating conditions, use cases, and created data widen.

Inclusive of the WSN vulnerabilities above, certain security features are required [13], [14].

1) Confidentiality: The secrecy of important data being transmitted in the wireless channel must be maintained. Classical cryptography can be adopted to encrypt critical data prior to transmission. However, a strict key management system may prove difficult, given WSN device resources.
2) Authenticity: Verifying packet authenticity is essential as the receiving node should be able to autonomously assert that the received packet has not been modified in transit (data integrity), and from which node the packet originated (origin authenticity). Cryptographic schemes, such as digital signatures, can simultaneously provide both functionalities. Without this security aspect, attackers could spoof node identities and spread false information throughout a WSN.
3) Availability: WSNs need to provide services whenever they are required and, therefore, need to exhibit qualities of robustness against a variety of impairments, both benign and malicious. Some degree of resilience (i.e. the ability to recovery from faults), diagnostics (i.e. able to identify why services became unavailable), or mitigation strategy (packet re-routing, channel switching, etc.) is necessary. Appropriate use of an IDS may help to ameliorate the network's availability.
4) Energy: Unique to WSNs, the constrained energy levels impact upon all security plans. Typically, nodes have a limited energy supply and, so, any security protocol or detection mechanism needs to take this energy constraint into account, since optimizing energy usage is vital for network longevity.
5) Data Freshness: Critical data circulating in a WSN must be the most recent update and, as such, outdated data should not circulate in a network.
6) Node Ability: WSN nodes must be self-organizing, react to node/link failures and only authorized nodes should be allowed to operate and share information in a WSN.

Evidently, no WSN will be 100% secure and it is extremely difficult to design a WSN where attackers cannot find some way in [23]. Timely mitigation strategies are required to combat attacks that exploit the WSN vulnerabilities. This provides a need for security measures which are either preventive, reactive or detective solutions [15]. Preventive measures include cryptography, spreading codes, frequency hopping, frame check sequences, etc. [9]. An IDS identifies the presence of intruders, so mitigation (or reactive) strategies can be implemented. The fundamentals of intrusions and intrusion detection were defined by James Anderson in 1980 and are; risk, threat, attack, vulnerability, and penetration [33]. Additionally, an IDS includes the delicate balance between detection and false-alarm rates, which can be particularly challenging in environments where many different physical layers occupy the same spectrum. Intrusion detection can be achieved using different methods [22], [30]:

- Misuse Detection compares the action or behavior

of transmitting/receiving nodes to well known attack patterns. These attack signatures form the knowledge base of the IDS.
- Anomaly Detection defines the characteristics of normal operation and activities and transmissions are compared against this normal operation. The IDS classifiers outliers, which are activities different from normal, as intruders.
- Hybrid or Specification-based detection includes IDSs which do not conform to anomaly or misuse. Normal behavior is manually defined by human perception. The focus is to determine deviations from this normal behavior, when it is not defined by training data or machine learning algorithms. Certain hybrid approaches can combine both anomaly and misuse detection.

The above discussion highlights the fact that security plays a major role in WSNs, is integral for any successful WSN based critical application and, typically, four pillars of WSN security exist; **vulnerabilities, requirements, attacks and defenses** [34]. Typically, networks have defined requirements, e.g. confidentiality, and employ specific defense strategies (encryption) to ensure each requirement is met. Networks, especially WSNs, have vulnerabilities and attacks can use these vulnerabilities to, potentially, increase attack efficiency. A notable example is the finite energy supply and, thus, attackers can focus on this vulnerable point. Therefore, this implies that the identified four pillars suit WSN security analysis. Furthermore, given the 3D model for reliability provided in [35], a similar approach can be taken for security, as provided in Fig. 3, which establishes a functional model for security using certain parameters. This model provides a simplified visual representation of some available security setups for WSNs. The specified model analyses whether a preventive, reactive or detection approach is used as the security mechanism, is a Hop-by-Hop or End-to-End basis applied and is security event-triggered or on each individual packet. Here, hop-by-hop refers to maintaining security across each and every link and end-to-end refers to only the source and destination maintaining security. Furthermore, typically, reliability provides bit loss recovery whilst security specifies bit loss prevention. Therefore, the topics can be linked in terms of packet loss and the model in [35] readily adapts to security.

