Hindawi Publishing Corporation
Journal of Electrical and Computer Engineering
Volume 2016, Article ID 7165952, 12 pages
http://dx.doi.org/10.1155/2016/7165952

Review Article

A Comprehensive Taxonomy and Analysis of IEEE 802.15.4 Attacks

Yasmin M. Amin and Amr T. Abdel-Hamid

Department of Networks Engineering, German University in Cairo, Cairo 11835, Egypt

Correspondence should be addressed to Yasmin M. Amin; yasminmahmoudamin@hotmail.com

Received 30 October 2015; Revised 10 June 2016; Accepted 27 June 2016

Academic Editor: Vinod Sharma

The IEEE 802.15.4 standard has been established as the dominant enabling technology for Wireless Sensor Networks (WSNs). With the proliferation of security-sensitive applications involving WSNs, WSN security has become a topic of great significance. In comparison with traditional wired and wireless networks, WSNs possess additional vulnerabilities which present opportunities for attackers to launch novel and more complicated attacks against such networks. For this reason, a thorough investigation of attacks against WSNs is required. This paper provides a single unified survey that dissects all IEEE 802.15.4 PHY and MAC layer attacks known to date. While the majority of existing references investigate the motive and behavior of each attack separately, this survey classifies the attacks according to clear metrics within the paper and addresses the interrelationships and differences between the attacks following their classification. The authors' opinions and comments regarding the placement of the attacks within the defined classifications are also provided. A comparative analysis between the classified attacks is then performed with respect to a set of defined evaluation criteria. The first half of this paper addresses attacks on the IEEE 802.15.4 PHY layer, whereas the second half of the paper addresses IEEE 802.15.4 MAC layer attacks.

1. Introduction

The IEEE 802.15.4 standard [1] has become the dominant enabling technology for WSNs. WSNs are networks of a large number of tiny sensor devices which target applications in a diverse set of fields, particularly military, healthcare, residential, transport, and industrial fields to name a few. Such applications require very low data rates and relaxed Quality of Service (QoS) requirements over short ranges for wireless devices with very small sizes [2].

Many applications involving WSNs are security-sensitive and possess zero tolerance for error and latency. While error and latency can occur due to network failure and congestion, they can also be triggered by malicious behavior. For instance, eavesdropping on confidential information exchange or injecting false information in battlefield monitoring applications can have severe consequences and can lead to injuries or at worst fatalities. Another example is Home Area Networks (HANs) in smart grids [3], in which adversaries can manipulate data transfer among smart meters and household electric appliances, for the purpose of manipulating control signals transmitted to targeted appliances or modifying billing and payment information, either in favor of or against the customer to whom the HAN belongs. Wireless Body Area Networks (WBANs) monitor human body functions and the surrounding environment and can lead to dangerous conditions or even death of patients in case of security threats. Also attacks launched against home Intrusion Detection Systems (IDSs) might cause home owners to be informed of the presence of intruders after significant delay at best or may cause intruder alarms to be overlooked altogether at worst.

IEEE 802.15.4 defines the Physical (PHY) and Media Access Control (MAC) layer specifications of Low-Rate Wireless Personal Area Networks (LR-WPANs) [1]. Since the PHY and MAC layers are considered as the base for any WSN [4], they are the main target of most launched attacks and malicious behavior. The primary focus of this paper is on providing a comprehensive classification of the attacks which can be launched on each of the IEEE 802.15.4 PHY

and MAC layers. For each layer, the provided classification is used as the basis for performing a comparative analysis between the attacks. *To the best of the authors' knowledge*, this survey is the first to provide a single reference consolidating all IEEE 802.15.4 PHY and MAC layer attacks known to date. The paper is organized as follows. In Section 2, we describe the operation and purpose of each PHY layer attack and its variants. In Section 3, we present our own two novel classifications of PHY layer attacks. In Section 4, we evaluate the differences between the discussed attacks based on a set of defined evaluation criteria. Sections 5, 6, and 7 are reiterations of Sections 2, 3, and 4 respectively, but for IEEE 802.15.4 MAC layer attacks instead. In Section 5, we also identify a new variant of the *GTS Attack*. In Section 6, we present two significant classifications of MAC layer attacks, collectively obtained from external references, along with our own additions to these existing classifications. Section 8 concludes the paper.

2. Attacks on IEEE 802.15.4 PHY Layer

This section explains the purpose and operation of the attacks which can be launched by a malicious adversary against the PHY layer of an IEEE 802.15.4-based network. We refer to the different methods of launching the same attack as the attack's *variants*, and we discuss how an attack's variants can be conducted. We assign names for attacks which have not previously been named in existing literature.

2.1. Radio Jamming. *Radio Jamming* [5] is a PHY layer attack which is launched with the intent of creating a Denial of Service (DoS) against the network. This attack achieves its purpose through the intentional emission of radio signals in order to decrease the Signal to Noise Ratio (SNR) of ongoing radio communications [3], thus disrupting the reception of messages at network nodes.

Sokullu et al. [6] identify four approaches to *Radio Jamming*, which are *Constant*, *Deceptive*, *Random*, and *Reactive Jamming*. Jokar et al. [3] classify Radio Jamming attacks into *Wide-Band Denial*, *Pulse-Band Denial*, and *IEEE 802.15.4-Specific Interruption Denial*. O'Flynn [4] extends the Radio Jamming attacks defined in Jokar et al. [3] by defining two additional attacks, which are *Node-Specific Denial* and *Message-Specific Denial*. Wood et al. [5] divide Radio Jamming into *Interrupt*, *Activity*, *Scan*, and *Pulse Jamming*. Balarengadurai and Saraswalhi [7] distinguish between *Signal*, *Radio*, and *Noise Jamming*. In our opinion, we consider *Signal* and *Noise Jamming* to be the same as *Radio Jamming*, as they possess the same intent and characteristics as *Radio Jamming*. This subsection discusses all of the *Radio Jamming* attacks explained in [3–7].

2.1.1. Wide-Band Denial. This jamming attack transmits radio interference signals with high transmission power over all channels of the related frequency band. This can be achieved either through continuous transmission of a jamming signal over the entire frequency band [3] or by using channel hopping in conjunction with single-channel Pulse Jamming, also known as *Pulse-Band Denial*, in order to emit pulse signals with short time periods on each and every single 802.15.4 channel before moving on to and repeating the same procedure in the successive channel. *Wide-Band Denial* causes DoS against the network by blocking the whole Radio Frequency (RF) spectrum, which in turn leads to the corruption of all ongoing transmissions [4].

2.1.2. Pulse-Band Denial. In contrast to *Wide-Band Denial*, Pulse-Band Denial targets a single channel rather than all channels within the related frequency band. For this reason, this method is also known as single-channel Pulse Jamming. A malicious adversary can use *Pulse-Band Denial* to prevent legitimate nodes from selecting a particular channel by jamming the target channel during the channel Energy Detection (ED) scan performed by legitimate nodes during the channel selection process. This act of jamming forces the channel to seem unattractive to the nodes, thus coercing the nodes into scanning for other interference-free channels. *Pulse-Band Denial* can be perceived as a misbehavior attack if the adversary not only prevents legitimate nodes from utilizing the target channel, but also selfishly frees up the channel for its own use [4]. We consider the four *Radio Jamming* attacks explained in [6] to be variants of *Pulse-Band Denial*, as shown in Figure 1. This is because the adversary targets a single channel in each of these four variants, as is the case with *Pulse-Band Denial*. These four variants differ with respect to the recurrence of the emitted jamming signal within the target channel.

