Book Title: XXXXXXXXXXXXXXXXXXXXXXXXXXXX

Editors

March 24, 2008

Contents

Chapter 1

Jamming in Wireless Sensor Networks

Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos and Grammati Pantziou

The objective of this chapter is to provide a general overview of the critical issue of jamming in WSNs and cover all the relevant work, providing the interested researcher pointers for open research issues in this field. Jamming represents the most serious security threat in the field of Wireless Sensor Networks (WSNs), as can easily put out of order even WSNs that utilize strong high-layer security mechanisms, simply because it is often ignored in the initial WSN design. Law at al. in [12] conclude that with typical WSN systems in use today no effective measures against link-layer jamming are possible. This chapter starts with a brief overview of the communication protocols typically used in WSN deployments. The next section highlights the characteristics of contemporary WSNs that make them susceptible to jamming attacks along with the various types of jamming which can be exercised against WSNs. Typical countermeasures against jamming are also detailed. Furthermore the key ideas of existing security mechanisms against jamming attacks in WSNs are reviewed, focusing on their respective advantages/disadvantages. The chapter concludes highlighting open research issues with respect to the defence against jamming attacks in sensor networks.

1.1 Introduction

Wireless sensor networks (WSNs) [2] are used in many applications which often include the monitoring and recording of sensitive information. Hence, their critical importance raises major security concerns. Jamming is defined as the act of intentionally directing electromagnetic energy towards a communication system to disrupt or prevent signal transmission [1]. In the context of WSNs, jamming is the type of attack which interferes with the radio frequencies used by network nodes [35]. In the event that an attacker uses a rather powerful jamming source, disruptions of WSNs' proper function are likely to occur. As a result, the use of countermeasures against jamming in WSN environments is of immense importance, especially taking into account that WSNs suffer from many constraints, including low computation capability, limited memory and energy resources, susceptibility to physical capture and the use of insecure wireless communication channels.

Jamming attacks may be viewed as a special case of Denial of Service (DoS) attacks. Wood and Stankovic define DoS attack as "any event that diminishes or eliminates a network's capacity to perform its expected function" [44]. Typically, DoS prevents or inhibits the normal use or management of communications through flooding a network with 'useless' information. In a jamming attack the Radio Frequency (RF) signal emitted by the jammer corresponds to the 'useless' information received by all sensor nodes. This signal can be white noise or any signal that resembles network traffic.

1.2 Communication in WSNs

A WSN is usually composed of hundreds or even thousands of sensor nodes. These sensor nodes are often randomly deployed in the field and form an infrastructure-less network. Each node is capable of collecting data and routing it back to the Processing Element (PE) via ad hoc connections with neighbor sensor nodes. A sensor consists of five basic parts: a sensing unit, a central processing unit (CPU), storage unit, a transceiver unit, and a power unit [2]. It may also have additional application-dependent components attached, such as location

finding system (GPS), mobilizer and power generator.

1.2.1 Communication Protocol Stack

The protocol stack used in sensor nodes contains physical, data link, network, transport, and application layers defined as follows [2]:

- Physical layer: responsible for frequency selection, carrier frequency generation, signal deflection, data encryption [1] and modulation. This is the layer that suffers the most damage from radio jamming attacks.
- Data link layer: responsible for the multiplexing of data streams, data frame detection, medium access control (MAC), data encryption and error control; as well as ensuring reliable point-to-point and point-to-multipoint connections. This layer and more specific MAC are heavily damaged by link-layer jamming. In link-layer jamming [10, 12], sophisticated jammers can take advantage of the data link layer to achieve energy-efficient jamming. Compared to radio jamming, link-layer jamming offers better energy efficiency.
- Network layer: responsible for specifying the assignment of addresses and how packets are forwarded.
- Transport layer: responsible for the reliable transport of packets and data encryption.
- Application layer: responsible for specifying how the data are requested and provided for both individual sensor nodes and interactions with the end user.

1.2.2 Communication Protocols and Standards used in WSNs

A considerable percentage of the nodes currently used in WSN environments comply with the ZigBee communications protocol. ZigBee protocol minimizes the time the radio functions so as to reduce power consumption. All ZigBee devices are required to comply with the IEEE

[1] data encryption more commonly is done at the data link or transport layers.

802.15.4-2003 or IEEE 802.15.4-2006 Low-Rate Wireless Personal Area Network (WPAN) standard. The standard only specifies the lower protocol layers -the physical layer (PHY), and the medium access control (MAC) portion of the data link layer (DLL). The standard's specified operation is in the unlicensed 2.4 GHz, 902-928 MHz (North America) and 868 MHz (Europe) ISM (Industrial, scientific and medical) bands. In the 2.4 GHz band there are 16 ZigBee channels (for both 2003, 2006 version of IEEE 802.15.4), with each channel occupying 3 MHz of wireless spectrum and 5 MHZ channel spacing. The center frequency for each channel can be calculated as, $FC = (2400 + 5 * k)MHz$, where $k = 1, 2, ..., 16$. In 902-928 MHz there are ten channels (extended to thirty in 2006) with 2 MHz channel spacing and in 868 MHz one channel (extended to two in 2006).

The radios use DSSS coding in which the transmitted signal takes up more bandwidth than the information signal that is being modulated. In IEEE 802.15.4-2003 two physical layers are specified: BPSK in the 868 MHz and 902-928 MHz, and orthogonal O-QPSK that transmits two bits per-symbol in the 2.4 GHz band. The raw, over-the-air data rate is 250 kbit/s per channel in the 2.4 GHz band, 40 kbit/s per channel in 902-928 MHz, and 20 kbit/s in the 868 MHz band. The 2006 revision improves the maximum data rates of the 868/915 MHz bands, bringing them up to support 100 and 250 kbit/s as well. Moreover, it defines four physical layers depending on the modulation method used: BPSK and O-QPSK in 868/915 MHz band, O-QPSK in 2.4 GHz band and a combination of binary keying and amplitude shift keying for 868/915 MHz band. Transmission range for both versions is between 10 and 75 meters (33 246 feet), although it is heavily dependent on the particular environment where the nodes are deployed. The maximum output power of the radios is generally 0 dBm (1 mW).

1.3 Vulnerabilities of Today WSNs that Make them Susceptible to Jamming

The above discussion makes clear that a node that follows the IEEE 802.15.4 communications protocol (2003 or 2006 revision) may connect to the network via a limited number of

frequencies (16 channels in 2.4 GHz band (2400-2483.5 MHZ), 10 channels (30 for 2006) in 902-928 MHz and 1 channel (3 for 2006) in 868.3 MHz). In addition, taking into account the maximum output power of the radio of a node (0 dBm), it becomes apparent that an attacker could easily jam a WSN (with the use of small power output) and disrupt sensor nodes communication. The main limitation of the above-mentioned protocols is that they have not been originally designed taking radio jamming into account. WSN nodes design also presents the same limitation. Other types of widely utilized motes such as Mica-2 [6] are even more susceptible to jamming since they use a limited number of frequencies (support of only lower 868/916 bands and not 2.4 GHz band) for communication. Thus with typical WSNs in use today is very difficult to take effective measures against jamming, which raises a major security issue. A significant number of research works suggest addressing jamming attacks utilizing hardware used in contemporary WSNs [19, 20, 43, 42, 44], while other works suggest new design requirements of nodes that can effectively defend jamming attacks [18]. The main advantage of the former is that the implementation is much cheaper and straightforward and the compatibility with currently available hardware; yet, they cannot easily cope with heavy jamming attacks. On the other hand, suggesting new design requirements for nodes, jamming attacks can be addressed more efficiently. However the implementation of these nodes requires a significant amount of research, while the associated cost is highly increased. In addition, this approach offers no compatibility with existing hardware.