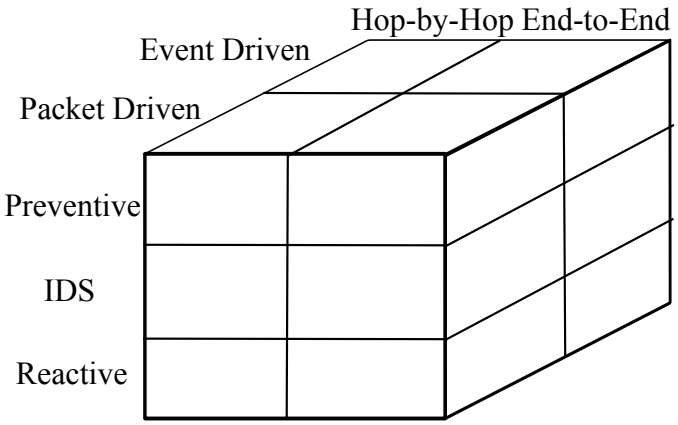


Figure 3. A functional simplified model for visualizing different security options in WSNs

VI. Attacks on Wireless Sensor Networks

Attacking a WSN involves either unauthorized access to data, data manipulation or denial of system services. These WSN attacks can be categorized into either passive or active attacks [13]. Passive attack styles do not modify information or messages but, instead, aim to learn the transmitted confidential data. Initially, this does not appear to have severe consequences, especially if data is encrypted. However, over time and given enough captured data, reverse engineering can provide the protocol in use and grant network access or packet decryption, which results in multiple network security consequences. In contrast, active attacks aim to modify/remove streams of data, cause a denial of service, disturb functionality or disguise an attack as a legitimate node. For convenience, a selection of known attacks on WSNs are categorized and described, where the focus is placed on PHY and MAC layer attacks, including jamming and congestion style intrusions. Generally, it is envisaged that external attacks, for example, jamming, will be implemented using a software-defined radio approach. This hardware provides the necessary ability to receive, analyze and transmit. The internal attacks, for example, sinkhole, will, typically, use a WSN device that has been captured or identified. Attack effectiveness and/or affected area, typically, depends on the strength of the transmitting power or how "transparent" the approach needs to be.

A. Conventional Jamming Attacks

These active attacks, typically, aim to overpower the legitimate signal with spurious radio-frequency transmissions. While higher jamming power increases attack effectiveness, it also boosts detectability. As such, the adversary is typically driven to optimize signal interference to maximize packet loss, while minimizing total broadcast power. Such attacks include:

1) The constant jammer continuously emits RF signals of random data into the wireless medium without following any MAC protocol, can be readily detected and is energy inefficient. However, this jammer can be easily implemented and causes severe damage to

a WSN, as congestion or destruction of packets can be achieved and the channel can appear permanently busy.

2) The deceptive jammer regularly transmits protocol specific packets into the network without pausing between successive packets, thereby preventing normal sources from transmitting successfully. Due to the transmission of legitimate packets, it is more difficult to detect than a constant jammer and can cause considerable damage in WSNs adhering to MAC protocols, which are sensing for channel access or the presence/absence of a signal.
3) Random jammers sporadically transmit random packets of data and conserve energy by switching between the jamming state, when jamming signals are emitted, and the sleeping state, when all transmissions are ceased. This unpredictable behavior makes this jammer difficult to mitigate and can cause similar levels of damage as the constant and deceptive jammers.
4) A reactive jammer [19] operates in idle mode until some legitimate activity is detected on the wireless channel. A RTS/CTS jammer detects request to send (RTS) messages and interferes with the channel to block any clear to send (CTS) messages, thereby denying further communications. Data acknowledgment jammers corrupt acknowledgment packets after a transmission has been sensed in the network and misleads nodes to decide that packets were undelivered, thereby invoking a retransmission and, potentially, resulting in the exhaustion of the power supply. This is particularly effective in protocols, such as ZigBee, which use CSMA/CA.
5) Specific function jammers perform explicit functions, depending on their calibration, and cause jamming on either a specific channel or across an entire network, while minimizing their energy consumption or maximizing their attack effect. For example, follow-on jammers jam one specific frequency at a time and maximize packet loss by continuously hopping between the channel frequencies. These jammers can be detected but are very effective, particularly in networks that use frequency hopping spread spectrum or when identified spectrum holes [36] are used to improve performance through spectrum sharing. Another example is the channel-hopping jammer, which follows a predefined pseudo-random sequence of channels and starts jamming at different time slots according to this sequence. By overwriting the sequence, multiple channels can be jammed at the same time. Finally, pulse noise jammers can be programmed to switch between different channels/bandwidths and conserve energy by temporarily halting transmissions.

B. Intelligent Jamming Attacks

Intelligent jammers are a combination of a passive and an active attack, as the jammer initially targets network privacy before inevitably targeting data packets. These devices are more likely to cause jamming but are harder to implement than conventional jammers [29]. Protocol aware and statistical jammers aim to determine the MAC protocol being used by the victim's network in order to launch energy efficient attacks [31]. Protocol aware jammers know the MAC layer operating rules and can deprive legitimate nodes of access to the channel and can, potentially, affect services identifying free channels or spectrum holes, used to, potentially, enhance spectrum coexistence [36]. Statistical jammers observe the packet inter-arrival time distribution and, based on its estimation, emit pulses of jamming signals to disrupt communications (DoS attack). Once the estimation is achieved, energy efficiency can be increased through pulse jamming. Collision makers target the identified acknowledgment packets by inhibiting transmissions. Certain intelligent jammers identify the cluster head/sinks by monitoring the network traffic and focus attacks on that specific node in an "Intelligent Cluster Head Attack". Learning based jammers, like LearJam, have been produced to attack low duty cycle networks where nodes sleep most of the time (a typical WSN characteristic) and consist of a learning phase, wherein the node transmission pattern is observed, and an attacking phase, where these transmissions are compromised. Therefore, clearly attackers are now able to learn the MAC and/or protocols in use by eavesdropping (privacy attack) on the channel for some period of time. This attack style could, for example, be launched on techniques for sensing the presence or absence of a signal (CSMA/CA or spectrum sharing), by learning when a service should be idle and producing "dummy" packets to avert potential transmissions.