(a) Constant Jamming. In this variant, a radio signal is continuously transmitted over the target channel [6].

(b) Deceptive Jamming. Similar to *Constant Jamming*, *Deceptive Jamming* involves continuous channel jamming. However, while the former involves the continuous transmission of radio signals over the target channel, an adversary performing the latter emits regular frames over the target channel [6].

(c) Random Jamming. This variant is performed by jamming the target channel at random times, either using a constant radio signal (as in *Constant Jamming*) or using regular frames (as in *Deceptive Jamming*) [6].

(d) Reactive Jamming. A reactive jammer only starts jamming the target channel when it senses ongoing network activity over the channel [6]. There are several ways for a malicious adversary to detect activity within the network. For this reason, we subdivide *Reactive Jamming* into five variants extracted from [4, 5], depending on how an adversary detects activity within its target network, as illustrated in Figure 1. For some of these variants, the adversary initiates jamming only when detected network activity includes frames of a specific nature, destination, or type:

(i) *Interrupt Jamming.* It is also known as *IEEE 802.15.4-Specific Interruption Denial* [4]: this variant triggers channel interference by the adversary only when IEEE 802.15.4 traffic is detected over the target channel.

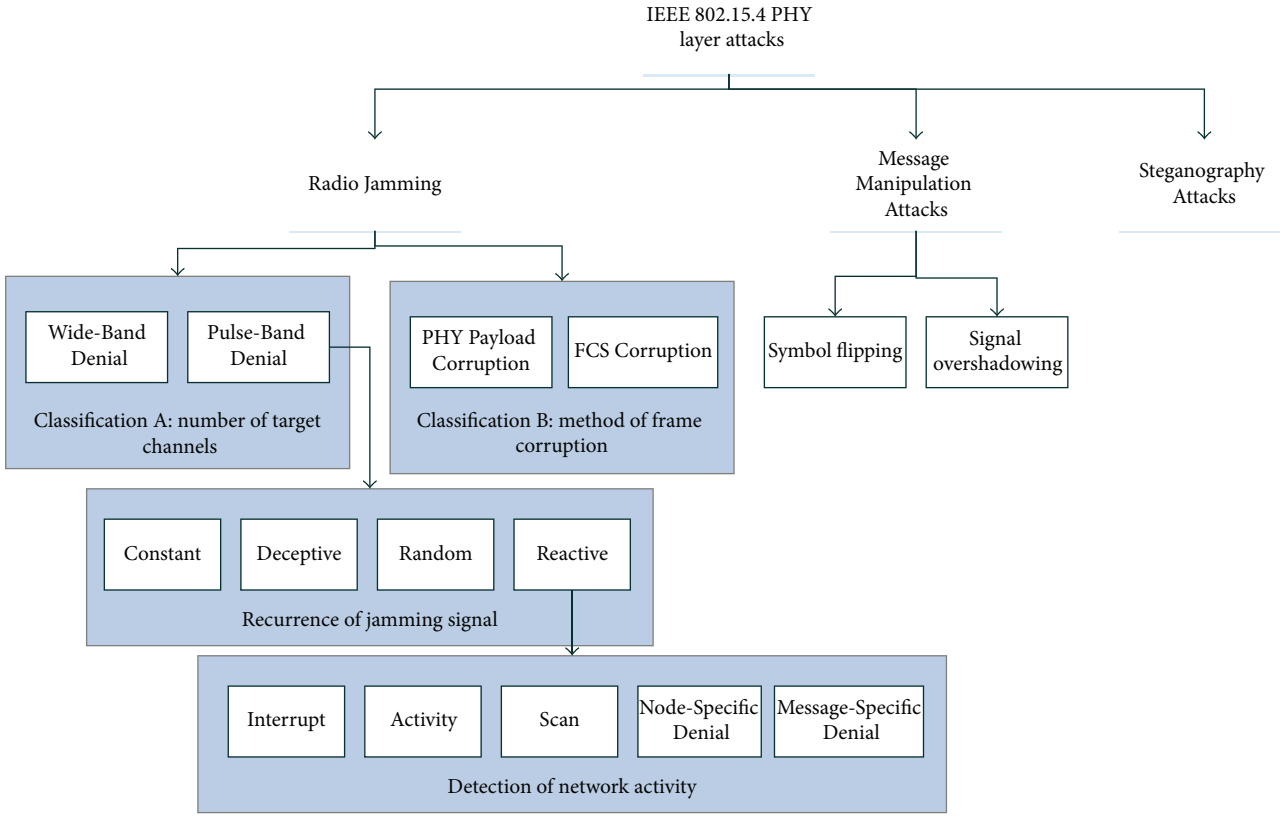

Figure 1: Classification of IEEE 802.15.4 PHY layer attacks.

While awaiting frame reception, the adversary's radio constantly scans for a preamble and a Start of Frame Delimiter (SFD), both of which precede the payload of a PHY frame. Upon their detection, the adversary starts transmitting a jamming frame in order to interfere with the ongoing transmission of the legitimate frame over the channel. Wood et al. [5] explain the use of frame masking as a defense against Interrupt Jamming. Frame masking is a mechanism which generates a secret pseudorandom sequence, which is agreed upon by sender and receiver, to be used for the SFD field in each frame. In this way, an adversary's radio will not be able to scan for a fixed SFD because the SFD now differs for each transmitted frame between sender and receiver. As such, launching an interrupt attack will not be possible [5].

(ii) *Activity Jamming.* Unlike *Interrupt Jamming*, an adversary does not need to know the value of each frame's SFD in order to launch an *Activity Jamming* attack. Rather, the adversary periodically samples the Radio Signal Strength Indicator (RSSI) or the radio's Clear Channel Assessment (CCA) output in order to detect the presence of network activity. Network activity is confirmed if the RSSI value is above a predefined threshold. Upon activity detection, the adversary initiates jamming. One defense mechanism suggested by Wood et al. [5] against *Activity Jamming* is channel hopping. An adversary can only sample RSSI or CCA for the channel on which its radio is listening. If a sender and receiver agree upon a secret pseudorandom channel sequence, they can use that sequence to hop between similar channels, thus leaving the adversary behind [5].

(iii) *Scan Jamming.* This *Reactive Jamming* variant enables an adversary to break the defense of the channel hopping mechanism by allowing the adversary to scan all channels within the frequency band before the termination of a single frame transmission from sender to receiver. Each time the adversary hops over to a new channel, it uses RSSI or CCA sampling, as in *Activity Jamming*, to determine if a frame is being transmitted on the current channel. If frame transmission is detected, the adversary begins jamming. If the channel is determined to be idle, the adversary hops over to the next channel in the frequency band. This attack variant can be overcome by fragmenting each frame and transmitting the different fragments on different channels with different SFDs [5].

(iv) *Node-Specific Denial.* In this *Radio Jamming* variant, an adversary only jams frames which are destined for specific target nodes. This is achieved by examining the addressing information contained in the MAC header of the ongoing data frame [4].