1.4 Definition of Jamming, Jamming Techniques and Types of Jammers

Jamming is defined as the emission of radio signals aiming at disturbing the transceivers' operation [1]. The key point in successful jamming attacks is Signal-To-Noise ratio (SNR), SNR $= P_{signal}/P_{noise}$ where P is the average power. Noise simply represents the undesirable accidental fluctuation of electromagnetic spectrum, collected by the antenna. Jamming can be considered effective if SNR < 1. Existing jamming techniques are described below.

1.4.1 Spot Jamming

The most popular jamming method is the spot jamming wherein the attacker directs all its transmitting power on a single frequency that the target uses with the same modulation and enough power to override the original signal. Spot jamming is usually very powerful, but since it jams a single frequency each time it may be easily avoided by changing to another frequency.

1.4.2 Sweep Jamming

In sweep jamming a jammer's full power shifts rapidly from one frequency to another. While this method of jamming has the advantage of being able to jam multiple frequencies in quick succession, it does not affect them all at the same time, and thus limits the effectiveness of this type of jamming. However, in a WSN environment, it is likely to cause considerable packet loss and retransmissions and, thereby, consume valuable energy resources.

1.4.3 Barrage jamming

In barrage jamming a range of frequencies is jammed at the same time. Its main advantage is that it is able to jam multiple frequencies at once with enough power to decrease the SNR ratio of the enemy receivers. However as the range of the jammed frequencies grows bigger the output power of the jamming is reduced proportionally.

1.4.4 Deceptive jamming

In this type of jamming the signal emitted by the adversary is not random but resembles network traffic. Deceptive jamming is used when the adversary does not want to reveal her existence. By flooding the WSN with fake data she can deceive the network's defensive mechanisms (if any) and complete her task without leaving any traces. Deceptive jamming is a very dangerous type of attack as it cannot be easily detected and has the potential to

flood the PE with useless or fake data that will mislead the WSN's operator and occupy the available bandwidth used by legitimate nodes.

1.4.5 Types of Jammers

There are several types of jammers that may be used against WSNs. Xu et al. in [42] propose generic jammer models, namely (1) the constant jammer, (2) the deceptive jammer, (3) the random jammer and (4) the reactive jammer.

Constant jammer emits continuous radio signals in the wireless medium (see Figure 1.1). The signals that she emits are totally random. They don't follow any underlying MAC protocol and are just random bits. This type of jammer aims at keeping the channel busy and disrupting nodes' communication or causing interference to nodes that have already commenced data transfers and corrupt their packets.

The deceptive jammer uses deceptive jamming techniques (see previous subsection 1.4.4) to attack the WSN (see Figure 1.1).

The random jammer sleeps for a random time t_s and jams for a random time t_j (see Figure 1.2).The type of jamming used can be of any kind depending on the situation. Also by changing t_s and t_j we can achieve different levels of effectiveness and power saving.

The reactive jammer (see Figure 1.2) listens for activity on the channel, and in case of activity, immediately sends out a random signal to collide with the existing signal on the channel. As a result the transmitted packets of data will be corrupted.

According to Xu et al. [42], the constant jammers, deceptive jammers and reactive jammers are effective jammers in that they can cause the packet delivery ratio to fall to zero or almost zero, if they are placed within a suitable distance from the victim nodes. However these jammers are also energy-inefficient, meaning they would exhaust their energy sooner than their victims would supposed they are energy-constrained. Although random jammers save energy by sleeping, they are less effective. With respect to energy-efficiency, DEEJAM [46] presents a reactive design that is relatively energy efficient.

1.5 Countermeasures Against Jamming

In this section we present countermeasures that deal with possible radio jamming scenarios.

1.5.1 Regulated Transmitted Power

Using low transmitted power decreases the discovery probability from an attacker (an attacker must locate first the target before transmitting jamming signal). Higher transmitted power implies higher resistance against jamming because a stronger jamming signal is needed to overcome the original signal. A considerable percentage of sensor nodes currently used in contemporary WSNs (e.g., Sunspots [37]) possess the capability to change the output power of their transmitter.

1.5.2 Frequency-Hopping Spread Spectrum (FHSS)

Frequency-hopping spread spectrum (FHSS) is a spread-spectrum method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a shared algorithm known both to the transmitter and the receiver. FHSS brings forward many advantages in WSN environments:

- it minimizes unauthorized interception and jamming of radio transmission between the nodes;
- the SNR required for the carrier relative to the background decreases as a wider range of frequencies is used for transmission;
- it deals effectively with the multipath effect[2];
- multiple WSNs can coexist in the same area without causing interference problems.

[2]Multipath in wireless telecommunications is the propagation phenomenon that results in radio signals reaching the receiving antenna through two or more paths due to reflections of the original signal [5, 13]. FHSS, when the hop rate is quite fast, eliminates the multipath effect because when the receiver receives the original signal it immediately changes frequency, thus the ghost of the original signal (harmonic signal) isn't received at all.

One of the main drawbacks of frequency-hopping is that the overall bandwidth required is much wider than that required to transmit the same data using a single carrier frequency. However, transmission in each frequency lasts for a very limited period of time so the frequency is not occupied for long.

1.5.3 Direct Sequence Spread Spectrum (DSSS)

Direct-sequence spread spectrum (DSSS) transmissions are performed by multiplying the data (RF carrier) being transmitted and a pseudo-noise (PN) digital signal. This PN digital signal is a pseudorandom sequence of 1 and -1 values, at a frequency (chip rate[3]) much higher than that of the original signal. This process causes the RF signal to be replaced with a very wide bandwidth signal with the spectral equivalent of a noise signal; however, this noise can be filtered out at the receiving end to recover the original data, through multiplying the incoming RF signal with the same PN modulated carrier.

The first three of the above-mentioned FHSS advantages also apply to DSSS. Furthermore, the processing applied to the original signal by DSSS makes it difficult to the attacker to descramble the transmitted RF carrier and recover the original signal (the key factor is the chip rate which in 802.15.4 is 2 Mchip/s). Also since the transmitted signal of DSSS resembles white noise, radio direction finding of the transmitting source is a difficult task.