C. MAC Layer Jamming Attacks

These are, initially, passive attacks that react to the network protocol in use by eavesdropping on or sniffing transmitted packets to gain access to network information. The analyzed results are used to implement active attacks including replay attacks, spoofed packets or forcing a device to remain in listening mode, which exploits CSMA/CA. These are not jamming attacks but, instead, try to mislead WSN devices. Replay attacks should be negated by the use of message integrity codes. However, due to hostile deployment scenarios, secrets may be accessible as legitimate nodes may be physically available and, if no key management system

is in use (home personal COTS network), devices may be available commercially and the keys extracted from device memory.

D. Network-Layer Attacks

Generally, these are active attacks that interfere with network operations causing either a DoS, a privacy or an impersonation attack.

1) Sinkhole/Blackhole Attacks: In this congestion based DoS attack, a malicious node acts like a black hole [32] and "pulls in" all of the traffic in the network. The malicious node listens to the route requests and replies that it has the shortest path, maximizing packet flow.
2) Selective Forwarding: Networks that rely on multi-hop transmissions require all nodes to faithfully forward any received packets to the base station. In this packet dropping DoS attack, a malicious node in the routing path selectively drops sensitive packets.
3) Node Replication Attacks: In WSNs, nodes are often deployed in unattended public environments where continued surveillance is unrealistic. In this impersonation attack, an attacker may replicate a legitimate node and introduce it to the network, thereby gaining access to the flow of packets throughout the network. This may involve the capture and analysis of a legitimate node in cases where some level of cryptographic security is applied.
4) Sybil Attacks: Many applications require node collaboration to accomplish a certain task. Applications can then implement management policies to distribute sub-tasks to different nodes. In this impersonation attack, a malicious node will pretend to be more than one node at the same time, using the identities of other legitimate nodes to effectively cause collaboration processes to fail and can target data aggregation, routing mechanisms, etc.
5) HELLO Flood Attacks: Often, routing protocols need to broadcast "HELLO" packets in order to discover one-hop neighbors. The attacker exploits this concept to attract and persuade nodes that an attacker is their neighbor. This is especially effective if the attacking node has a large radio range and enough processing power to flood an entire area of a network, affecting a large number of nodes and persuading these nodes to use the attacker as a relay node in the process. Packets are lost in this energy consumption DoS attack due to, for example, distances being too large for transmission as a node will try to transmit to a non-neighbor (attacker).
6) Wormhole Attacks: An attacker records the packets at one location in the network and tunnels those packets to another area in the network using a long range wireless channel or optical link. Attackers offer fewer hops and less delay and entice nodes to use the attacker to forward packets, thereby causing collisions and packet loss in this DoS congestion attack.
7) Spoofing: Network nodes can become malicious and provide an attacker network access, when nodes are physically available in environments without continued surveillance and each individual node is not tamper proofed due to, generally, cost reasons. Spoofing is the method of disguising a communication from an unknown source as being from a known, trusted source. It can severely harm any WSN, as it is both difficult to detect and effective. A spoofing situation can involve either an attacker successfully identifying as a network node by falsifying data or by transmitting falsified data with real credentials from a malicious node. This type of attack is difficult to detect and requires an IDS which can identify node anomalies.

It is clear from analyzing the above attacks that a detection algorithm which has both centralized and distributed features is optimal as the attacks in VI-A, VI-B and VI-C above could be detected in a distributed structure, while certain attacks in VI-D will need to be detected in a centralized structure and others in a distributed manner; for example, a black hole may fail to generate application-level acknowledgments that can imply network failure, even though the attacker is sending protocol level acknowledgments. Another very interesting point was highlighted in [37], which stated that, in future attacks, more than one style will likely be used at the same time and multiple layers will be attacked in a cross-layer approach. For example, using a sinkhole attack to guide packets to a specific region so a jammer could jam a larger area.

E. System Coexistence

This section identifies intrusions from spectrum coexistence and spectrum sharing fields. Intrusions from the coexistence of systems in the same frequency range and when protocols misuse sharing capabilities are discussed.

1) A secondary user (SU) occupying a primary user's (PU) spectrum and causing interference. The SU operates for too long or when the PU is operating and interferes with the PU's performance. The intention was to maximize spectrum use but the SU became an intruder.
2) An attacker or a certain spectrum user consumes all resources and deliberately denies spectrum sharing,

causing other equal users to suffer performance loss or denial of service.
3) Specific users being saturated by coexisting legitimate signals, leading to a DoS attack.

