Title	Investigating the prevalent security techniques in wireless sensor network protocols
Author(s)	O'Mahony, George D.; Harris, Philip J.; Murphy, Colin D.
Publication date	2019-06
Original citation	O'Mahony, G. D., Harris, P. J. and Murphy, C. C. (2019) 'Investigating the Prevalent Security Techniques in Wireless Sensor Network Protocols', 2019 30th Irish Signals and Systems Conference (ISSC), Maynooth, 17-18 June, pp. 1-6. doi: 10.1109/ISSC.2019.8904934
Type of publication	Conference item
Link to publisher's version	https://ieeexplore.ieee.org/abstract/document/8904934 http://dx.doi.org/10.1109/ISSC.2019.8904934 Access to the full text of the published version may require a subscription.
Rights	**© 2019 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.**
Item downloaded from	http://hdl.handle.net/10468/9534

Investigating the Prevalent Security Techniques in Wireless Sensor Network Protocols

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*—The radio architectures of and protocols used by wireless sensor networks (WSNs) are, typically, very similar and are based on IEEE 802.15.4. By concentrating on this standard and the associated employed security techniques, the possibility of designing a transferable safety and privacy enhancement across protocols and services, becomes a reality. WSN applications have expanded significantly over the past decade or so and adopt commercial off-the-shelf (COTS) devices and publicly available standards, which inherently creates intruder incentives and security challenges. Securing WSNs is a critical requirement due to the challenging burden of protecting the transmitted sensitive information across various applications, while operating under unique security vulnerabilities and a fluctuating radio frequency (RF) spectrum and physical environment. Couple this aspect with establishing a level of trust among network nodes, while providing resilience to interference, it becomes clear that maintaining security is challenging. This paper identifies unique vulnerabilities in WSNs, which have a direct impact on privacy and safety. The prevalent security techniques used in the common PHY and MAC layers of various WSN protocols are discussed in terms of providing the essential security requirements. An experimental visualization of the coexistence issues in the industrial, scientific and medical (ISM) RF band, which is integral for IoT operations, is provided as an introduction to a new perspective on attacking WSNs. Fundamental attack styles and spectrum sharing/coexistence based intrusions are presented. Typical methods, which use COTS devices and open source software to exploit WSN security holes, are also discussed.**

***Index Terms*—Interference, Intrusion, IoT, MAC, Packet, PHY, Protocol, Security, & WSN.**

I. Introduction

As Wireless Sensor Networks (WSNs) continue to develop into an indispensable component of modern technology and as the radio frequency (RF) spectrum becomes increasingly congested, the enhanced security of the communication link evolves into a necessity. Applications and innovative solutions continue to use WSNs to permit easier design, installation and maintenance, while simultaneously providing new deployment options. Since WSN utilization has expanded, new challenges in terms of security materialize due to the rise of stricter operational and availability requirements. This is evident in various innovative applications based on over a decade of research and development, like, spaced-based WSNs [1], the Internet of Things (IoT), wireless networked control systems (WNCS) [2] and C4ISRT systems [3].

These applications combined with coexistence issues in the $2.4GHz$ industrial, scientific and medical (ISM) radio frequency (RF) band, due to expanding numbers of connected devices, add layers of complexity to security issues. The various applications and the ISM band coupled with the trend of using available commercial off the shelf (COTS) devices and publicly known standardized protocols, demonstrates the essential need for security in each WSN protocol in use. Consequently, network compromise, whether malicious or unintentional, can have significant consequences for privacy and safety. Therefore, the security and availability of the communication link and the delivery of authentic and confidential packets are essential for safety critical WSNs.

This paper analyzes the unique vulnerabilities of WSNs in order to incentivize the need for security enhancements. The main WSN protocols in use are identified and their common packet and signal structures are investigated in terms of employed security techniques. The security feature is expanded through a real world visualization of the coexistence issue in the ISM RF band and acts as an introduction to a unique WSN attack style. Fundamental attack styles focused on the employed security in the PHY and MAC layers are defined to demonstrate the severity of the safety and privacy issue in WSNs. Example methods of exploiting WSN vulnerabilities are also provided, along with suitable low-cost COTS devices.