(v) *Message-Specific Denial. Message-Specific Denial* is quite similar to *Node-Specific Denial*, with the difference being that the adversary only jams frames of a specific type rather than a specific destination address. The type of the frame can be known by examining the frame type field of the transmitted frame's MAC header [4].

2.2. Message Manipulation Attacks. These attacks are used by adversaries to inject false data into the network by transforming a legitimate data frame into a modified frame containing information of the adversary's choice. Wilhelm et al. [8] explain that frame manipulation can be accomplished using one of the following two techniques.

2.2.1. Symbol Flipping. An adversary can emit RF waves whose amplitude and phase are synchronized with those of the original transmitted signal. If these RF waves are combined with the original signal at the correct time, this leads to a new signal containing the falsely injected data. This technique is referred to as *Symbol Flipping* [8].

2.2.2. Signal Overshadowing. This technique is used in conjunction with angular modulation schemes, in which only the stronger of two colliding signals is received. While *Symbol Flipping* is highly sensitive to the physical properties of the original transmitted signal, Signal Overshadowing overcomes this limitation. However, *Signal Overshadowing* is still concerned with tight timing and phase synchronization requirements from a technical, as opposed to a physical, perspective [8].

2.3. Steganography Attacks. Martins and Guyennet [9] explain how attacks can be performed on the PHY and MAC layers of the 802.15.4 protocol using steganography. In a general context, steganography is used to hide the existence of data. This is accomplished by embedding secret data within existing data, known as cover data, thus resulting in a stegomessage. Data can be hidden in 802.15.4 networks by using the PHY header field of PHY frames. The PHY header field is one byte long, with only seven used bits and one reserved bit. The eighth reserved bit within the PHY header field can be used to transmit one bit of an intended stegomessage per PHY frame. A receiver which is aware of the existence of the stegomessage reads every hidden bit of all sent frames until it recovers the entire stegomessage. *Steganography Attacks* create a hidden channel between collaborating adversaries in the network, which opens up endless opportunities for adversaries. For instance, the hidden channel could be used by adversaries to exchange information regarding the execution of new attacks in the network. Moreover, adversaries could use the hidden channel to monitor the network and warn each other when the network detects or senses launched attacks. The latter enables adversaries to stop executing their attacks just in time to remove suspicions and prevent detection by the network. *Steganography Attacks* can also be launched by hiding information within the MAC fields of the 802.15.4 protocol [9].

3. Classification of IEEE 802.15.4 PHY Layer Attacks

While [3–7] focus on explaining the operation, intent, and impact of each of the *Radio Jamming* attacks individually, we provide our own two novel classifications in order to illustrate the dependencies and interrelationships between these attacks, as illustrated in Figure 1. It is important to note that the two presented classifications only consider *Radio Jamming* attacks. *Message Manipulation* and *Steganography Attacks* are not considered.

3.1. Classification A. In this classification, we define two broad categories of *Radio Jamming* attacks with respect to the number of target channels within the related frequency band over which jamming signals are transmitted. *Wide-Band Denial* targets all channels within the related frequency band, whereas all variants of *Pulse-Band Denial* target a single channel.

3.2. Classification B. This classification classifies attacks with respect to the fields of the transmitted frame which are corrupted due to adversary jamming. We infer from O'Flynn [4] that each of the *Radio Jamming* attacks explained in the previous section can corrupt a data frame using one of the following two techniques.

3.2.1. PHY Payload Corruption. In this method, the adversary aims to jam a few or all bytes of the PHY payload, thus corrupting the frame and indirectly leading to an incorrect Frame Check Sequence (FCS) at the receiver. Upon frame reception, the receiver discards the frame due to its incorrect FCS [4].

3.2.2. FCS Corruption. Contrary to *PHY Payload Corruption*, *FCS Corruption* involves the direct jamming of one or both bytes of the frame's two-byte FCS field while leaving the PHY payload as it is. This still leads to the received frame not being accepted by the receiver node [4].

It is worth noting that, for each of the two aforementioned frame corruption techniques, an adversary is able to detect the point in time at which the transmission of a frame's PHY payload or FCS starts by examining the frame's PHY layer header, which contains the length of the transmission frame. The frame content targeted for corruption by the adversary depends on the point in time at which the adversary starts emitting jamming energy, as well as how long the adversary continues to jam throughout the entire duration of frame transmission [4].

4. Comparative Analysis of IEEE 802.15.4 PHY Layer Attacks

In this section, we first define the criteria which will be used to evaluate each of the PHY layer attacks discussed in the previous section. Following this, we perform a detailed comparison between the attacks with respect to the defined evaluation criteria.

Table 1: Comparative analysis of IEEE 802.15.4 PHY layer attacks.

Attack	Energy efficiency	Effectiveness	Stealthiness	Primary security goals	
				Integrity	Availability
Wide-Band Denial	Low [3]	High	Low [3]		
Constant Jamming	Low [6]	High	Low [6]		
Deceptive Jamming	Low [6]	High	Moderate [6]		
Random Jamming	Moderate [6]	Moderate [6]	Moderate [6]	×	√ [7]
Interrupt Jamming	High [5]	High [5]	High [4]		
Activity Jamming and Scan Jamming	Moderate [5]	High	Moderate [5]		
Node-Specific Denial and Message-Specific Denial	High	High	High		
Message Manipulation Attacks	No enough information			√ [8]	×
Steganography Attacks	Dependent			×	×

4.1. Evaluation Criteria. We define four criteria for the purpose of PHY layer attack evaluation.

4.1.1. Energy Efficiency. An adversary launching an energy-efficient attack consumes minimum energy in order to disrupt network communications, thus preventing drainage of the adversary node's limited battery power [5].

4.1.2. Effectiveness. An effective attack is one that yields maximum disruption of network communications throughout the length of its deployment.

4.1.3. Stealthiness. A stealthy attack is an unintrusive attack which is launched with minimum probability of detection by the network [5].

4.1.4. Security Goal Violation. Security goals are used to assess a WPAN's level of security. Kumar et al. [10] define two classes of security goals: primary and secondary. Since no secondary goals are violated by any of the discussed attacks, we only focus on primary security goals.

4.2. Comparison between IEEE 802.15.4 PHY Layer Attacks. Table 1 compares between the IEEE 802.15.4 PHY layer attacks with respect to energy efficiency, effectiveness, stealthiness, and the primary security goals violated by each attack. Unreferenced entries in Table 1 indicate our own suggestions and inferences.

It is noted that Table 1 exhibits a direct proportionality between energy efficiency and stealthiness for almost all of the discussed PHY attacks. In other words, the lower the amount of energy consumed by an adversary during the attack (the higher the energy efficiency), the lower the probability of attack detection by the network within which the attack is launched (the higher the stealthiness).

4.2.1. Energy Efficiency, Effectiveness, and Stealthiness. The differences between the discussed IEEE 802.15.4 PHY layer attacks with respect to energy efficiency, effectiveness, and stealthiness are as follows.

(a) Radio Jamming. The following observations for all *Radio Jamming* attacks and their variants with respect to the above three evaluation criteria are noteworthy.