In these examples network performance is affected and, so, intrusions exist. Clearly, a SU occupying a PU's channel for too long and affecting the PU's performance becomes an attacker. Resources can be denied by, for example, blocking CTS packets, and so any device operating as such inherently becomes an intruder. In spectrum sharing, a cognitive radio (CR) senses for the absence of a PU (spectrum holes) [38] and a user could block the discovery of these spectrum holes, becoming an attacker in the process. This coexistence issue will be examined in Section VII using Monte-Carlo simulations and a spectrum analyzer in the ISM band.

VII. Discussion: Attacks on WSNs

Particular WSN attacks and coexistence issues are discussed here by examining the ZigBee signal model, described in Section III, and the PER, which, typically, describes the success of an attack as a successful intrusion can be attributed to resulting packet losses. This subarea of attacks introduced in section VI are of particular interest for the expanding IoT sector, which leverages WSNs, and spectrum usage. Intentional jamming and spectral coexistence serve as an introduction into IoT penetration testing, where both potential attackers and co-existing with other protocols and systems are evaluated. Taking this approach can, potentially, identify application weaknesses in terms of the operating wireless channel, environment and spectrum. Furthermore, this focus on ZigBee's PHY and MAC depicts the performance of the IEEE 802.15.4 PHY and MAC, which are implemented across a variety of WSN protocols. Fig. 4 contains a Matlab simulated subgroup of jamming attacks and, to highlight the difficulties of a congested spectrum, ISM band coexistence issues. The effects of a constant jamming continuous wave (CW) jammer, an AWGN jammer, an intelligent matched protocol jammer (which here refers to a ZigBee signal and frame structure (Table II) being used by an intruder to attack a ZigBee network) and IEEE 802.11b coexistence are demonstrated. The CW and matched protocol jamming attacks were first discussed in [29], along with a practical demonstration of the matched protocol interference. The approach was practically tested using a ZigBee network of five XBee nodes and a software defined radio (SDR). The SDR artificially created an IEEE 802.15.4 signal and frame structure in Matlab/Simulink to produce the matched protocol interference, which caused a working network to fail. This was an example of a learning based jammer where the packet structure was identified by eavesdropping on the open interface of the WSN.

The CW response represents a simple jamming attack as a sine wave is injected into the spectrum (added to signals during simulations). The jammer-to-signal ratio (JSR) is significantly higher for a disruptive PER and, therefore, would be detectable in the spectrum. The CW response represents the operational mode of many jammers in Section VI-A as it is, generally, spurious interference. The matched protocol jammer simulations show that it is more of a threat to WSNs than conventional CW techniques, while adjacent channels (ZigBee 5 MHz) have little to no effect. At a JSR of 0dB, the matched interference causes a PER of approximately 0.18 and the signal structure matches expected signals in the channel. Therefore, the matched interference is a threat at low JSR values while simultaneously being difficult to detect. In both the CW and matched protocol cases, once jamming power rises above a certain threshold, substantial numbers of packets will be lost, but this threshold is much lower when the interference is protocol specific. The AWGN interference is included to show the difficulty in differentiating noisy congested networks from attacks. The AWGN attack (white noise across the spectrum centered on the channel) has more of an effect on the signal than a CW jammer at JSR above 11dB. Detecting these attacks would typically be based on classical spectrum analysis exploiting higher signal powers and offset spurs. However, matched signal interference, which causes more damage than CW, is more difficult to detect as packets resemble those of the network, meaning that traditional spectrum approaches may not be appropriate. This amplifies the need for IDSs to utilize extra available analysis tools, for example, machine learning, as attackers can discover and mimic WSN protocols and noisy environments can resemble attack situations.

The IEEE 802.15.4 based protocols (ZigBee) coexist with various signals in the ISM RF band, including WiFi (IEEE 802.11b). This phenomenon was simulated for the 802.11b 1Mb/s DSSS protocol offset by 2, 3 and 7 MHz, as these offsets relate to the offsets seen by a ZigBee signal compared to the center of an 802.11b signal. For example, 802.11b channel 11 (2.462 GHz) and ZigBee channels 21 (2.455 GHz), 22 (2.460 GHz) and 23 (2.465 GHz). The simulations show that other services can act as interference (PER $\geq$ 0.1), given a high enough JSR ($\geq$ 16.5 dB). These coexistence issues were experimentally benchtop tested using an XBee ZigBee peer-to-peer network, multiple PCs and the Tektronix real time spectrum analyzer (RTSA) 306B