The remainder of this paper is organized as follows: Section II describes WSNs and their associated applications. Section III characterizes unique WSN security vulnerabilities. Section IV defines IEEE 802.15.4 and how it links WSN protocols. Section V specifies the main security techniques employed, while section VI illustrates how these security techniques are exploited. Finally, section VII concludes this paper.

II. WSN Description & Applications

WSNs consist of multiple lightweight devices (nodes) used to sense the physical world and, typically, incorporate a radio transceiver, a micro-controller, sensors and a limited energy source. These nodes gather data from their environment and, often, collaborate together to transmit the sensed data

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.

to a centralized sink or cluster head. Main characteristics include energy usage, handling node failures, nodes joining and heterogeneity of nodes, operating in harsh conditions, ability to scale and incorporating mobile nodes. A general network communication approach is provided in Fig. 1, where a WSN protocol is used for communications between the sensing devices and coordinator, which acts as an access point for network users to capture and analyze data and permit the use of a network/security manager. Transmission between the access point and other components is usually achieved through internet access but can include cellular, wired connections and more computationally powerful relay nodes, for example, Low Earth Orbit (LEO) satellites as a WSN component [4].

WSNs operate either a star, mesh or peer-to-peer topology and, in each case, are self-organizing, self-repairing, dynamic and can exploit the cluster head approach. Individual devices can be either a full function device (FFD), which act as a Personal Area Network (PAN) coordinator, router or end device, or a reduced function device (RFD), which act as a simple sensing end device. A FFD can communicate with other FFDs or RFDs, while a RFD can only communicate with one FFD. Two or more of these devices (minimum of one FFD as coordinator) operating on the same channel and within a personal operation space form a wireless PAN. Each PAN selects an unique identifier (PANId) and all devices have an unique 64-bit address. An example mesh topology, which exploits clustering, is provided in Fig. 2. This typical WSN approach can use data aggregation techniques at routers or relay nodes to minimize communication overhead and maximize energy efficiency. Generally, this is achieved by unifying several data items into a single packet, applying compression techniques or processing data at the relay nodes. A network manager is responsible for the configuration between nodes and a security manager is responsible for key management.

WSN applications are diverse and, according to [3], can be classified into precision agriculture, environmental monitoring, vehicle tracking, health care, smart buildings, military and animal tracking. Expansions exist and include aerospace [5], space-based applications [1], the ever expanding IoT, wireless body area networks (WBANs) and unmanned aerial vehicles (UAVS) [6]. Evidently WSNs require security across a wide range of physical environments, deployments scenarios and structures, in which privacy and safety are pivotal. Furthermore, these applications can be valuable and, typically, use sensitive data, which incentivize malicious actors to intentionally disrupt or compromise network operation. This coupled with unique WSN vulnerabilities, provided in section III, demonstrates the difficulty in guaranteeing security.

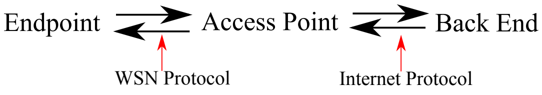

Fig. 1. Typical communications strategy in a WSN application

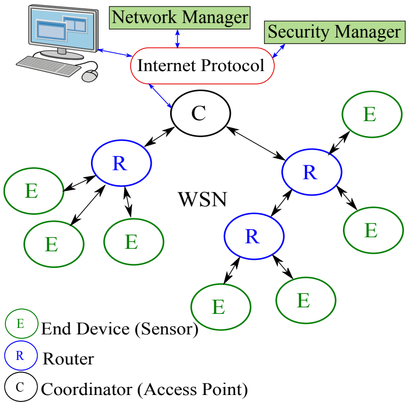

Fig. 2. Example WSN mesh topology utilizing a cluster approach

III. WSN Security Vulnerabilities

WSNs require security, particularly when the networks are designed for use in hostile environments and critical applications, like military or IoT, which have strict security and availability requirements. When WSNs are analyzed in terms of their construction, deployment and usage, certain unique security vulnerabilities become apparent. This indicates that securing WSNs appropriately is more difficult when compared to other wireless/wired networks. Furthermore, WSNs are susceptible to various attack styles, including jamming, eavesdropping and tampering. Therefore, when providing the necessary security requirements, it is clear that WSNs will not be 100% secure and as WSNs become more integrated in modern applications, possibilities exists that security enhancements are required. These vulnerabilities, partially identified in [7], are expanded and summarized below:

- Open Interface: Generally, WSN protocols are unavoidably known publicly due to the requirement for interoperability and use of standardized open access protocols. Additionally, the wireless channel is open to anyone with suitable equipment, resulting in an increased susceptibility to attacks.
- Device Resources: Typically WSN devices operate on a constrained energy supply and, for reasons of cost, have low processing power, meaning computationally expensive protocols/techniques are not employed. The use of COTS devices is seen as relevant given the general trends towards using these devices in applications where high redundancy high replenishment rate is favored over custom built components.
- Hostile Environments: WSNs are regularly deployed and left unattended in harsh environmental conditions without any fixed infrastructure, where it is difficult to have continued surveillance [8]. This strategy means legitimate nodes are potentially physically available to being captured and/or tampered with by attackers, leading to a high probability of node secrets being discovered and specific nodes becoming malicious. Tamper proofing nodes is possible, but, for reasons of cost, may not be appropriate and, so, encryption keys may be obtained from device memory. Typically, the physical environment contains varying fading levels, obstacles, path

losses and spurious interference, while the RF spectrum changes rapidly as it adjusts to the number of connected devices, demand, packet size and services in operation. These non-malicious factors coupled with the availability of nodes, increases the probability of network compromise.

- Topology [8]: Network topologies constantly change due to variations in the environment (fading levels, obstacles, path losses, spurious interference etc.), the natural dynamic nature of WSNs or damage/“death” of network nodes. This WSN feature can be exploited by potential attackers who wish to either gain access or cause spurious harm to the network.
- 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. Additionally, the computational ability of available devices is expanding, leading to advanced attack styles. This was illustrated when a low-cost software defined radio (SDR) caused matched protocol interference in a WSN in [9].
- Deployment Diversification: As the application space of WSNs continues to expand into new frontiers, a more diverse range of deployments becomes the norm. WSNs were traditionally involved in monitoring applications but have now extended into space operations, WBANs and UAVS etc. The potential uses and critical data of these innovative applications create security and spectral coexistence challenges.

IV. WSN Protocols

To understand WSN operation and the security techniques which help to overcome the vulnerabilities outlined in section III, the protocols which govern the operation of these networks must be analyzed. Multiple protocols are used in WSNs and the main available technologies include ZigBee, WirelessHART, ISA100.11a, 6LoWPAN, Thread and MiWi. Presently, these protocols are used in applications as mentioned in section II and are the most prominent participants of the expansion of the IoT. The common aspect across these protocols is using the IEEE 802.15.4 [10] standard as the fundamental network infrastructure, on which the more complex networks are formed. This standard originated in 2003 and has undergone various amendments over the years and, here, the focus is on both the 2006 revision and IEEE 802.15.4e. Typically, the standard defines the physical (PHY) and media access control (MAC) layers of Low-Rate Wireless Personal Area Networks (LR-WPANs), which describes WSNs. Three possible operating RF bands (868/915/2450 MHz) are provided, which use different modulation schemes, support various data rates and offer different topologies and security suites.

Here, the security analysis concentrates on the $2450 MHz$ band, which operates in the unlicensed ISM band, and the IEEE 802.15.4 PHY and MAC layers. This area of the RF spectrum is highly congested due to varying high numbers of connected devices, potentially, running different protocols at the same frequency, location and time. This level of congestion requires efficient use of the spectrum and this aspect is experimentally visualized using Tektronix's digital phosphor (DPX) technology and a real time spectrum analyzer in Fig. 6. Securing ISM band signals becomes increasingly complex due to these levels of coexistence and congestion combined with the rapid ability of the spectrum to change due to the number of connected devices, demand, packet size or services in operation. This coupled with the varying nature of the networks physical environment, it becomes clear that WSN security must contend with both malicious and unintentional interference and intrusions.