1.5.4 Hybrid FHSS/DSSS

Hybrid FHSS/DSSS communication between WSN nodes represents a promising anti-jamming measure. In general terms direct-sequence systems achieve their processing gains through interference attenuation using a wider bandwidth for signal transmission, while frequency hopping systems through interference avoidance. Consequently using both these two modulations, resistance to jamming may be highly increased. Also Hybrid FHSS/DSSS compared to standard FHSS or DSSS modulation provides better low-probability-of-detection/low-probability-of-interception (LPD/LPI) properties. Fairly specialized interception equipment

[3]chip represents a single bit of a pseudo-noise sequence while chip rate is the rate at which chips are sent.

is required to mirror the frequency changes uninvited. It is stressed though that both the frequency sequence and the PN code of DSSS should be known to recover the original signal. Thus Hybrid FHSS/DSSS improves the ability to combat the near-far problem which arises in DSSS communications schemes. Another welcome feature is the ability to adapt to a variety of channel problems.

1.5.5 Ultra Wide Band Technology

Ultra Wide Band (UWB) technology is a modulation technique based on transmitting very short pulses [40] on a large spectrum of a frequency band simultaneously. This renders the transmitted signal very hard to be intercepted/jammed and also resistant to multipath effects. In the context of WSNs, UWB can provide many advantages. The research work of Oppermann et al. [23] promises low power and low-cost wide-deployment of sensor networks. In addition, UWB-based sensor networks guarantee more accurate localization and prolonged battery lifetime. The IEEE standard for UWB, 802.15.3.a, is under development.

1.5.6 Antenna Polarization

The polarization of an antenna is the orientation of the electric field of the radio wave with respect to the earths' surface and is determined by the physical structure of the antenna and its orientation. The antenna polarization of a nodes' radio unit plays a significant role in jamming environments. For line-of-sight communications (mainly used in WSNs) for which polarization can be relied upon, it can make a significant difference in signal quality to have the transmitter and receiver using the same polarization. Thus, an antenna with circular polarization will not receive signals that are circularly polarized as for the opposite direction. Furthermore, there will be 3 Db loss from a linear polarized antenna that receives signals circular polarized; the same also stands vice-versa. Hence, if the nodes of a WSN are capable of changing the polarization of their antennas when they sense interference they will be able to effectively defend in jamming environments. One problem is that the nodes must inform first each other about the change of their antenna's polarization, otherwise communication among

peers will be interrupted. A method to overcome this problem is to program the nodes when they sense interference or lack of network connectivity, to change to specific polarizations until they establish reliable link to the network. The change of nodes' polarization of a WSN hinders the jamming process because it makes necessary to use specialized jamming equipment with the capability to change its signal polarization rapidly during the jamming.

1.5.7 Directional Transmission

Today's sensor nodes typically use omni-directional antennas. The use of directional antennas could dramatically improve jamming tolerance in WSNs. In general, directional antennas/transmission provide better protection against eavesdropping, detection and jamming than omni-directional transmission [21, 29, 36]. A directional antenna transmits or receives radio waves only from one particular direction unlike the omni-directional antenna that transmits and receives radio waves from all directions in the same time. This feature allows increased transmission performance, more receiving sensitivity and reduced interference from unwanted sources (e.g. jammers) compared to omni-directional antennas.

The main problems with directional transmission are (a) the requirement of a more sophisticated MAC protocol [3, 9] and (b) multipath routing becomes more complex [14, 31].

Two types of directional antennas are commonly used in wireless ad hoc networks (sensor networks are not included): sectored and beamforming. Sectored antennas have multiple fixed antenna elements, pointed in different directions that can often operate independently. On the other hand, beamforming antennas have multiple antenna elements that work in tandem to transmit or receive in different directions. Beamforming antennas can be electronically switched or steered. Switched beamforming antennas can select one from a set of predefined beams by shifting the phase of each antenna element's signal by a precalculated amount. Steered beamforming antennas are more dynamic in nature since the main antenna lobe can be directed in any desired direction. They have increased performance and cost compared to switched beamforming antennas.

In the context of wireless sensor networks, Noubir [22] proposed the use of sectored

antennas as more resistant to jamming, however, the specific antennas are not yet available.

1.6 Proposed Security Schemes Against Jamming in WSNs

Securing WSNs against jamming attacks is an issue of immense importance. In the following subsections we review security schemes proposed in the WSN literature to address this issue. We propose taxonomy that categorizes these approaches in:

- proactive,
- reactive,
- mobile agent-based.

The relevant advantages and disadvantages of each method are highlighted and evaluated.

1.6.1 Proactive Countermeasures

The role of proactive countermeasures is rather to make a WSN immune to jamming attacks rather than to react in the event of such incident. Proactive countermeasures can be classified in software (e.g. algorithms for the detection of jamming or encryption of transmitted packets) and combined software-hardware countermeasures (e.g. encryption of packets and FHSS transmission in parallel).

1.6.1.1 Proactive Software Countermeasures

This class of countermeasures makes use of software approaches (e.g. specialized algorithms and MAC protocols) to help a node survive jamming attacks or detect them and then employ other defensive mechanisms.

The Feasibility of Launching and Detecting Jamming Attacks in WSNs. In [42] Xu et al. claim that understanding the nature of jamming attacks is critical to assuring the operation of wireless networks. They present four different jammer attack models that may be employed against a WSN and they explore various techniques for detecting jamming attacks in WSNs. In order to improve detection, they introduce the notion of consistency checking, where the packet delivery ratio is used to classify a radio link as having poor utility, and then a consistency check is performed to classify whether poor link quality is due to jamming. They propose two enhanced detection algorithms: one employing signal strength for consistency check, and one employing location information for consistency check.

The advantage of this work is that knowing and identifying the adversary (e.g. the jammer type) the WSN can deal with the problem more efficiently. However the authors focus on the analysis and detection of jamming signals and they do not deal with effective countermeasures against jamming.

Energy-Efficient Link-Layer Jamming Attacks against WSN MAC Protocols. Law et al. In [12] explore energy-efficient attacks against the data link layer. They examine three representative MAC protocols, S-MAC, L-MAC and B-MAC and they derive several jamming attacks that allow an adversary to jam the above MAC protocols in energy-efficient manner : (a) they are effective on encrypted packets, (b) they are as effective as constant/deceptive/reactive jamming, and (c) they are more energy-efficient than random jamming or reactive jamming.

The authors also, discuss potential countermeasures against the proposed jamming attacks for each of the above-mentioned MAC protocols. For S-MAC they propose the use of high duty cycle as a partial countermeasure to energy-efficient link-layer jamming and for L-MAC shorter data packets. Finally they suggest the use of L-MAC as a better choice compared to other MAC protocols in terms of resistance against link-layer jamming.

The main conclusion drawn from this work is that with typical WSN systems in use today no effective measures against link-layer jamming are possible. Regarding WSNs that require increased security against link-layer jamming the authors propose: (a) the encryption of

link-layer packets to ensure a high entry barrier for jammers, (b) the use of spread spectrum hardware, (c) the use of TDMA protocol, and (d) the use of randomized intervals.

The strong points of this work lie in the in-depth exploration of jamming attacks against MAC protocols and the suggestion of several countermeasures. Mainly software countermeasures are proposed and tested. The only drawback is that although the use of spread spectrum hardware is suggested, such solution is neither tested nor simulated; also, the authors do not suggest a specific type of spread spectrum technique (e.g. FHSS, DSSS or UWB). It is quite obvious that even the less sophisticated jamming attack could put out of order sensor nodes that use only one communication channel, whatever MAC protocol these nodes use.