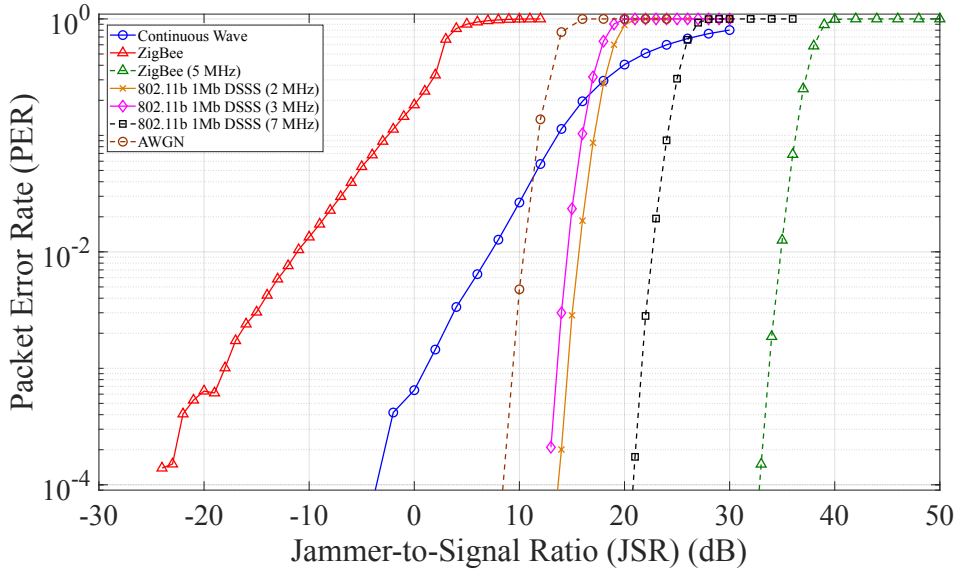


Figure 4. ZigBee PERs for CW, matched, offset matched and 802.11b coexistence interference for a range of JSRs

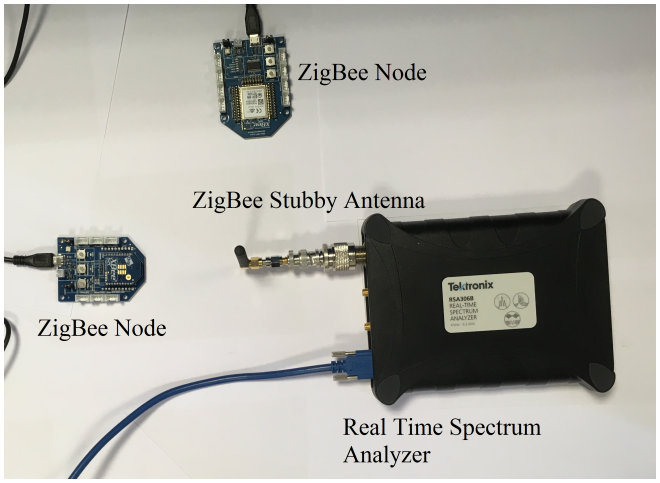
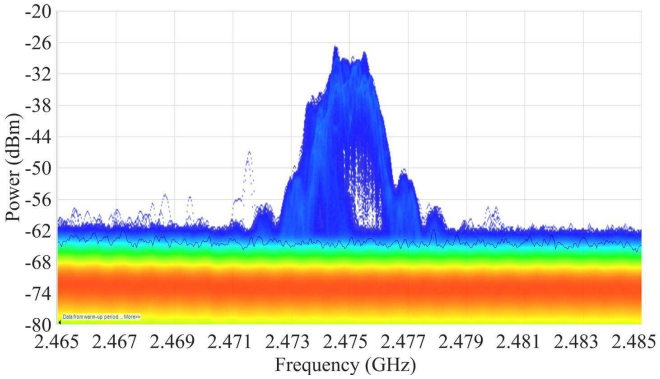
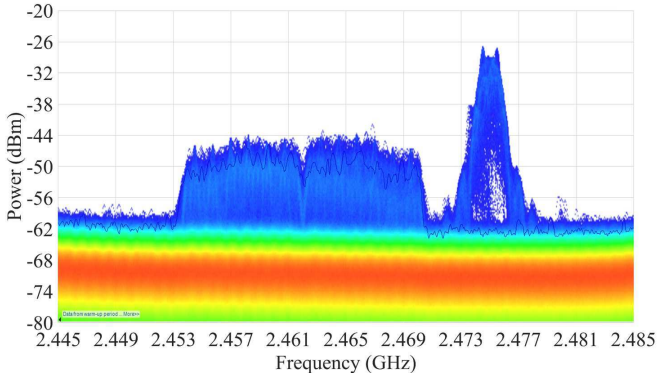


Figure 5. Hardware used in experimental setup to highlight the issues in a congested spectrum and to produce the DPX spectrum graphs for the signals of interest