A. IEEE 802.15.4 PHY

The IEEE 802.15.4 PHY layer (Fig. 3) has specifications as per Table I and 16 available 2 MHz wide channels ranging from $2405 \rightarrow 2483.5 MHz$. Each specific center frequency is calculated using (1), where F_c and i are the center frequency and channel number respectively. This PHY uses direct sequence spread spectrum (DSSS) to split each outgoing byte into two 4-bit symbols, four most significant bits (MSB) and four least significant bits (LSB). Each symbol is spread to a 32-bit pseudo-noise (PN) sequence from a predefined mapping table of 16 PN codes and this process is visualized in Fig. 4. The chip sequences are modulated using offset quadrature phase shift keying (O-QPSK) with half sine shaping. This signal was examined under normal operation by simulating the bit error rate (BER) over a zero mean additive white Gaussian noise (AWGN) channel for a range of energy-per-bit-to-noise (E_b/N_o) ratios and results are shown in Fig. 5. The packet error rate (PER) was incorporated by using a predictive approach calculated using the probability of receiving an incorrect symbol (P_e), given 16 different DSSS PN codes transmitted in an AWGN channel. Assuming a matched filter receiver the symbol error probability can be expressed as (2) and the PER estimated using (4) and provided in Fig. 5, where σ is the variance, $erf()$ is the error function, L is the number of codes and N_{Bytes} is the total bytes per packet.

The general PHY packet structure, known as PHY protocol data unit (PPDU), is provided in Table II, where the MAC frames passed to the PHY are enclosed in the PSDU. The SHR contains a preamble, which allows receivers to synchronize and lock onto the packet bit stream, and the start frame delimiter (SFD), which marks the end of the preamble and start of data. These values are predefined, for example, in ZigBee the preamble sets all 4 bytes set to $0x00$ and the SFD is $0x7A$. The PHR contains the number of bytes in the payload, including the 2 byte frame check sequence (FCS). The maximum IEEE 802.15.4 packet size is $133 bytes$, including all headers, but some radios, like the CC2420, allow the preamble to be increased to $17 bytes$ [11]. From a security perspective, the FCS and any encryption is on the PSDU payload, meaning the headers are minimally protected.

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

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

TABLE I
IEEE 802.15.4 PHY Parameters

Parameter:	2.4 GHz PHY Value:
Data Rate	$250kbps$
Number of Channels	16
Channel Spacing / Width	$5MHz$ / $2MHz$
Pulse Shaping	Half Sine/Normal Raised Cosine
Spreading	DSSS
Chip Rate	$2Mchipsps$
Modulation	O-QPSK

TABLE II
IEEE 802.15.4 PHY Frame Layout

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

$$\sigma = \sqrt{\frac{1}{2E_bN_o}} \tag{3}$$

$$PER = 1 - (1 - P_e)^{2*N_{Bytes}} \tag{4}$$

B. IEEE 802.15.4 MAC

Primarily, the MAC layer allows multiple devices to use the same physical radio channel by employing carrier sense multiple access with collision avoidance (CSMA/CA) [11]. Prior to transmitting a packet, devices performs a clear channel assessment (CCA) to ensure the channel is available. This decision is based on either energy detection, which uses the received channel energy to compare against a predetermined maximum threshold, or carrier sense, which identifies the occupying signal and if an IEEE 802.15.4 signal is sensed, then the channel may be busy even if the energy threshold is not exceeded. If the channel is busy, devices back off for a random period and try again up to a user-defined maximum number of retries. Two modes of operation are used: beacon-enabled and beaconless. In beacon-enabled mode, the coordinator transmits regular beacons used for synchronization and communication control. A superframe, which is divided into equal slots, is used to synchronize data transfer between devices and the coordinator by identifying active and inactive periods. Communications take place during the active period, which may consist of a contention access period (CAP) and a contention free period (CFP). Nodes enter low-power mode during the inactive period. In a CAP all devices use slotted CSMA/CA and the first device that identifies channel availability starts transmitting. A CFP uses guaranteed time slots (GTS) and occurs at the end of the active period, which is immediately after a CAP. In the beaconless approach, communications use unslotted CSMA/CA and the PAN coordinator does not transmit beacons, which means devices cannot be synchronized with one another and no GTS exist. Acknowledgment frames are sent without using CSMA/CA and are not encrypted [12].