(i) *Wide-Band Denial. Wide-Band Denial* is not an energy-efficient attack because an adversary consumes a relatively large amount of power in order to constantly transmit jamming signals of high power over the entire frequency band. On the other hand, this attack is considered to be highly effective at disrupting network communications because it spans all channels of the related frequency band. Since a continuous jamming signal is present, this attack is very unstealthy and easy to detect [3].

(ii) *Constant Jamming.* Recall that the *Constant Jamming* variant of *Pulse-Band Denial* targets only a single channel within the frequency band. If all devices within the attacked network are expected to operate within a single common frequency channel, then the energy efficiency, effectiveness, and stealthiness characteristics of this attack converge to those of *Wide-Band Denial*.

(iii) *Deceptive Jamming.* This *Pulse-Band Denial* variant is as energy-efficient and as effective as *Constant Jamming* but is slightly more difficult to detect. This is because the deceptive use of packets instead of radio signals for the purpose of jamming confuses the receiver as to whether the received packets are being sent by a legitimate or illegitimate network node [6].

(iv) *Random Jamming.* By randomly alternating between sleeping and jamming modes, the *Random Jamming* variant of *Pulse-Band Denial* saves more energy, thus making it stealthier than its previous counterparts. The fact that jamming is no longer a continuous occurrence makes *Random Jamming* more effective and harder to detect [6].

(v) *Interrupt Jamming.* In this variant of *Reactive Jamming*, an adversary only starts jamming upon detection of a frame's preamble and SFD, making it a highly energy-efficient attack. Despite its low energy consumption, *Interrupt Jamming* is still highly effective,

as an adversary only enters sleep state in the absence of radio activity [5]. *Interrupt Jamming* is very difficult to detect because jamming never extends beyond the length of frame transmission [4].

(vi) *Activity and Scan Jamming.* Due to their reliance on RSSI and CCA output, these two *Reactive Jamming* variants are known for displaying high rates of false positives in detecting network activity. False positives result either from the detection of channel noise or from the high latencies incurred by RSSI and CCA mechanisms in detecting channel activity. Channel noise detected by RSSI and CCA mechanisms can be either background noise or noise resulting from channel access contention over channels which are common between IEEE 802.15.4 Wireless Personal Area Networks (WPANs) and 802.11 Wireless Local Area Networks (WLANs). In order to compensate for this inaccurate detection of network activity, an adversary launching either attack must transmit more frequent jamming signals, thus consuming more energy and increasing the probability of detection [5]. Since Wood et al. [5] do not mention the possibility of false negative generation by *Activity* and *Scan Jamming*, it is safe to assume that network activity is always detected by both variants. From this, we infer that *Activity* and *Scan Jamming* are both highly effective at disrupting network communications.

(vii) *Node-Specific and Message-Specific Denial.* For these two *Reactive Jamming* variants, jamming is only initiated upon detection of a frame whose header indicates a specific destination address or frame type. As such, we consider both variants to be very energy-efficient. We also infer that both variants are highly effective at corrupting the targeted traffic and are very difficult to detect for the same reason as *Interrupt Jamming*.

(viii) *PHY Payload and FCS Corruption.* The reason for not including these two frame corruption techniques in Table 1 is because we consider them to be methods of launching the *Radio Jamming* attacks shown in Table 1, but they are not actual attacks themselves. Wood et al. [5] argue that energy savings with *FCS Corruption* are greater than with *PHY Payload Corruption*. This is because *FCS Corruption* involves jamming for at most two bytes of the intended frame's FCS field, whereas *PHY Payload Corruption* involves higher energy consumption due to the use of a longer jamming signal for a few or all bytes of the intended frame's payload. In our opinion, both methods of frame corruption are equally effective, as they both intend to directly or indirectly corrupt frame FCS, thus leading to the frame's rejection at the receiver.

(b) Message Manipulation Attacks. Wilhelm et al. [8] do not reveal any information regarding the energy efficiency, effectiveness, or ease of detection of *Symbol Flipping* and *Signal Overshadowing*. However, in the results section of [8], it is stated that *Signal Overshadowing* has a 66.97% success rate in its deployment.

(c) Steganography Attacks. While Martins and Guyennet [9] make no explicit comments on this attack's energy efficiency, effectiveness, and stealthiness, we believe that there exists a tight relationship between these three criteria for this attack. The effectiveness of a *Steganography Attack* depends on the value and length of information exchanged among cooperating adversaries over the created hidden channel, as well as the effectiveness of the attacks launched by cooperating adversaries in response to the exchanged information. Recall that each bit of a secret message is embedded instead of the reserved bit of the PHY header field.

The longer the secret message that needs to be transmitted, the larger the number of frames exchanged over the network. Exchanging a larger number of frames leads to shorter lifetime of malicious adversaries due to higher energy consumption, in addition to higher probability of detection due to abnormal activity monitored by the network. Energy efficiency of PHY layer *Steganography Attacks* can be improved by transmitting some bits of a secret message in both PHY and MAC fields of transmitted frames, thus reducing the total number of exchanged frames [9].

4.2.2. Security Goal Violation. With reference to the security goals acquired from Kumar et al. [10], we find that the discussed PHY layer attacks target the violation of only two primary security goals, which are data integrity and network availability.

(a) Radio Jamming. Since all types of *Radio Jamming* attacks are launched with the intent of creating a DoS on the target network, all *Radio Jamming* attacks are considered to violate network availability [7]. A common misconception is that *Radio Jamming* attacks also target the integrity of data transmitted across the network because jamming corrupts, and thus modifies, either the payload or FCS fields of the frame if the modified frame is accepted by the receiver. This is not the case in *Radio Jamming* attacks, because the modified frame is rejected by the receiver due to an incorrect FCS.

(b) Message Manipulation Attacks. Contrary to *Radio Jamming*, *Message Manipulation Attacks* cause the acceptance of a modified message by the receiver, thus violating the integrity of the message [8]. *Message Manipulation Attacks* make no effort to target the availability of network resources.

(c) Steganography Attacks. Similar to *Message Manipulation Attacks*, *Steganography Attacks* do not target the violation of network availability. In our opinion, *Steganography Attacks* are not considered to violate the integrity of network transmissions. This is because adversaries merely use steganography to embed data within unused fields of transmitted frames, but no modifications are made to the existing frame data. This results in a correct FCS and frame acceptance at the receiver. As such, the original content of the frame and hence its integrity are retained.

5. Attacks on IEEE 802.15.4 MAC Layer

This section addresses attacks against the IEEE 802.15.4 MAC layer and is based on the research in [11].

5.1. Link Layer Jamming. Similar to *Radio Jamming* at the PHY layer, *Link Layer Jamming* is a MAC layer attack which is launched with the intent of creating a Denial of Service (DoS) against the network by disrupting the exchange of messages between transmitting and receiving network nodes. While *Radio Jamming* achieves its purpose by creating radio interference through the emission of radio signals, *Link Layer Jamming* involves the emission of packets rather than signals [12]. Two variants of *Link Layer Jamming* can be defined, both of which cause degradation and reduction of network performance and throughput [13]. These two variants differ with respect to the recurrence of packet transmission by the malicious adversary.