Radio Interference Detection in Wireless Sensor Networks. Radio interference relations among the nodes of a WSN and the design of a radio interference detection protocol (RID) are discussed in [47]. The main purpose of RID and its variation RID-Basic (RID-B) is to detect run-time radio interferences relations among nodes. The interference detection results are used to design real collision-free TDMA protocols.

The basic idea of RID is that a transmitter broadcasts a High Power Detection packet (HD packet), and subsequently a Normal Power Detection packet (ND packet). This is called an HD-ND detection sequence. The receiver uses the HD-ND detection sequence to estimate the transmitter's interference strength. An HD packet includes the transmitter's ID. The receiver estimates possible interference caused by the transmitter by sensing the power level of the transmitter's ND packet.

After the HD-ND detection, each node propagates the detected interference information to its neighbor nodes, and then uses this information to figure out all collision cases within the system.

Briefly RID comprises three phases, (a) HD-ND detection, (b) information sharing, (c) interference calculation. RID-B is a simpler and more lightweight version of RID (it lacks phase 3).

The main advantage of RID and RID-B is that in simulated WSNs combined with the TDMA protocol the packet delivery ratio reaches 100% while TDMA alone has packet loss up to 60%, in high packet traffic.

The main problem with RID and RID-B is the extended usage of bandwidth and energy of sensor nodes in the constrained environment of WSNs (especially in the case of RID). Furthermore only interference from adjacent sensor nodes is efficiently addressed. Jamming from external sources is not investigated; hence RID remains highly vulnerable to jamming attacks.

DEEJAM: Defeating Energy-Efficient Jamming. Wood et al. in [46] propose DEEJAM, a new MAC-Layer protocol for defending against stealthy jammers using IEEE 802.15.4-based hardware. The general design approach of this protocol is to hide messages from a jammer, evade its search and reduce the impact of messages that are corrupted anyway.

In this work the authors provide the definition, implementation and evaluation of four jamming attack classes and the suitable countermeasures against these attacks which are all combined in DEEJAM protocol. They also assume that the attacker uses the same or similar hardware as WSN nodes in terms of capability, energy capacity, and complexity. For more sophisticated attackers they suggest other approaches [43, 45] more suitable than DEEJAM. The jamming attacks and the relevant countermeasures proposed in this work are:

- Interrupt jamming in which the jammer transmits only when its radio captures a multi-byte preamble and a Start of Frame Delimeter (SFD) sequence (see Figure 1.3). The capture of the above sequence is an indication for the jammer that a packet of data follows, so she initiates jamming. The defense proposed for this type of jammer is 'Frame Masking', where the sender and the receiver node agree on a secret pseudo-random sequence for the SFD in each packet. As a result, no interrupt will be signaled to begin jamming. However against a constant jammer this method can not defend effectively.

- Activity jamming illustrated in Figure 1.4 where the attacker is trying to detect ra-

dio activity by periodically sampling the radio signal strength indicator (RSSI) or the radio's clear-channel assessment (CCA) input (if available). When RSSI is above a programmable threshold the jammer initiates her attack. The proposed defense for this type of jamming is frequency hopping, since the attacker can only sample RSSI only for the channel on which its radio listens to.

- Scan Jamming illustrated in Figure 1.5, is the appropriate attack against frequency hopping. However, the attacker must have a significant higher hopping rate from the victim. In this type of attack the attacker samples each channel as briefly as possible to determine if activity is present (the same method used in activity jamming). If she discovers radio activity, jamming is immediately initiated. The authors for this type of attack suggest packet fragmentation as the most suitable countermeasure. Scan jamming is most successful if the transmitted messages are long enough to be intercepted (the required transmission time is longer and this gives more time to the attacker for channel scanning). Using packet fragmentation a node breaks the transmitted packet into fragments which are transmitted separately on different channel and with different SFDs. If the fragments are short enough, an attacker's reactive jamming message does not start until after the sender has finished transmitting and hopped to another channel.

- Pulse jamming where the attacker is blindly jamming on short pulses on a single channel. This will corrupt the fragments of a packet that would use the current channel and taking into account that corrupting even one fragment is sufficient to cause the drop of the entire packet, pulse jamming can achieve excellent results in WSNs with limited communication channels available for frequency hopping. Redundant encoding is the proposed countermeasure, wherein the receiver is able to recover from one or more corrupted fragments. However there is an increased cost in energy and bandwidth usage since transmission redundancy is occurred.

To conclude, DEEJAM utilizes all above-mentioned defensive mechanisms to protect a WSN against jamming from adversaries that use hardware with same capabilities as the deployed nodes. The main advantage are that it is compatible with existing nodes' hardware (no hardware modification is needed); the authors have also provided evidence of its effectiveness via simulations on MICAz nodes [6]. However as the authors already noted against

a powerful and more sophisticated jammer DEEJAM cannot effectively defend the WSN and the most probable scenario is that an adversary will use more advanced hardware compared to that of the nodes'. Another drawback is the overhead that DEEJAM requires to operate and the increased computational and energy cost in the already resource constrained nodes of a WSN.

1.6.1.2 Proactive Software-Hardware Combined Countermeasures

The category of proactive countermeasures focuses on the design of innovative anti-jamming hardware along with the proposal of algorithms that will utilize the new properties of the hardware.

Hermes II node. Mpitziopoulos and Gavalas outline the design specifications of a prototype node, named Hermes II that effectively defends jamming attacks [18]. Hermes II uses a hybrid FHSS/DSSS scheme as the main countermeasure against jamming.

The band that the authors propose for communication among Hermes nodes is the unlicensed 5 GHz band (5650-5925 MHz) which suffers less interference compared to the heavily used 2.4 GHz band. Also the increase in frequency has as a result a narrower and more directional transmitted signal, however with decreased transmission range. In the proposed 5 GHz band, there is 275 MHz of bandwidth available for spread-spectrum transmission. The same digital modulation that incorporated in ZigBee is used (O-QPSK for 5 GHz band). Hermes uses 55 frequency channels for FHSS with 5 MHz of bandwidth each available for DSSS. Each channel uses DSSS modulation with 270 KHz modulating (pre-spreading) bandwidth and 5 MHz total (two-sided) spread-spectrum signal bandwidth and so a 12.67 dB processing gain. The resulting raw, over-the-air data rate is approximately 252 Kbps per channel in the 5 GHz band. Hermes II nodes are able to perform up to 100.000 frequency hops/sec, so is rather difficult for contemporary fast follow jammers to hop along and jam in the same time.

The sequence of channels used is determined by a channel sequence generation algorithm

that uses a secret key as a seed. This secret key is derived from a secret word, known only to the nodes and the PE, using Password-Based Key Derivation Function 2 (PBKDF2)[30]. Even if the secret word leaks, the adversary is not able to compromise the security of the entire WSN because she would not know the derivation function parameters of the secret key (salt[4], iterations and key length). The encryption key can change upon PE request, at specific time intervals or in arbitrary fashion, depending to nodes computational power and energy availability. The authors propose -for security reasons- to 'hard-code' the initial secret word onto nodes prior to the WSN deployment, however, the PE is able to modify it at any time. The generation of the channels' sequence is done with the use of the Mersenne Twister or MT19937 algorithm [16] combined with a hash function (SHA-1) for enhanced security [34]. Hermes II node also incorporates a DSSS chip with 5 MHz chip rate.