The general IEEE 802.15.4 MAC data packet is provided in Fig. 7 and shows how the PSDU encloses the MAC protocol data unit (MPDU). The MHR contains information such as addressing and security, the payload includes data or commands and the FCS is an error detecting code used as a security

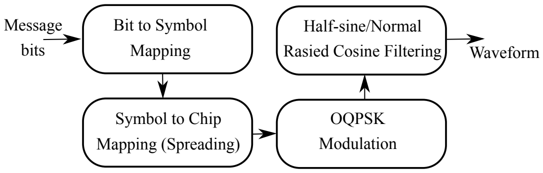
Message bits
Bit to Symbol Mapping
Half-sine/Normal Rasied Cosine Filtering
Waveform
Symbol to Chip Mapping (Spreading)
OQPSK Modulation

Fig. 3. Flow graph defining IEEE802.15.4 2.4GHz PHY

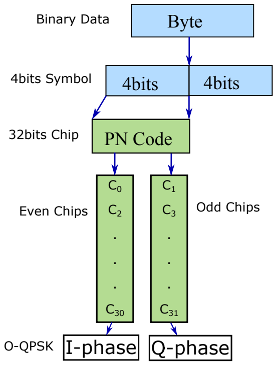

Fig. 4. A flowchart visualizing the spreading of each byte

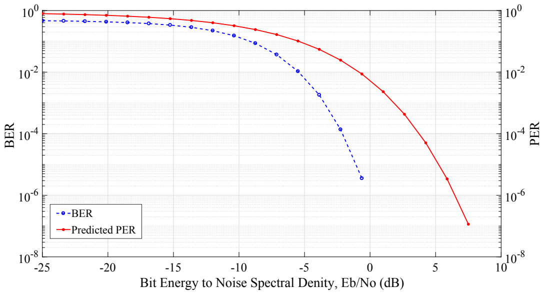

Fig. 5. Simulated IEEE 802.15.4 O-QPSK 2450 MHz BER Curve & associated predicted PER for a AWGN channel for a range of E_b/N_0

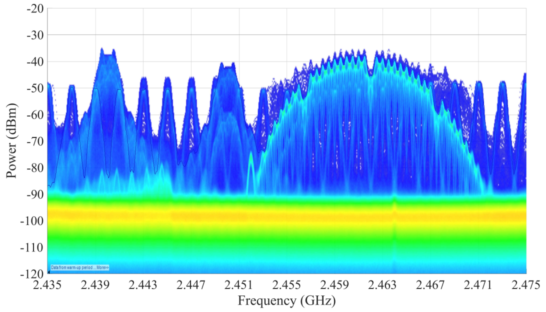

Fig. 6. An IEEE 802.15.4 signal (ZigBee) coexisting with WiFi, Bluetooth & another separate ZigBee signal

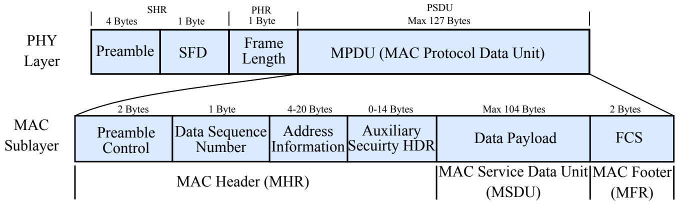

Fig. 7. An expanded MAC sublayer view of the PSDU

technique for data verification. The auxiliary security header is optional and incorporates information required for security processing [13]. Similarly, the MSDU encompasses the network frame and the network payload encases the application frame, which incorporates a message integrity code. Other MAC frames which exist are the beacon, acknowledgment and command frames, which are explained in detail in [14].