5.1.1. Random Jamming (Also Known as Blind Jamming [12]). In this variant, a malicious adversary emits packets of useless content at random time intervals and for no specific purpose. While this variant can be considered as a stand-alone attack, it is also the basis for the *One Random Attacker (ORA)* and *Two Random Attackers (TRA)* scenarios of the *Interference During CFP* variant of the *GTS Attack*, which are explained later.

5.1.2. Intelligent Jamming. An intelligent jammer emits packets of useless content at specific times for specific purposes [12]. In addition to acting as a stand-alone attack, this variant can also be used as the basis for launching more powerful and complicated types of attacks, such as *Acknowledgment (ACK) Attack*, *Man-In-The-Middle (MITM) Attack*, and the *One Intelligent Attacker (OIA)* and *Two Intelligent Attackers (TIA)* scenarios of the *Interference During CFP* variant of the *GTS Attack*, as explained later.

5.2. Node-Specific Flooding. Mišić et al. [13] describe an attack which involves the transmission of unnecessary packets whose destination addresses are set to the addresses of destination nodes targeted by malicious adversaries. The targeted nodes' power sources are eventually depleted due to excessive packet reception from the adversaries.

5.3. Back-Off Manipulation. The Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) [1] channel access mechanism is used to govern the rules for medium contention among network nodes in IEEE 802.15.4 networks. For beacon-less networks, unslotted CSMA-CA is used. For beacon-enabled networks, slotted CSMA-CA is used during the Contention Access Period (CAP) of each superframe duration. A malicious adversary can manipulate CSMA-CA rules in such a way that the adversary constantly uses a short back-off period instead of selecting a random back-off period from its contention window. In doing so, the adversary hijacks channel access by ensuring that it is always granted higher priority to access the channel than legitimate nodes, which use larger back-off periods [6]. This attack increases both waiting time of legitimate nodes during channel access and power consumption of nodes during the reception of adversary data [13].

Mišić et al. [13] mention two variants of *Back-Off Manipulation*, the difference between which is with respect to the methods they use to accomplish the common objective explained above.

5.3.1. Battery Life Extension (BLE) Pretense. BLE mode ensures the conservation of power for nodes operating on battery power. A malicious adversary can take advantage of this CSMA-CA feature by falsely pretending to run in BLE mode in order to acquire a smaller initial contention window size than the other legitimate nodes. This reduces the range of values from which the adversary can select its back-off period and ensures that its probability of accessing the medium is much higher than legitimate nodes.

5.3.2. Constant Back-Off Exponent (BE). A malicious adversary can choose not to increment its BE after a failed transmission attempt. Maintaining a constant BE prevents contention window size from being increased, thus increasing probability of channel access.

5.3.3. Random Number Generator (RNG) Tampering. Another way of increasing the odds of channel access is for a malicious adversary to modify its RNG in such a way that ensures that the back-off periods selected by the adversary are much smaller than those selected by legitimate nodes.

5.3.4. Back-Off Countdown Omission. Mišić et al. [13] describe an attack which involves the complete omission of the random back-off countdown by a malicious adversary. We consider this omission to be the same as the complete omission of the entire CSMA-CA protocol. The effect of this would be the ability of the adversary to transmit its packets more frequently than legitimate network nodes, thus causing collisions between the adversary's packets and legitimate network packets, resulting in the same DoS outcome as *Link Layer Jamming*.

5.4. Clear Channel Assessment (CCA) Manipulation. Mišić et al. [13] describe two attacks which can be launched against the CCA procedure of the CSMA-CA protocol. CCA is the process of initiating packet transmission if the channel is sensed idle for 2 successive back-off periods. Two variants of the CCA Manipulation attack can be defined as follows.

5.4.1. Clear Channel Assessment (CCA) Reduction. In this attack variant, if the adversary senses that the channel is idle for only 1 back-off period (not 2), it initiates packet transmission, giving channel access more quickly and frequently to adversaries than to legitimate network nodes.

5.4.2. Clear Channel Assessment (CCA) Omission. Rather than reducing the number of back-off periods during which CCA is performed, an adversary may choose to omit the

CCA procedure altogether in order to immediately start transmitting whenever the random back-off countdown is over. This could potentially cause collisions if the channel is not idle, leading to a DoS effect as in *Link Layer Jamming*.

5.5. Same-Nonce Attack. Consider a node providing the access control service in secured operating mode. In this case, if two entries within this node's Access Control List (ACL) possess the same key and nonce, a malicious adversary obtaining the cipher texts pertaining to these two entries will be able to infer useful information about the transmitted data, as explained in [6].

5.6. Replay-Protection Attack. Replay-protection is an IEEE 802.15.4 mechanism which causes a node to drop a frame if its sequence number is equal to or less than the sequence number of a preceding frame received by that same node. An adversary can send frames with large sequence numbers to targeted legitimate nodes, causing frames with smaller sequence numbers from other legitimate nodes to be dropped [6].

5.7. Acknowledgment (ACK) Attacks. In IEEE 802.15.4 as well as in other types of networks, ACK frames are sent between network nodes in order to confirm successful frame transmission. For some types of frames, an *Acknowledgment Request* field is present, which is set to 1 if an acknowledgment is required upon frame receipt or 0 if no acknowledgment is required [1].

In this subsection, we explain two variants of the *ACK Attack*.

5.7.1. ACK Spoofing. An adversary can perform *Intelligent Link Layer Jamming*, as described in Section 5.1.2, in order to prevent legitimate data from correctly being received by the receiver. The adversary then sends back a forged ACK on the receiver's behalf with the correct expected sequence number to the sender, thus preventing data retransmission by tricking the sender into thinking that the frame has successfully reached the receiver [3].

5.7.2. ACK Dropping. In this variant, although the transmitted data is correctly received by the receiver, *ACK dropping* uses *Intelligent Link Layer Jamming* to jam the true ACK that is sent back by the receiver to the sender. Unlike *ACK Spoofing*, the malicious adversary sends no forged ACK in place of the jammed ACK. As such, the sender and receiver nodes' power and bandwidth are wasted during retransmissions up to a maximum number of retransmissions [6].

5.8. Man-In-The-Middle (MITM) Attack. This attack is an extension of the *ACK Spoofing* variant of the *ACK Attack* described in Section 5.7.1. Following the transmission of the forged ACK by the adversary to the sender node, the adversary also transmits an altered version of the original data frame to the receiver and receives a true ACK frame from the receiver by pretending to be the original sender. *ACK* and *MITM Attacks* are also referred to as *Interception Attacks* [4].

5.9. Guaranteed Time Slot (GTS) Attacks. In beacon-enabled networks, the PAN coordinator reserves Guaranteed Time Slots (GTS) within the Contention Free Period (CFP) of each superframe duration in order to guarantee channel access for network nodes running time-critical applications with real-time delivery, low latency, or specific bandwidth requirements. A maximum of 7 GTS can be assigned at any one time, with each GTS possibly occupying more than one superframe slot within the superframe's CFP. Allocation and deallocation of GTS are performed by the PAN coordinator on a first-come-first-serve basis [1]. *GTS Attacks* are launched against the network by misusing the GTS management scheme [12].

Since there is no method of verifying of sensor nodes' identifiers (IDs), Jung et al. [14] define two categories of variants of the IEEE 802.15.4 *GTS Attack* as follows.