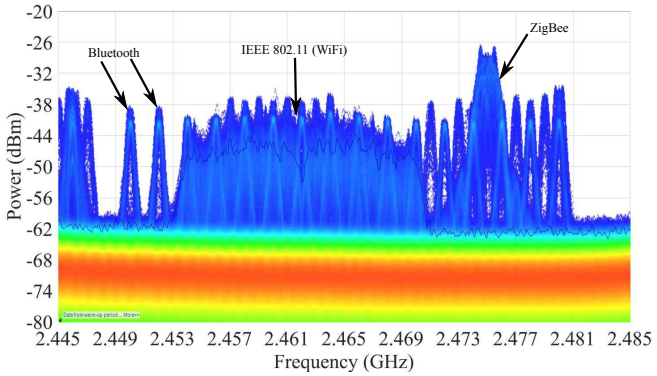
using a Siretta ZigBee stubby antenna. WiFi signals (campus WiFi) and/or Bluetooth signals (local devices) were provided by enabling laptops, phones, and speakers in the vicinity around one XBee transceiver. The main hardware utilized is provided in Fig. 5, where the components are close together for photographic convenience only, as the transmitting and receiving XBee devices were sufficiently separated during testing. Spectrum graphs are developed using Tektronix's Digital Phosphor technology (DPX), which runs on the SignalVu-PC software package and acquires signals in real time. DPX performs hardware digital signal processing and rasterizing of samples into pixel information, which can be plotted in real time and as a bitmap image (instead of a conventional line trace). This allows signals to be distinguished at the same frequency and a color scheme is used to identify signals which are more frequent than others. Here, the 2475 MHz ZigBee channel was used and a spectral DPX image is shown in Fig. 6a, where the dark blue is the highest level and corresponds to how frequent the signal is. All transmitted and received packets were monitored by using DIGI's XCTU software, which provides a graphical user interface for packet monitoring. Each transmission required an acknowledgment packet, stating either "Delivery Status: Success" for a successful transmission or "Delivery Status: Address not found" for an unsuccessful transmission. Real time coexistence issues are visualized in Fig. 6b and Fig. 6c, where the ZigBee signal coexisted with WiFi only and WiFi/Bluetooth, respectively. Fig. 6d provides the



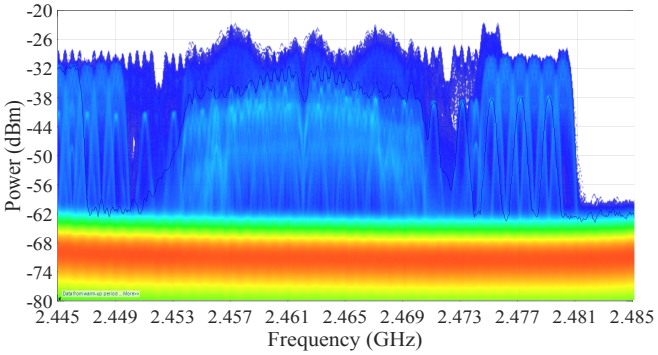
(a) DPX image showing the ZigBee signal at 2475 MHz



(b) DPX image showing coexistence of ZigBee with 802.11 WiFi



(c) DPX image showing coexistence of ZigBee with 802.11 WiFi and Bluetooth



(d) DPX image showing the spectral environment when ZigBee packets were lost

Figure 6. DPX visualization of the ISM RF Spectrum during the benchtop experiments

spectral analysis for when packets were dropped in the network. These unsuccessful transmissions were due to the interference caused by multiple devices using WiFi and Bluetooth in the vicinity of the intended XBee receiver. This differs from Fig. 6c due to both the higher power interference signals at 2.475 GHz and recurring number of transmissions, given by the fuller nature and more intense color of the DPX image. Compared to Fig. 6c, Fig. 6d has approximately 6dBm higher coexisting signals and, due to a higher volume of connected devices, more frequent ISM band transmissions. Essentially, these benchtop tests provided visual proof of the spectrum coexistence issues, the noisy environments and legitimate signal intrusions which exist in WSNs. The undelivered packets, which occurred under extreme coexistence circumstances, provided evidence that environments and coexisting signals can be seen as both unintentional and, in malicious cases, intentional interference. Therefore, the detection of both intentional and unintentional interference is important for providing a holistic IDS and adequate security.

Furthermore, other attacks (Section VI-D) on the upper layers of the protocol stack can be detected by analyzing both the routing process and network properties. However, detection can become skewed if the attackers are subtle about their operation. For example, monitoring network operation and implementing a sinkhole attack that sporadically drops critical packets, which may mimic PER levels resulting from a noisy environment, or a wormhole attack tunneling only one of every N packets. With the threat of legitimate nodes being captured, detection and security mechanisms need to account for malicious nodes in the network. Finally, it is clear that an attacker is either an “outlaw” who breaks spectrum laws (excessive radiated power) or a “non-compliant” operator who adheres to broadcast power limitations but simply refuses to follow protocol operation (service refusing to give up resources). Additionally, each layer, from the PHY upwards is vulnerable and it is clear that intrusion detection and security are complex processes and cannot simply focus on one aspect but, rather, must examine the whole process from transmission to reception, and everything in between.