For the synchronization of communication nodes the authors suggest the use of the flooding time synchronization protocol (FSTP) [15] in a predefined frequency channel. FTSP is designed especially for sensor networks and guarantees average precision of 0.5 $\mu s/hop$ in a multi-hop scenario. It uses low communication bandwidth and exhibits proven robustness against node and link failures.

The main advantage of Hermes II is that it deals with the problem of jamming using a powerful hardware scheme, capable of defending a WSN even against the most sophisticated and with unlimited power resources jammers. In simulations that the authors have made Hermes II nodes guarantee a satisfactory packet even in heavily jammed environments where the attacker(s) are able to jam the entire area, the WSN is deployed, with barrage jamming, as opposed to typical sensor nodes communication schemes. However all these advantages come with an increased cost.

As and the authors state the implementation of Hermes nodes is not a straight-forward task due to the technologies incorporated, hence a significant amount of research is needed in various fields. First, a radio unit that complies with the Hermes II standards needs to be designed along with a new communication protocol that uses the 5 GHz band. Even if Hermes node is finally implemented the cost is expected to be considerably high and for sure

[4]Salt is a seed value used in the encryption of a plaintext password to expand the number of possible resulting cipher texts from a given plaintext. The use of a salt value is a defensive measure used to protect encrypted passwords against dictionary attacks.

not affordable for common WSNs. Only WSNs that will be used for applications that need extra high security (e.g. military) could afford the increased cost of Hermes nodes.

How to Secure a Wireless Sensor Network. Law and Havinga in [11] deal with many WSN security aspects including jamming on the physical and data link layer.

In physical layer they concentrate on spread spectrum modulations as ideally countermeasures. They suggest the use of FHSS instead of DSSS because the latter requires more circuitry (higher cost) to implement, is more energy-demanding and more sensitive to environmental effects [17, 28]; on the contrary they claim that the hop rate in a FHSS system is typically much lower than the chip rate in a DSSS system, resulting in lower energy usage [17, 39].

They do not recommend DSSS transceivers in WSNs but only the use of FHSS transceivers. For the latter they suggest the use of quaternary/binary frequency-shift keying (FSK) for data modulation [17, 27] and a hop rate between 500 and 1000 hops/s [38]. Also they state that although a maximum hop rate of 1000 hops/s is not able to cope with most sophisticated jammers [33], however for most of cases 500-1000 hops/s should be a practical compromise. For transceivers that do not support spread spectrum they recommend the channel surfing method by Xu et al.[43].

Finally for jamming on data link layer, in absence of effective countermeasures they propose the use TDMA protocols like LMAC [7] as more resistant to jamming attacks.

The main advantage of this work is the recommendation of specific hardware that can cope with jamming clearly more efficiently than software countermeasures. However FHSS alone, as also noted by the authors, is not able to deal with contemporary fast-follower military jammers, which are able of jamming FHSS communications that perform even thousands of hops/sec [33]. Furthermore the disapproval of DSSS transceivers is not really justified since DSSS presents many advantages against jamming attacks [26]. For instance, since the transmitted signal of DSSS resembles white noise, crucial information for an adversary as the interception of the transmission channel and radio direction finding of the transmitting

source become difficult. Also the use of UWB transceivers [23], which are used in many military systems as an effective countermeasure against jamming, is not considered as a possible countermeasure by the authors.

Regarding the countermeasures against physical layer it is stated that for transceivers not supporting spread spectrum, the channel surfing method by Xu et al. [43] is recommended. Channel surfing though, as detailed in a previous section, is in effect an adaptive form of FHSS, so it uses some type of spread spectrum hardware that allows switching to a different, orthogonal frequency $\pm\delta$ away when it discovers the current frequency is jammed.

1.6.2 Reactive Countermeasures

The main characteristic of reactive countermeasures is that they enable reaction only upon the incident of a jamming attack sensed by the WSN nodes. Reactive countermeasures can be further classified into software and combined software - hardware, similarly to proactive countermeasures.

1.6.2.1 Reactive Software Countermeasures

This category employs the use of exclusively software-based solutions to defend against jamming attacks. Similarly to proactive software countermeasures, this category is also compatible with IEEE 802.15.4-based hardware that is most often used in today's WSN.

JAM: A Jammed-Area Mapping Service for Sensor Networks. JAM algorithm enables the detection and mapping of jammed regions (see Figure 1.6) to increase network efficiency [45]. Data is then simply routed around the jammed regions. The output of the jamming detection module is a JAMMED or UNJAMMED message broadcast to the node's neighbors. However, as the authors stress, a jammed node would not be able to send any messages, since almost all MAC protocols require a carrier sense to indicate a clear channel in order to have clearance for transmission. To deal with this problem, MAC must provide a way

to override carrier-sense so as to allow broadcasting a brief, high-priority, unacknowledged message. However this could lead to the energy exhaustion of the jammed nodes in case of link-layer jamming. The mapping service that the authors propose can provide the following benefits:

- feedback to routing and directory services;
- an effective abstraction at a higher-level than local congestion, failed neighbors and broken routes;
- support for avoiding the region by network-controlled vehicles, military assets, and emergency personnel;
- reports to a base-station for further jamming localization;
- aid to power management strategies for nodes inside and around jammed regions.

In cases that jamming attacks are restricted to small portions of the WSN, JAM has beneficial results for the robustness and functionality of the network. However, this method exhibits several shortcomings: first, it cannot practically defend in the scenario that the attacker jams the entire WSN or a significant percentage of nodes; second, in the case that the attacker targets some specific nodes (e.g. those that guard a security entrance) to obstruct their data transmission, again this technique fails to protect the attacked sensor nodes.

1.6.2.2 Reactive Software-Hardware Combined Countermeasures

This type of countermeasures requires the use of specialized hardware along with proposed software solutions.

Channel Surfing and Spatial Retreat. Xu et al. [43] proposed two evasion strategies against constant jammers: channel surfing and spatial retreat. Channel surfing is essentially an adaptive form of FHSS. Instead of continuously hopping from frequency to frequency,

a node only switches to a different, orthogonal frequency $\pm\delta$ away when it discovers the current frequency is being jammed. The δ value can be determined by experiments, e.g. for Berkeley motes, δ is found to be multiples of 800 kHz [43]. The frequency hopping pattern suggested by [43] is $C(n+1) = C(n)+1 \, mod \, M$. The authors admit the predictability of this pattern and have suggested using of a pre-shared secret between the communicating parties. Finally, a node can detect a jammed medium, if the packet delivery ratio is low while the received signal strength is high [42].