5.9.1. Existing Identities in the PAN. In this category, a *GTS Attack* is launched when malicious adversaries spoof the IDs of existing legitimate nodes in the PAN. Two variants for this category are defined in [12] as follows.

(a) DoS against Data Transmissions during CFP. This variant requires the adversary to passively eavesdrop on network traffic in order to collect information about the IDs of legitimate nodes and their allocated GTS. The adversary can then use this collected data to spoof the IDs of the legitimate nodes and to send GTS deallocation requests on their behalf to the PAN coordinator. This leads to the termination of channel access rights previously granted to the legitimate nodes during their previously assigned GTS.

(b) False Data Injection. While the *DoS During CFP* variant collects information about the IDs of nodes that have already been allocated GTS by the PAN coordinator, *False Data Injection* collects information about the IDs of legitimate PAN nodes that have not yet been allocated any GTS during the superframe's CFP. Using the collected information, the adversary pretends to be one of the unallocated nodes by spoofing its ID and sends a GTS allocation request on its behalf to the PAN coordinator. Finally, the adversary injects false traffic into the network during its falsely assigned GTS.

5.9.2. Nonexisting Identities in the PAN. Rather than spoofing the IDs of legitimate nodes within the PAN, a malicious adversary can use its own or other nonexisting IDs to conduct either of the two attack variants contained within this category [4].

(a) DoS against GTS Requests. For this variant, a malicious adversary collects information about the GTS list, which contains both allocated and free GTS. Following this, the adversary keeps sending GTS allocation requests to the PAN coordinator until all 7 slots in the GTS list are filled up. Contrary to the *False Data Injection variant*, no

ID spoofing is involved, as the adversary sends allocation requests using its own or other nonexisting IDs to the PAN coordinator.

(b) Stealing Network Bandwidth. This attack variant is identical to the previous *DoS against GTS Requests* variant with the addition that the adversary also injects false data into the network during the assigned GTS. This variant is harder to detect than the previous *DoS against GTS Requests* variant because the PAN coordinator recognizes that the allocated slots are indeed being used for transmitting data and thus does not drop the allocated slots.

Sokullu et al. [12] identify four additional variants of the *GTS Attack*. We include these additional variants within a category of our choosing, which we call *Interference During CFP*.

5.9.3. Interference during CFP. In this type of *GTS Attack*, a malicious adversary collects information about the beginnings and ends of GTS which have been assigned to legitimate network nodes by the PAN coordinator. The adversary then creates interference by using *Link Layer Jamming* during these assigned slots with the intent of corrupting ongoing transmissions. The four variants defined in [12], which fall into this category, are as follows.

(a) One Intelligent Attacker (OIA). In the *OIA* scenario, a malicious adversary corrupts the communication with the maximum GTS length, either by corrupting only the GTS's first superframe slot or by corrupting all of the superframe slots contained within the GTS.

(b) One Random Attacker (ORA). In this scenario, a malicious adversary attacks the GTS of a randomly selected communication.

(c) Two Intelligent Attackers (TIA). This attack variant is considered as an extension to the *OIA* attack variant, with one malicious adversary attacking the communication with the largest GTS length and a second adversary attacking the communication with the second largest GTS length. This requires collaboration between the two adversaries.

(d) Two Random Attackers (TRA). As an extension to the *ORA* scenario, two malicious adversaries can attack the GTS of two randomly selected communications. Due to the random nature of this attack, it is possible for both adversaries to target the same communication.

5.9.4. DoS against CAP Maintenance. CAP maintenance involves the use of a number of preventative actions in order to ensure that the length of the CAP period of each superframe does not fall below a predefined threshold known as *aMinCAPLength* [1]. An adversary can launch an attack against CAP maintenance by constantly sending GTS requests, even when the superframe has no available capacity and/or the length of the CAP is about to fall below *aMinCAPLength*. This causes the length of the CAP to momentarily fall below *aMinCAPLength*, thus reducing the amount of time which member nodes have in order to contend for channel access [1]. While this variant of the *GTS Attack* has not been previously mentioned in any references, its discovery is inspired by the brief statement made by Jung et al. [14] that preventative actions of CAP maintenance are ineffective if a malicious node constantly sends either GTS requests or data at the assigned GTS during the CFP.

5.10. PANId Conflict Attack. IEEE 802.15.4 defines a conflict resolution procedure, which is initiated when two PAN coordinators residing within the same Personal Operating Space (POS) have the same coordinator ID, also referred to as *PANId* [1]. A malicious adversary can abuse the conflict resolution procedure by transmitting fake *PANId* conflict notifications to the targeted PAN coordinator in order to initiate conflict resolution, thus momentarily delaying or even preventing communication between member nodes and the PAN coordinator [6].

5.11. Ping-Pong Effect. The *Ping-Pong Effect* is an attack which is launched with the aim of causing packet loss and service interruption, reducing node performance, and increasing energy consumption and network load. As per its name, this attack causes fast, repeated, and undue handovers of nodes between the coordinators of different PANs.

Balarengadurai and Saraswalhi [7] explain that a *Ping-Pong Effect* can be launched via the manipulation of one or both of the following two network parameters.

5.11.1. Membership Degree. A node switches to a new PAN coordinator if the membership degree to the new PAN coordinator is greater than its membership degree to its current PAN coordinator.

5.11.2. Election Possibility. A new node is elected as the PAN coordinator if its election possibility is higher than the election possibility of the current coordinator. Election possibility is determined with respect to factors such as mobility and remaining battery capacity.

5.12. Bootstrapping Attack. O'Flynn [4] explains an attack which forces a targeted network node to become unassociated with its PAN at a time of the adversary's choosing by launching any of the PHY or MAC layer attacks aimed at causing DoS. The next time that the legitimate node wants to rejoin the network, either the adversary passively eavesdrops on the association process in order to collect valuable bootstrapping information that it can use to perform its own association with the PAN, or the adversary can perform a *MITM Attack* in order to intervene with and thus prevent the association of the legitimate node with the PAN.

5.13. Steganography Attacks. Steganography Attacks are explained in Section 2 and can be launched by hiding information within the PHY and/or MAC frame fields of the 802.15.4 protocol.