VIII. Future Directions

Security and intrusion detection, both intentional and unintentional, is integral for the future of successful WSN deployments, especially in critical applications, like aerospace, space-based WSNs, IoT, and using nanosatellites as relay nodes. Security and IDSs cannot simply focus on particular attack strategies, they must also consider coexistence issues as intrusions and need to recognize that hostile noisy environments exist. Due to the flexible topology, open interface and power limitations of these WSNs, this is a complex challenge and needs to be solved to allow WSNs to be used in safety critical applications and to safely exploit COTS devices and standardized protocols. Based on the aforementioned pillars of security (vulnerabilities, requirements, attacks, and defenses) and attack discussion, future work lies in security development in terms of intrusion detection, both intentional and unintentional, and mitigation. Attack effects on WSNs and the associated signals and analysis of why each specific security technique is used will be beneficial. Additionally, the data from the PHY layer has potential to be investigated as the radio architectures are usually very similar between wireless standards and so, by concentrating on the PHY symbol stream and related measurements, the possibility of designing a transferable solution exists. This future work entails both a reactive and detection approach, which has potential to be environment specific. As the wireless channel is a non-linear phenomenon, an approach which can model nonlinearities and adapt to new models is recommended. From this perspective, a feature/featureless based machine learning algorithm focused on received samples in the PHY is seen as an appropriate continuation from this article. The focus lies in the development of a detection strategy, which can distinguish between good operating and interference intensive channels, while classifying the cause. A machine learning approach seems applicable due to previous work in non-linear time series [39].

IX. Conclusion

This article discussed interference and intrusions in WSNs in terms of the four pillars of security; vulnerabilities, requirements, attacks, and defenses. An extensive overview of both WSN security issues and WSN attacks were provided and two main types of adversaries were defined; the outlaw, who breaks the spectrum laws, and the non-compliant operator, who adheres to laws but does not follow protocol rules. By utilizing ZigBee, certain attacks were simulated, using Matlab, and it was shown that matched protocol interference was more of a threat than conventional CW jamming and, also, harder to detect. This implies that traditional interference detection schemes might be inadequate, as intruder signals can be indistinguishable from legitimate ones. A real time analysis of coexisting signals causing interference and denial of service expanded this point and highlighted the two main types of adversaries. Therefore, the work in this article implies that WSN can be vulnerable to interference and/or intrusions, but techniques can be used to add resilience and detectability. To conclude, this paper highlighted that if WSNs are to become integrated into modern society and to be used frequently in critical applications, like the IoT and aerospace, enhancements to both security and the detection of intentional and unintentional intrusions is necessary. Detection strategies need to advance and look at aspects outside the norm, for example, received raw bits, while maintaining the optimization of device resources. Future designs should encapsulate security at the beginning of the design process and incorporate an IDS and utilize all layers from the PHY upwards. The IDS should be able to characterize the intrusion and be able to distinguish between intentional and unintentional intrusions.

Acknowledgments

This work has been jointly funded by the Irish Research Council (IRC) and United Technologies Research Center Ireland (UTRC-I) under the post-graduate Enterprise Partnership Scheme 2016, award number EPSPG/2016/66.

References

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

[2] Kruger,C. P. and Hancke,G. P., "Implementing the Internet of Things Vision in Industrial Wireless Sensor Networks," in *12th IEEE International Conference on Industrial Informatics (INDIN)*, pp. 627–632, 2014.

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

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

[5] Li,S., Chen,B., and Yu,L., "A modified 802.11 protocol applicated in space wireless local area network," *International Conference on Computer Design and Applications, ICCDA*, vol. 2, pp. 585–588, 2010.

[6] Celandroni,N., Ferro,E., Gotta,A., Oligeri,G., Roseti,C., and Luglio,M., "A survey of architectures and scenarios in satellite-based WSN," *International Journal of Satellite Communications and Networking*, vol. 31, pp. 1–38, 2012.

[7] Addaim,A., Kherras,A., and Guennoun,Z., "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.

[8] Yedavalli,R. K. and Belapurkar,R. K., "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.

[9] O Mahony,G. D., Harris,P. J., and Murphy,C. C., "Investigating the Prevalent Security Techniques in Wireless Sensor Network Protocols," in *30th IEEE Irish Signals and Systems Conference (ISSC)*, pp. 1–6, 2019.

[10] Bowler,T., "The low-cost mini satellites bringing mobile to the world," 2018.

[11] Marszalek,M., Rummelhagen,M., and Schramm,F., "Potentials and limitations of IEEE 802.11 for satellite swarms," *IEEE Aerospace Conference*, pp. 1–9, 2014.

[12] Wood,A. D. and Stankovic,J. A., "Denial of Service in Sensor Networks," *IEEE Computer Magazine*, vol. 35, no. 10, pp. 54–62, 2002.

[13] Tyagi,A., Kushwah,J., and Bhalla,M., "Threats to security of Wireless Sensor Networks," *7th International Conference on Cloud Computing, Data Science and Engineering*, pp. 402–405, 2017.

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

[15] Tomi,I. and Mccann,J. A., "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1910–1923, 2017.

[16] Shanthi,S. and Rajan,E. G., "Comprehensive Analysis of Security Attacks and Intrusion Detection System in Wireless Sensor Networks," in *IEEE 2nd International Conference on Next Generation Computing Technologies (NGCT)*, pp. 426–431, 2016.