Spatial retreat, which can be applied only upon sensor nodes that have the capability of mobility, is an algorithm according to which two nodes move in Manhattan distances to escape from a jammed region. The key to the success of this strategy, as the authors state, is to decide where the participants should move and how should they coordinate their movements. The main shortcoming of the two above mentioned strategies is that they are effective only against constant jammers and they have no results against more intelligent or follow-on jammers.

Wormhole-Based Anti-Jamming Techniques in Sensor Networks. Wormholes, until recently were considered as a threat for a WSN [21, 24, 8]. However Cagalj et al. proposed a reactive anti-jamming scheme for WSNs using wormholes [4]. The basic idea is that jammed nodes use channel diversity in order to establish a communication with another node outside the jammed area. The authors propose 3 types of wormholes:

- Wired pair of sensors: In this solution the authors propose the construction of a WSN with certain number of pairs of sensor nodes, each connected through a wire. The wired sensors are also equipped with wireless transceivers. To have a large probability that an arbitrary pair forms a wormhole from the exposure region to the area not affected by jamming, it might be required to create a large number of wired pairs. In large-scale WSNs this solution is very expensive and needs a large amount of time for the deployment of the sensor nodes. Also the scenario that an adversary simply tries to cut the wires before the attack should be taken into account.
- Frequency hopping pairs: In this solution enables the creation of pairs by using fre-

quency hopping techniques, like Bluetooth. All pairs are being deployed by wireless links and can afford longer links between pairs. A problem that arises with this solution is the synchronization among the nodes that use FHSS. This problem can be addressed with the use of a time synchronization protocol (e.g. FTSP [15]). Another one problem is that some nodes must be equipped with special and more sophisticated transceivers, which increases significant the cost of the WSN. Also the deployment of the WSN becomes more complex and time consuming. Finally FHSS alone is not an effective countermeasure against fast-follower jammers [33].

- Uncoordinated channel-hopping: In this solution the authors seek to create probabilistic wormholes by using sensor nodes capable of hopping between radio channels that ideally span a large frequency band. Unlike the previously mentioned solution, individual packets are transmitted on a single channel. As a result the hops between the channels are much slower. That simplifies the adversary's work since she has more time in her disposal to recover the channel in use and jam it. Finally the problems of frequency hopping pairs are also applied in this solution.

From the above, we conclude that wormholes may be an interesting idea to defend against jamming attacks but a different approach must be taken. In a large-scale attack or against sophisticated fast follower jammers the proposed countermeasures cannot efficiently protect the WSN.

1.6.3 Mobile Agent-Based Solutions

In this class of anti-jamming approaches enables Mobile Agents (MAs) to enhance the survivability of WSNs. The term MA [25] refers to an autonomous program with the ability to move from host to host and act on behalf of users towards the completion of an assigned task.

Jamming Attack Detection and Countermeasures in WSNs Using Ant System. Muraleedharan and Osadciw propose the use of ant system algorithm as an effective coun-

termeasure against jamming attacks in a WSN [20].In effect, ants may be viewed as a type of mobile agents.

An initial set of ants traverse through the nodes in a random manner and once they reach their destinations, they deposit pheromone on trails as a means of communication indirectly with the other ants. The amount of pheromone left by the previous ant agents increases the probability that the same route is taken during the current iteration. Parameters such as hops, energy, distance, packet loss, signal-to-noise ratio (SNR), bit error rate (BER) and packet delivery affect the probability of selecting a specific path or solution. Also pheromone evaporation over time prevents suboptimal solutions from dominating in the beginning.

The main advantage of the ant solution is that the ant agents spread into the network and continuously try to find optimal and jamming-free routes for data transferring, taking into account crucial node and network parameters (e.g. nodes' remaining energy, packet loss, SNR). In a large WSN they have a clear advantage over other anti-jamming solutions since they can adapt more easily to the jammed environment. An ant agent can remain in a node when this is under attack and move to an adjacent node upon detecting a 'clear' communication channel (jamming pause).

Unfortunately, this system has not been tested in large-scale simulated WSNs (simulations have been conducted in topologies comprising 16 nodes), hence its scalability is questionable. Also the extra computational and energy cost required by ants is not evaluated. Furthermore the authors omitted information on how quickly the "pheromone" trails are able to react to nimble attackers. Finally, in the case that a considerable proportion of WSN nodes are jammed then ants will probably fail to guarantee the uninterrupted network's operation.

JAID: An Algorithm for Data Fusion and Jamming Avoidance on WSNs. In [19] Mpitziopoulos et al. describe the critical role MAs can play in the field of security and robustness of a WSN in addition to data fusion. They propose the Jam Avoidance Itinerary Design (JAID) algorithm. The design objective of JAID algorithm is twofold: (a) to calculate near-optimal routes for MAs that incrementally fuse the data as they visit the nodes; (b) in the face of jamming attacks against the WSN, to modify the itineraries of the

MAs so to avoid the jammed area(s) while not disrupting the efficient data dissemination from working sensors.

To meet the second objective, the Processing Element (PE) uses the JAM algorithm [45] to map the jammed area(s) and identify the problematic nodes[5]. Furthermore, it executes queries in specific time intervals so as to be informed as soon as they resume function. Assuming that not the entire WSN is affected, the MAs are scheduled not to visit the jammed nodes. Instead, they visit nodes in the perimeter of the jammed area(s) that are not affected in order to avoid the security risk and thus the collapse of the WSN. If the number of jammed nodes is below a specific threshold, JAID only modifies the pre-jamming scheduled itineraries ('connects' the cut off nodes to jam-free nodes) to increase the algorithm's promptness. Otherwise, JAID reconstructs the agent itineraries excluding the jammed area(s).

The authors evaluated the performance of JAID in simulated topologies, examining the scenario wherein multiple jammers initiate jamming attacks against a WSN consisted of 100 nodes randomly deployed in a field (see Figure 1.7). They assume that jammers have limited jamming range, not covering the entire WSN because; the authors admit that in case the whole WSN is jammed, no algorithmic solution could effectively defend the network.

The MAs used in JAID have the advantage of excluding jammed and problematic nodes from their itineraries and efficiently deliver the data from the working nodes to the PE. Furthermore JAID calculates near-optimal routes for MAs minimizing the energy cost needed for transmission.

The drawback of JAID is that it cannot defend the WSN in case the jammer(s) exercise efficient attack against all nodes simultaneously. However if a WSN consisted of nodes that utilize specialized spread spectrum radio units (e.g. Hermes II) and used JAID the best of the two worlds could be combined (effective defence even against heavy jamming attacks while maintaining the advantages of JAID, i.e. lower energy consumption, high responsiveness and enhanced security).

[5]Simulation results in [45] in a WSN composed of 121 sensor nodes proved that the mapping activity varies from 1.5 seconds for moderately-connected networks to just over 5 seconds for the largest jammed region. This is fast enough to allow a reasonable real-time response to jamming in the current sensor network.

1.7 Comparison of Anti-Jamming Approaches

Proactive countermeasures are performed in the background, even in jamming-free environments; typically, they cannot be initiated, stopped or resumed on demand. Hence, they enable instant response against jamming at the expense of increased computational and energy cost upon the resource constrained sensor nodes. Thus they defend more efficiently against stealth jamming attacks which may pass undetected for a significant period of time from a reactive countermeasure.