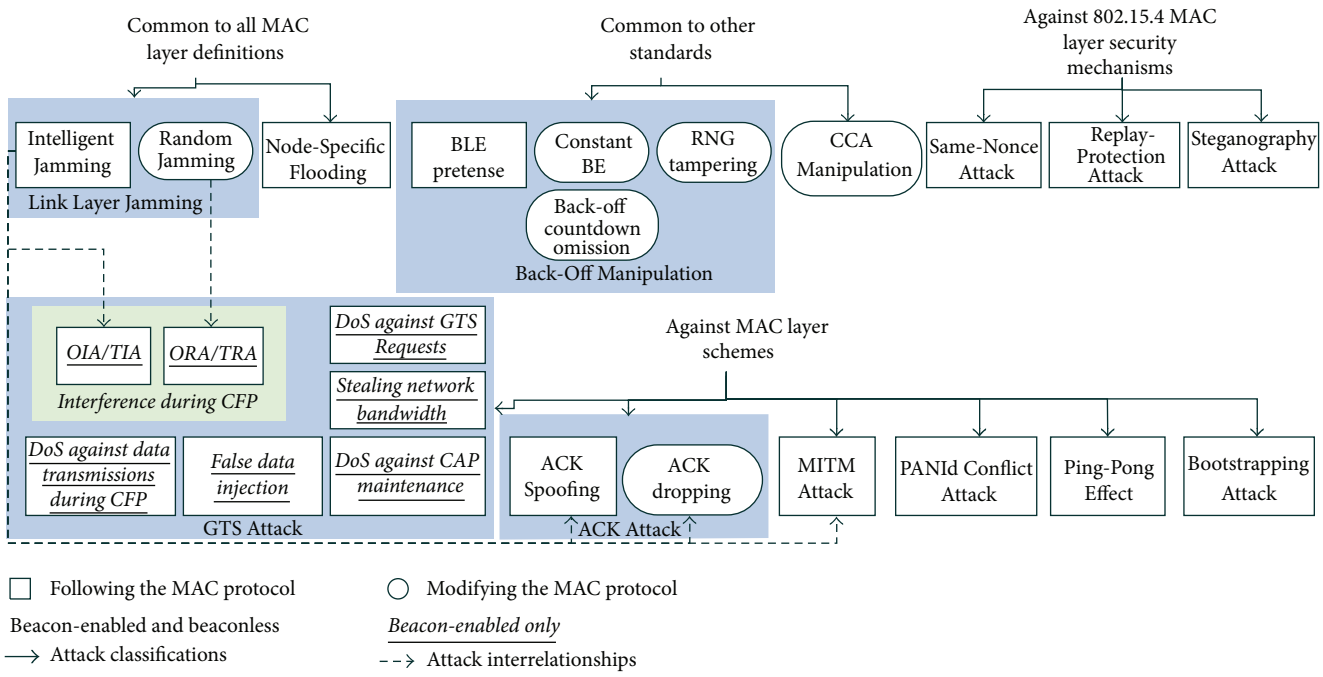

Figure 2: Classification of IEEE 802.15.4 MAC layer attacks.

6. Classification of IEEE 802.15.4 MAC Layer Attacks

The explained MAC layer attacks cannot be classified using one single deterministic classification. Therefore, we present two classifications which include some of the most important methods of classifying IEEE 802.15.4 MAC layer attacks obtained from external references. Novel extensions to these classifications are also presented. Figure 2 illustrates both classification methods, including our proposed extensions and the interrelationships between related attacks, which denote the attacks used to facilitate the launching of other attacks.

6.1. Classification A. Sokullu et al. [6] classify IEEE 802.15.4 MAC layer attacks into the following three main classes.

6.1.1. Common to All MAC Layer Definitions. *Link Layer Jamming* can be launched against all MAC layer definitions of all existing standards. We extend this class of attacks by adding *Node-Specific Flooding*.

6.1.2. Common to Other Standards. *Back-Off Manipulation* and *CCA Manipulation* attacks can be launched against both IEEE 802.15.4 Wireless Personal Area Networks (WPANs) and IEEE 802.11 Wireless Local Area Networks (WLANs) due to their similar CSMA-CA and Distributed Coordination Function (DCF) channel access protocols, respectively.

6.1.3. Against 802.15.4 MAC Layer Security Mechanisms. This class contains specific variants of some general attacks applied against IEEE 802.15.4 MAC layer security mechanisms. *Same-Nonce* Attack targets the access control service, and *Replay-Protection Attack* targets the replay-protection mechanism. *Steganography Attacks* are also included.

In addition to the above three classes of attacks, we extend this classification by including the following additional class of attacks.

6.1.4. Against 802.15.4 MAC Layer Schemes. This class refers to attacks applied against IEEE 802.15.4 MAC layer schemes. Contrary to Sokullu et al. [6], we argue that acknowledgments are considered to be an implemented MAC layer scheme and not a security mechanism. As such, we include *ACK* and *MITM Attacks* here. We also include the following additional attacks; *PANId Conflict Attack* targets the PANId conflict resolution procedure, *GTS Attacks* target the GTS management scheme, and *Ping-Pong Effect* and *Bootstrapping Attack* target PAN association.

6.2. Classification B. In this classification, we classify attacks with respect to conformance to MAC protocol rules and mode of network operation.

6.2.1. Conformance to MAC Protocol. Mišić et al. [13] classify attacks into those which either follow the MAC protocol to the letter or modify its rules.

6.2.2. Mode of Network Operation. All MAC layer attacks can be launched against both beacon-less and beacon-enabled networks except for all *GTS Attack* variants, as GTS are only present during the CFP of each superframe in beacon-enabled networks.

Table 2: Comparative analysis of IEEE 802.15.4 MAC layer attacks (√ for cause, √√ for effect).

Attack	DoS intent				Primary security goals			
	Exhaustion	Collision	Unfairness	Sleep	Confidentiality	Integrity	Authenticity	Availability
Link Layer Jamming	√√	√	√	×	×	×	√√	√
Node-Specific Flooding	×	√	√	×	×	×	√√	√√
BLE pretense, constant BE, RNG tampering, and CCA reduction	×	√√ [7]	×	×	×	×	√√	×
Back-off countdown omission and CCA omission	√	√√ [7]	×	×	×	×	√√	×
Same-Nonce Attack	×	×	×	√√	×	×	×	×
Replay-Protection Attack	×	√√	√	×	×	×	√√	√
ACK spoofing attack	×	√√	×	×	×	√√	√√	×
ACK dropping attack	×	√	√	×	×	×	√√	√√
MITM Attack	×	√√	×	×	√√	√√	√√	×
PANId Conflict Attack	×	√	√	×	×	×	√√	√√
DoS against data transmissions during CFP	×	√	×	×	×	√√	√√	×
DoS against GTS Requests	×	√	×	×	×	×	√√	√√
False Data Injection	×	√	×	×	√√	√√	√√	√√
Stealing network bandwidth	×	√	×	×	√√	×	√√	√√
DoS against CAP maintenance	×	√	×	×	×	×	√√	√√
Interference during CFP	√√	√	√	×	×	×	√√	√
Ping-Pong Effect	×	√	√	×	×	×	√√	√√
Bootstrapping Attack	×	√√	×	×	×	×	√√	√
Steganography Attack	×	√	×	×	×	×	×	×

7. Comparative Analysis of IEEE 802.15.4 MAC Layer Attacks

In this section, we perform a detailed comparison between the attacks with respect to the following evaluation criteria.

7.1. Evaluation Criteria

7.1.1. DoS Intent. The primary intent of most MAC layer attacks is to cause a DoS against a specific part of or the entire network [12].

(a) Exhaustion Attacks. One form of DoS involves the depletion of the already-constrained power, bandwidth, memory, and/or storage resources of legitimate network nodes [7].

(b) Collision Attacks. An adversary can corrupt legitimate packets by initiating transmission during ongoing legitimate packet transmissions [7].

(c) Unfairness Attacks (Also Known as Misbehavior Attacks [4]). This attack ensures that an adversary is granted the same priority as or higher priority than legitimate nodes with respect to utilization of network resources, such as bandwidth and channel access. The latter causes starvation of legitimate nodes from network resources [7].