[17] Mpitziopoulos,A., Gavalas,D., Konstantopoulos,C., and Pantziou,G., "A survey on jamming attacks and countermeasures in WSNs," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[18] Li,M., Koutsopoulos,I., and Poovendran,R., "Optimal jamming attacks and network defense policies in wireless sensor networks," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications*, pp. 1307–1315, IEEE, 2007.

[19] Wilhelm,M., Martinovic,I., Schmitt,J. B., and Lenders,V., "Short paper: Reactive jamming in wireless networks - How realistic is the threat?," *4th ACM Conference on Wireless Network Security*, no. June, pp. 47–52, 2011.

[20] Liu,D., Raymer,J., and Fox,A., "Efficient and Timely Jamming Detection in Wireless Sensor Networks," in *IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS)*, pp. 335–343, 2012.

[21] Yu,Z. and Tsai,J. J. P., "A Framework of Machine Learning Based Intrusion Detection for Wireless Sensor Networks," in *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, pp. 272–279, 2008.

[22] Can,O. and Sahingoz,O. K., "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," in *6th International Conference on Modeling, Simulation and Applied Optimization (ICMSAO)*, 2015.

[23] Abduvaliyev,A., Pathan,A.-S. K., Zhou,J., Roman,R., and Wong,L. W.-C., "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks," *IEEE Communiations Surveys and Tutorials*, vol. 15, no. 3, pp. 1223–1237, 2013.

[24] O'Mahony,G. D., O'Mahony,S., Curran,J. T., and Murphy,C. C., "Developing a low-cost platform for GNSS interference detection," in *European Navigation Conference*, 2015, pp.1-8.

[25] Puñal,O., Aktas,I., Schnelke,C.-J., Abidin,G., Wehrle,K., and Gross,J., "Machine learning-based jamming detection for IEEE 802.11: Design and experimental evaluation," in *IEEE 15th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 1–10, IEEE, 2014.

[26] Sikora,A. and Groza,V. F., "Coexistence of IEEE 802.15.4 with other systems in the 2.4 GHz-ISM-band," in *IEEE Instrumentation and Measurement Technology Conference (IMTC)*, pp. 1786–1791, 2005.

[27] Stelte,B. and Rodosek,G. D., "Thwarting attacks on ZigBee - Removal of the KillerBee stinger," in *Proceedings of the 9th International Conference on Network and Service Management*, pp. 219–226, 2013.

[28] ZigBee Alliance,, "ZigBee Specification. ZigBee document 053474r20," tech. rep., 2012.

[29] O Mahony,G. D., Harris,P. J., and Murphy,C. C., "Analyzing the Vulnerability of Wireless Sensor Networks to a Malicious Matched Protocol Attack," in *52nd IEEE International Carnahan Conference on Security Technology (ICCST)*, pp. 1–5, IEEE, 2018.

[30] Wood,A. D., Stankovic,J. A., and Son,S. H., "JAM : A Jammed-Area Mapping Service for Sensor Networks," in *24th IEEE Real-Time Systems Symposium*, pp. 286–297, 2003.

[31] Hamza,T., Kaddoum,G., Meddeb,A., and Matar,G., "A Survey on Intelligent MAC Layer Jamming Attacks and Countermeasures in WSNs," in *IEEE 84th Vehicular Technology Conference (VTC-Fall)*, 2016.

[32] Ahmed,N., Kanhere,S. S., and Jha,S., "The holes problem in wireless sensor networks: a survey," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 9, no. 2, pp. 4–18, 2005.

[33] Anderson,J. P., "Computer security threat monitoring and surveillance," *James P Anderson Company, Fort Washington, Pennsylvania*, 1980.

[34] Kocher,I. S., Chow,C.-O., Ishii,H., and Zia,T. A., "Threat Models and Security Issues in Wireless Sensor Networks," *International Journal of Computer Theory and Engineering*, vol. 5, no. 5, pp. 830–835, 2013.

[35] Mahmood,M. A., Seah,W. K., and Welch,I., "Reliability in wireless sensor networks: A survey and challenges ahead," *Computer Networks*, vol. 79, pp. 166–187, 2015.

[36] Dehnie,S., Chakravarthy,V., Wu,Z., Ghosh,C., and Li,H., "Spectrum Coexistence Issues : Challenges and Research Directions," in *IEEE Military Communications Conference (MILCOM)*, pp. 1681–1689, 2013.

[37] Tayebi,A., Berber,S., and Swain,A., "Wireless Sensor Network attacks: An overview and critical analysis," in *Seventh International Conference on Sensing Technology (ICST)*, pp. 97–102, IEEE, 2013.

[38] Rawat,A. S., Anand,P., Chen,H., and Varshney,P. K., "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 2, pp. 774–786, 2011.

[39] Alhajri,M. I., Ali,N. T., and Shubair,R. M., "Classification of Indoor Environments for IoT Applications: A Machine Learning Approach," *IEEE Antennas and Wireless Propagation Letters*, vol. 17, no. 12, pp. 2164–2168, 2018.