Proactive software countermeasures pose no requirement for specialized hardware; they only utilize the capabilities of IEEE 802.15.4-compliant hardware. Hence, they are compatible with existing nodes' hardware and can be applied on any contemporary WSN. On the contrary, proactive software-hardware combined countermeasures, since they imply new nodes design, are typically associated with prolonged implementation time and relatively high implementation cost. However countermeasures of the particular category demonstrate improved results compared to alternative methods, namely superior resistance against jamming.

Reactive countermeasures need reduced computational and energy cost compared to proactive countermeasures but in the case of stealth or deceptive jamming there is a great possibility for delayed sensing of jamming. Reactive software countermeasures category, similarly to proactive software countermeasures, is also compatible with IEEE 802.15.4-based hardware that is most often used in todays WSN. The approaches belonging to reactive software-hardware combined countermeasures category,because of the need for specialized hardware along with proposed software solutions suffer considerable impact, (a) on the implementation cost of the sensor nodes, and (b) in the deployment complexity of the WSN. On the other hand, reactive software-hardware combined countermeasures present higher effectiveness.

Finally mobile agent-based solutions do not require the use of specialized hardware. However in conjunction with spread spectrum hardware their anti-jamming properties can be significantly improved.

Figure 1.8 lists all the works reviewed in this chapter. We focus on the countermeasures that have been extensively analyzed and evaluated (general-purposed and undocumented countermeasures, e.g the use of spread spectrum hardware, are not listed). Furthermore we assume an efficient number of constant jammers with unlimited power supply that perform spot jamming attacks upon large-scale WSNs. We assume that not all WSN nodes are jammed at a same time. In the "defence" column we evaluate the level of defence each countermeasure provides against the above-mentioned jamming scenario while in "compatibility with existing hardware" column we report if the proposed countermeasures are compatible with existing hardware or need a specialized hardware platform. Finally in "expected implementation/deployment cost" column we evaluate the implementation and deployment cost of each countermeasure.

1.8 Open Research Issues

The constraints of contemporary sensor nodes resources (e.g. limited energy, computation and communication capabilities) and the fact that they are often deployed in insecure or even hostile terrains underline their susceptibility to jamming attacks. Therefore, the problem of jamming on the Physical and Link Data layers of WSNs has been a subject of intense research during the last few years. However, there are still many open research issues, outlined below:

- UWB tranceivers: Despite the proposal of several spread spectrum schemes for defense against jamming attacks, the usage of UWB radio units has not extensively examined, although UWB exhibits many advantages against jamming.

- Mobile Agents: The use of mobile agents for defending against jamming attacks is a partially unexplored and promising method. Currently only two works address jamming in WSNs with the use of MAs [19, 20]. The unique characteristics of mobile agents could be explored to intensify their benefit upon WSNs under jamming attacks (e.g. the fact that travelling agents can temporary remain on their current position and return to the PE with their collected data when they sense clear terrain).

- A new communication protocol that uses the 5 GHz free band, which suffers less interference compared to the heavily used 2.4 GHz band, needs to be proposed and designed.
- The antennas that sensor nodes currently use are omni-directional. The design requirements and the implementation of alternative, interference and jamming-resistant antennas need to be devised.

1.9 Conclusion

This chapter reviewed the main aspects of wireless sensor network security against jamming attacks: vulnerabilities of today's WSNs, types of jammers and attacks, and effective countermeasures against jamming.

It also classifies the research works that deal with jamming in WSNs in three main categories: proactive, reactive and mobile agent based highlighting their relevant positive aspects and shortcomings. Furthermore it highlights open research issues in the field of jamming in WSNs. In the near future, the wider adoption and usage of WSN technologies in military and monitoring applications is expected to bring out the immense importance of this security issue.

References

[1] D. L. Adamy and D. Adamy, "EW 102: A Second Course in Electronic Warfare", Artech House, Inc. Norwood, MA, USA, 2004.

[2] F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine, pp. 102-114, August 2002.

[3] S. Bandyopadhyay, K. Hasuike, S. Horisawa, S. Tawara, "An Adaptive MAC and Directional Routing Protocol for Ad Hoc Wireless Network Using Directional ESPAR Antenna", in Proc. of the ACM Symposium on Mobile Ad Hoc Networking & Computing 2001 (MOBIHOC 2001), Long Beach, California, USA, pp. 243-246 October 2001.

[4] M. Cagalj, S. Capkun, J. P. Hubaux, "Wormhole-Based Anti-Jamming Techniques in Sensor Networks", IEEE Transactions on Mobile Computing, vol. 6, no. 1, pp. 100-114 May, 2006

[5] R.J. Cramer, M.Z. Win, R.A. Scholtz, "Impulse Radio Multipath Characteristics and Diversity Reception",in the Proc. of the IEEE International Conference on Communications ICC'98, pp. 1650-1654, 1998.

[6] Crossbow Technology Inc. http://www.xbow.com/

[7] L.V. Hoesel and P. Havinga, "A Lightweight Medium Access Protocol (LMAC) for Wireless Sensor Networks: Reducing Preamble Transmissions and Transceiver State Switches" in Proc. of the First International Conference on Networked Sensing Systems, Tokyo, 2004.

[8] Y. Hu, A. Perrig, D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks", in Proc. Of the IEEE INFOCOM 2003, vol. 3, pp. 1976-1986 2003.

[9] Y.B. Ko, V. Shankarkumar, N.H. Vaidya, "Medium access control protocols using directional antennas in ad hoc networks", in Proc. of the IEEE INFOCOM 2000, vol. 1, pp. 13-21, March 2000.

[10] Y. Law, P. Hartel, J. den Hartog, P. Havinga, "Link-layer jamming attacks on S-MAC", in Proc. of the 2nd European Workshop on Wireless Sensor Networks (EWSN 2005), pp. 217-225. 2005 [Online]. Available: http://ieeexplore.ieee.org/iel5/9875/31391/01462013.pdf

[11] Y. Law and P. Havinga, " How to Secure a Wireless Sensor Network", in the Proc. of the 2005 International Conference on Intelligent Sensors, Sensor Networks and Information Processing, pp. 89-95, December 2005.

[12] Y. Law, L.V. Hoesel, J. Doumen, P. Hartel, P. Havinga, "Energy-Efficient Link-Layer Jamming Attacks against Wireless Sensor Network MAC Protocols" in Proc. of the Third ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2005), ACM Press,pp. 76-78 2005.

[13] H. Lee, B. Han, Y. Shin, S. Im, "Multipath Characteristics of Impulse Radio Channels", in Proc. of the IEEE Vehicular Technology Conference, pp. 2487-2491, 2000.

[14] Y. Li, H. Man, "Analysis of multipath routing for ad hoc networks using directional antennas" in the Proc. of the IEEE 60th Vehicular Technology Conference, vol. 4, pp.

2759 - 2763, September 2004.