(d) Sleep Attacks. A *Sleep Attack* manipulates a targeted node's duty cycle (the percentage of time during which the node remains in active state). If the attack causes the targeted node's duty cycle to increase above average, it is also referred to as a *Battery Exhaustion Attack* [15].

7.1.2. Security Goal Violation. As in Section 4, MAC layer attacks are compared with respect to their violations of the security goals obtained from Kumar et al. [10]. This paper only focuses on primary security goals, as no secondary goals are violated by any of the discussed attacks.

7.2. Comparison between IEEE 802.15.4 MAC Layer Attacks. Table 2 illustrates the comparison between IEEE 802.15.4 MAC layer attacks with respect to both DoS intent and primary security goal violation. We analyze each of the MAC layer attacks and their variants from a *cause* and *effect* perspective. The *cause* (√) of an attack is the primary intent with which the attack is launched, whereas the *effect* (√√) of an attack refers to an unplanned repercussion of launching the attack in question.

(a) Data Confidentiality. Same-Nonce Attack is the only attack considered to violate data confidentiality, as it enables an adversary to decrypt ciphered network transmissions.

(b) Data Integrity. We consider attacks that corrupt only the payload field of the frame, while preserving the value of the original frame's Frame Check Sequence (FCS) field, to violate data integrity. As such, *Steganography Attacks* are not considered to violate the integrity of network transmissions.

(c) Data Authenticity. Attacks which involve the spoofing of legitimate node IDs violate authenticity.

(d) Network Availability. Any attack variant which has at least one DoS intent as its *cause*, as illustrated in Table 2, is considered to violate network availability.

8. Conclusion

This work constitutes a detailed survey on IEEE 802.15.4 PHY and MAC layer attacks.

In the first part of this survey, we extensively discussed 802.15.4 PHY layer attacks. The purpose and operation of each attack and its variants were explained. We presented two classifications for *Radio Jamming* attacks in particular. *Classification A* divided *Radio Jamming* attacks into *Wide-Band Denial* and *Pulse-Band Denial*, depending on the number of channels targeted by each within the related frequency band. *Classification B* classified *Radio Jamming* attacks into *PHY Payload Corruption* and *FCS Corruption* categories, depending on the method used for frame corruption. We explained how both frame corruption techniques in *Classification B* could be applied to any of the *Radio Jamming* attacks mentioned in *Classification A*. We concluded our discussion of 802.15.4 PHY layer attacks with a comparative analysis of the discussed PHY layer attacks, including their multiple techniques and variants. Attack differences were evaluated with respect to four evaluation criteria: energy efficiency, effectiveness, stealthiness, and violation of two particular primary security goals, which were data integrity and network availability.

IEEE 802.15.4 MAC layer attacks were addressed in the second part of this survey. We started off by clarifying the purpose and method of operation of each attack and its variants. A novel variant of the *GTS Attack*, which we called *DoS against CAP maintenance*, was proposed. Two classifications of the MAC layer attacks were presented. *Classification A* divided the attacks into four classes: common to all MAC layer definitions of all existing network standards, common to only a subset of other standards, launched against 802.15.4 MAC security mechanisms, and launched against implemented 802.15.4 MAC schemes. *Classification B* classified MAC attacks based on their conformance to MAC layer protocol rules and network mode of operation. Finally, a comparative analysis between all MAC layer attacks, as well as their multiple techniques and variants, was performed with respect to DoS intent and primary security goal violation.

Competing Interests

The authors declare that they have no competing interests.

References

[1] IEEE Standard for Information Technology, "Local and metropolitan area networks—specific requirements—part 15.4: wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for low rate Wireless Personal Area Networks (WPANs)," IEEE 802.15.4-2006, 2006.

[2] S. C. Ergen, *ZigBee/IEEE 802.15.4 Summary*, 2004, http://users.ece.utexas.edu/~valvano/EE345L/Labs/Fall2011/Zigbeeinfo.pdf.

[3] P. Jokar, H. Nicanfar, and V. C. M. Leung, "Specification-based intrusion detection for home area networks in smart grids," in *Proceedings of the IEEE 2nd International Conference on Smart Grid Communications (SmartGridComm '11)*, pp. 208–213, Brussels, Belgium, October 2011.

[4] C. P. O'Flynn, "Message denial and alteration on IEEE 802.15.4 low-power radio networks," in *Proceedings of the 4th IFIP International Conference on New Technologies, Mobility and Security (NTMS '11)*, pp. 1–5, IEEE, Paris, France, February 2011.

[5] A. D. Wood, J. A. Stankovic, and G. Zhou, "DEEJAM: defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks," in *Proceedings of the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '07)*, pp. 60–69, IEEE, San Diego, Calif, USA, June 2007.

[6] R. Sokullu, I. Korkmaz, O. Dagdeviren, A. Mitseva, and N. R. Prasad, An Investigation of IEEE 802.15.4 MAC Layer Attacks, http://netos.ube.ege.edu.tr/source/publications/wpmc07.pdf.

[7] C. Balarengadurai and S. Saraswalhi, "Comparative analysis of detection of DDoS attacks in IEEE 802.15.4 low rate wireless personal area network," in *Proceedings of the International Conference on Modelling Optimization and Computing*, vol. 38, pp. 3855–3863, April 2012.

[8] M. Wilhelm, J. B. Schmitt, and V. Lenders, "*Practical Message Manipulation Attacks in IEEE 802.15.4 Wireless Networks*," 2015, http://www.lenders.ch/publications/conferences/Pilates12.pdf.

[9] D. Martins and H. Guyennet, "Attacks with steganography in PHY and MAC layers of 802.15.4 protocol," in *Proceedings of the 5th International Conference on Systems and Networks Communications (ICSNC '10)*, pp. 31–36, Nice, France, August 2010.

[10] J. V. Kumar, A. Jain, and P. N. Barwal, "Wireless sensor networks: security issues, challenges and solutions," *International Journal of Information and Computation Technology (IJICT)*, vol. 4, no. 8, pp. 859–868, 2014.

[11] Y. M. Amin and A. T. Abdel-Hamid, "Classification and analysis of IEEE 802.15.4 MAC layer attacks," in *Proceedings of the 11th International Conference on Innovations in Information Technology (IIT '15)*, pp. 74–79, Dubai, United Arab Emirates, November 2015.

[12] R. Sokullu, O. Dagdeviren, and I. Korkmaz, "On the IEEE 802.15.4 MAC layer attacks: GTS attack," in *Proceedings of the 2nd International Conference on Sensor Technologies and Applications (SENSORCOMM '08)*, pp. 673–678, Cap Esterel, France, August 2008.

[13] V. B. Mišić, J. Fung, and J. Mišić, "MAC layer security of 802.15.4-compliant networks," in *Proceedings of the 2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS '05)*, pp. 847–854, IEEE, Washington, DC, USA, November 2005.

[14] S. S. Jung, M. Valero, A. Bourgeois, and R. Beyah, "Attacking Beacon-enabled 802.15.4 networks," in *Security and Privacy in Communication Networks*, vol. 50 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 253–271, Springer, Berlin, Germany, 2010.

[15] F. Amini, J. Misic, and R. Eskicioglu, *Simulation and Evaluation of Security and Intrusion Detection in IEEE 802.15.4 Network*, University of Manitoba, Winnipeg, Canada, 2008.