V. Security

Security defines various characteristics, which protect a network from interference, especially when sensitive information is being transmitted, ensures privacy and permits safety and reliability. Therefore, certain operating goals are required and these essential elements of security are as follows:

1) Confidentiality: The secrecy of critical transmitted data in the wireless channel must be maintained by keeping the contents from all but those authorized to have it. Critical parts of the transmitted packets are encrypted prior to transmission such that only authorized nodes can decipher them. A strict key management system is essential as privacy attacks can be used to degrade confidentiality and can include eavesdropping and tampering.
2) Authentication: For the authenticity of packets, the receiving node should be able to autonomously assert that the received packet has not been modified in transit (data integrity), and it should also be capable of asserting from which node the packed originated (origin authenticity). Traditional cryptographic schemes such as digital signatures can simultaneously provide both functionalities.
3) Availability: WSNs need to provide services whenever they are required, resulting in a need to exhibit qualities of robustness against a variety of impairments, both benign and malicious. Some degree of resilience (i.e. the ability to recover from faults), diagnostics (i.e. if services become unavailable, it should be possible to identify why), or mitigation (packet re-routing, channel switching) is necessary.
4) Energy: In WSNs, energy is a key security concept as it is a limited resource and must be optimized on each device. This affects the ability to ensure each basic security concept and the use of computationally heavy algorithms.

WSN protocols in use are susceptible to various attack styles due to both the vulnerabilities in section III and incentives created by the application areas. As the dependency on transmitted information increases, the potential risk of privacy and safety being compromised due to an attack rises. These WSN intrusions are the largest contributor to link and path problems and resulting packet losses can lead to avalanche effects and potential network collapse [15]. Thus, techniques are employed in WSN protocols to protect important information and add resilience to attacks. However, it is likely improvements are required because of the evolving nature of both attack styles and WSN deployments. Below, the main security techniques used in IEEE 802.15.4 are discussed.

- DSSS: This spreading technique provides resilience to interference. Every4 bits is spread to one of 16 predefined 32 bit PN codes, which increases system redundancy because the codes are chosen so that the resulting signal is noise-like. Therefore, there should be approximately equal number of ones and zeros in the spreading code and few to no repeated patterns. This method provides immunity from various kinds of noise, multi-path distortions and jamming and grants security as only recipients who know the spreading code can recover the encoded information. Essentially, certain bit errors can occur, while maintaining correct reception at the receiver by utilizing maximum correlation through, for example, a maximum likelihood decoder.
- Frequency Hopping was added to the IEEE 802.15.4e amendment to increase robustness against external interference and persistent multi-path fading. Multiple available channel are used and only network nodes know the pattern.
- A FCS is an error detecting code used to detect changes in the received raw data. The blocks of data being transmitted get a $checkvalue$ attached based on the remainder of a polynomial division on their contents. In IEEE 802.15.4, the contents refer to the PSDU, exposing the preamble. On reception of the raw bits, the calculation is repeated and if the check values do not match, the packet is corrupt.
- Cryptography: To stop intruders accessing sensitive information by simply listening to transmitted messages, data is encrypted before transmission. This provides data confidentiality as the message is modified using a string of bits known as the security key and, theoretically, only the intended user can recover the original message. IEEE 802.15.4 only encrypts the MAC payload [12] and supports the advanced encryption standard (AES) and so, security depends on the predistribution, initialization, use and storage of the keys.
- Message Integrity Code (MIC): This approach protects against intruders modifying and resending messages, even if the packets are encrypted. By including a MIC with each transmitted message, data authentication is achieved because a confirmation of who transmitted the message is achievable.

VI. Exploitation

The aforementioned IEEE 802.15.4 protocol and its associated security techniques are susceptible to exploitation through different attack styles [16]. For example, a specific denial of service (DoS) attack aims to increase the probability of error, P_e , to one. Thus causing packet losses and, potentially, node links to collapse, nodes to become unreachable and network failure. Privacy attacks pursue the interception of sensitive data to degrade a network or for more threatening actions. For convenience, certain WSN attacks are categorized as follows:

- Conventional jamming attacks, typically, aim to overpower legitimate signals with spurious RF transmissions. While higher jamming power increases effectiveness, it is also easier to detect, as such, adversaries typically operate to optimize the interference signal to maximize packet loss while minimizing total broadcast power. Examples include, constant, deceptive, reactive and intelligent jammers.
- MAC layer attacks react to the network protocol in use by eavesdropping or sniffing on transmitted packets. The analyzed results are used to implement network specific attacks including replay attacks, spoofed packets, matched protocol interference [9] or forcing a device to remain in listening mode, which exploits CSMA/CA. Replay attacks should be negated by the use of MIC, however due to hostile deployment scenarios secrets may be accessible.
- Network layer attacks, generally, cause a DoS, a privacy or an impersonation attack and include selective forwarding, sinkhole, blackhole, Sybil and HELLO flood attacks.
- System coexistence is an innovative approach for attacking WSNs. The ISM band is unlicensed and incorporates various protocols as shown by the Tektronix DPX acquisition in Fig. 6. The coexisting legitimate signals can attack a WSN [11] when, for example, a secondary user (SU) occupying a primary user's (PU) spectrum causes interference or when a specific user consumes all resources and deliberately denies spectrum sharing.

Due to identified unique vulnerabilities and security holes, the above attack approaches can be applied to the employed security technique in IEEE 802.15.4 by using COTS hardware and open source software. Currently available COTS devices are becoming cheaper and more computationally powerful, which allows various attacks to be implemented from a single device. SDRs combined with open source software, like GNU Radio, can apply various interference and privacy attacks by using signal processing blocks and can mimic legitimate signals and packet structures by exploiting known WSN protocol designs and bitstreams [9]. Receiving capabilities can support attacks on specific frame sections, where certain security measures are unimplemented. For example, listen for SHR and focus attack on the PHR, thereby, affecting the frame length and, likely, causing inaccurate packet reception. SDRs or sniffers (TI's CC2531EMK) can monitor a node joining process where, potentially, encryption keys are disclosed or can replay modified/unmodified packets. Notably, for WSNs, devices can be both physically and/or commercially available, leading to the possibility of gaining network access through key extraction from memory, specially when no key management system is in use. In addition, without the use of forward error correction, packets are more unreliable over noisy or hostile communication channels, which aides the process of intrusion by coexistence. Therefore, by using both WSN knowledge and available COTS devices, specific aspects of protected networks can, potentially, be compromised. This clearly shows that exploiting WSNs is possible, even when security techniques are used and improvements are required.

VII. Conclusion

This paper concentrated on WSN security by analyzing implemented network devices, deployment environments, ISM coexistence and the IEEE 802.15.4 standard. Defining the diversity of innovative solutions requiring a WSN approach expands the array of applications and deployment areas, most notably the IoT, and incentivizes attackers. Unique WSN vulnerabilities exist and have repercussions for providing adequate levels of security. These vulnerabilities and essential security operating goals were analyzed by focusing on the fundamental use of the IEEE 802.15.4 standard in WSN protocols and its associated PHY and MAC layer security techniques. An experimental visualization of the ISM RF band coexistence issues demonstrated additional complexity when providing security. This paper indicated the existence of security holes in the standardized IEEE 802.15.4 protocol, notably in terms of preambles and headers, WSN deployments and spectral coexistence. COTS devices and open source software can effectively capitalize on these security holes, providing evidence for establishing WSN security enhancements.

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] S. R. J. Ramson and D. J. Moni, "Applications of Wireless Sensor Networks - A Survey," in *IEEE International Conference on Innovations in Electrical, Electronics, Instrumentation and Media Technology*, 2017, pp. 325–329.

[4] 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.

[5] 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.

[6] C. Dragana, G. Stamatescu, L. Ichim, and D. Popescu, "Interlinking Unmanned Aerial Vehicles with Wireless Sensor Networks for Improved Large Area Monitoring," in *International Conference on Control, Decision and Information Technologies*, 2017, pp. 359–364.

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

[8] 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.

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

[10] IEEE, *IEEE Standard for Low-Rate Wireless Networks*, 2015.

[11] G. Shi and K. Li, "Signal Interference in WiFi and ZigBee Networks," 2017.

[12] I. Tomi and J. A. Mccann, "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.

[13] S. Farahani, *ZigBee Wireless Networks and Transceivers*, 2008.

[14] A. Reziouk, E. Laurent, and J.-C. Demay, "Practical security overview of IEEE 802 .15 .4," *International Conference on Engineering & MIS (ICEMIS)*, pp. 1–9, 2016.

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

[16] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 74–81, 2008.