[15] M. Maroti, B. Kusy, G. Simon, A. Ledeczi, "The flooding time synchronization protocol", Technical Report ISIS-04-501, Institute for Software Integrated Systems, Vanderbilt University, Nashville Tennessee, 2004. [Online]. Available: http://www.eecs.harvard.edu/ mdw/course/cs263/papers/ftsp-sensys04.pdf

[16] M. Matsumoto, T. Nishimura, "Mersenne Twister: A 623-dimensionally equidistributed uniform pseudo-random number generator", ACM Transactions on Modeling and Computer Simulation,vol. 8(1), pp. 3-30, 1998.

[17] J. Min, "Analysis and design of a frequency-hopped spread-spectrum transceiver for wireless personal communications", Ph.D. dissertation, University of California, Los Angeles, 1995. [Online]. Available: http://www.icsl.ucla.edu/aagroup/PDF files/tcvr-arch.pdf

[18] A.Mpitziopoulos and D. Gavalas, "Countermeasures Against Radio Jamming Attacks in Wireless Sensor Networks", International Journal of Computer Research, vol. 15(1), March 2007.

[19] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos and G. Pantziou, "JAID: An Algorithm for Data Fusion and Jamming Avoidance on Sensor Networks", Technical Report, TR-2007-09-10, Dept of Cultural Technology & Communication, University of the Aegean, Greece, September 2007. [Online]. Available: http://www.aegean.gr/culturaltec/dgavalas/TR/TR-2007-09-10.pdf

[20] R. Muraleedharan and L. Osadciw, "Jamming Attack Detection and Countermea-sures In Wireless Sensor Network Using Ant System", 2006 SPIE Symposium on Defense and Security, Orlando, FL, April, 2006.

[21] C.S.R. Murthy and B.S. Manoj. "Transport Layer and Security Protocols for Ad Hoc Wireless Networks", in Ad Hoc Wireless Networks: Architectures and Protocols. Prentice Hall PTR, May 2004.

[22] G. Noubir, "On connectivity in ad hoc networks under jamming using directional antennas and mobility", in Proc. of the Wired/Wireless Internet Communications conference, LNCS vol. 2957, pp. 186-200, 2004.

[23] I. Oppermann, L. Stoica, A. Rabbachin, Z. Shelby, J. Haapola, "Uwb wireless sensor networks: Uwen- a practical example", IEEE Communications Magazine, vol. 42(12),

pp. 27-32, December 2004.

[24] P. Papadimitratos and Z. Haas,"Secure routing for mobile ad hoc networks" in Proc. SCS Communication Networks and Distributed Systems Modeling and Simulation, 2002.

[25] V. Pham and A. Karmouch, "Mobile Software Agents: An Overview", IEEE Communications Magazine,vol. 36(7), pp. 26-37, 1998.

[26] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein, "Theory of spread spectrum communications-a tutorial" ,IEEE Transactions on Communications, vol. 20(5), pp. 855-884, 1982.

[27] S. Pollin, B. Bougard, R. Mangharam, L.V. der Perre, F. Catthoor, R. Rajkumar, I. Moerman, "Optimizing transmission and shutdown for energy-efficient packet scheduling in sensor networks", in Proc. of the Second European Workshop on Wireless Sensor Networks (EWSN 2005), IEEE, pp. 290-301, February 2005.

[28] G. J. Pottie and L. P. Clare, "Wireless integrated network sensors: toward low-cost and robust self-organizing security networks", in Sensors, C3I, Information, and Training Technologies for Law Enforcement, ser. SPIE Proceedings, vol. 3577, pp. 86-95, 1999,. [Online]. Available: http://wins.rsc.rockwell.com/publications/spie3577-12.pdf

[29] R. Ramanathan, "On the Performance of Ad Hoc Networks With Beamforming Antennas", ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'01), pp. 95-105, Long Beach, California, USA, October 2001.

[30] RFC 2898, "PKCS #5: Password-Based Cryptography Specification Version 2.0", 2000, http:// rfc. net/ rfc2898 .html

[31] S. Roy, S. Bandyopadhyay, T. Ueda, K. Hasuike, "Multipath Routing in Ad Hoc Wireless Networks with Omni Directional and Directional Antenna: A Comparative Study", in Proc. of 4th International Workshop of Distributed Computing, Mobile and Wireless Computing, IWDC 2002 , pp 184-191, Calcutta, India, December 2002.

[32] K. Sanzgiri, B. Dahill, B. Levine, C Shields,E. Belding-Royer, "A secure routing protocol for ad hoc networks", in Proc. of the 10th IEEE International Conference on Network Protocols, pp. 78-87, November 2002.

[33] D.C. Schleher, "Electronic Warfare in the Information Age". Artech House, Inc. Norwood, MA, USA, July 1999.

[34] B. Schneier. Applied Cryptography : Protocols, Algorithms, and Source Code in C.

Wiley, 2nd Edition, 1995.

[35] E. Shi and A. Perrig, "Designing Secure Sensor Networks", Wireless Communications Magazine, 11(6), pp. 38-43, December 2004.

[36] A. Spyropoulos and C.S. Raghavendra. "Energy Efficient Communications in Ad Hoc Networks Using Directional Antennas", in Proc. of IEEE Conference on Computer Communications (INFOCOM'02), vol. 1, pp. 220-228, New York, USA, June 2002.

[37] SunSpotWorld. http://www.sunspotworld.com/

[38] D.J. Torrieri, "Fundamental limitations on repeater jamming of frequency-hopping communications", IEEE Journal on Selected Areas in Communications, vol. 7(4), pp. 569-575, May 1989.

[39] K. Tovmark, Chipcon Application Note AN014,"Frequency Hopping Systems (Rev. 1.0)", Chipcon AS, Mar. 2002. [Online]. Available: http://www.chipcon.com/files/AN014 Frequency Hopping Systems 1 0.pdf

[40] UWB-wikipedia. http://en.wikipedia.org/wiki/Ultra wideband.

[41] W. Xu, K. Ma, W. Trappe, Y. Zhang, "Jamming sensor networks: attack and defense strategies", IEEE Network Magazine, vol. 20, pp. 41-47, 2006.

[42] W. Xu, W. Trappe, Y. Zhang, T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", in Proc. of the 6th ACM international symposium on Mobile ad hoc networking and computing, pp. 46-57, 2005.

[43] W. Xu, T. Wood, W. Trappe, Y. Zhang."Channel surfing and spatial retreats: defenses against wireless denial of service",in Proc. of the 2004 ACM workshop on Wireless security, pages 80-89, New York, USA, 2004.

[44] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks", Computer, 35(10), pp. 54-62, 2002.

[45] A.D. Wood, J.A. Stankovic, S.H. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks", in Proc. of the 24th IEEE Real-Time Systems Symposium (RTSS'2003), pp. 286-297, 2003.

[46] A. D. Wood, J. A. Stankovic, G. Zhou, "DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks" in the PROC. of the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), pp. 60-69, San Diego, CA, June 2007.

[47] G. Zhou, T. He, J.A. Stankovic, T.F. Abdelzaher, "RID: Radio Interference Detection in Wireless Sensor Networks", in Proc. of the IEEE INFOCOM'2005, vol. 2, pp. 891-901, 2005.

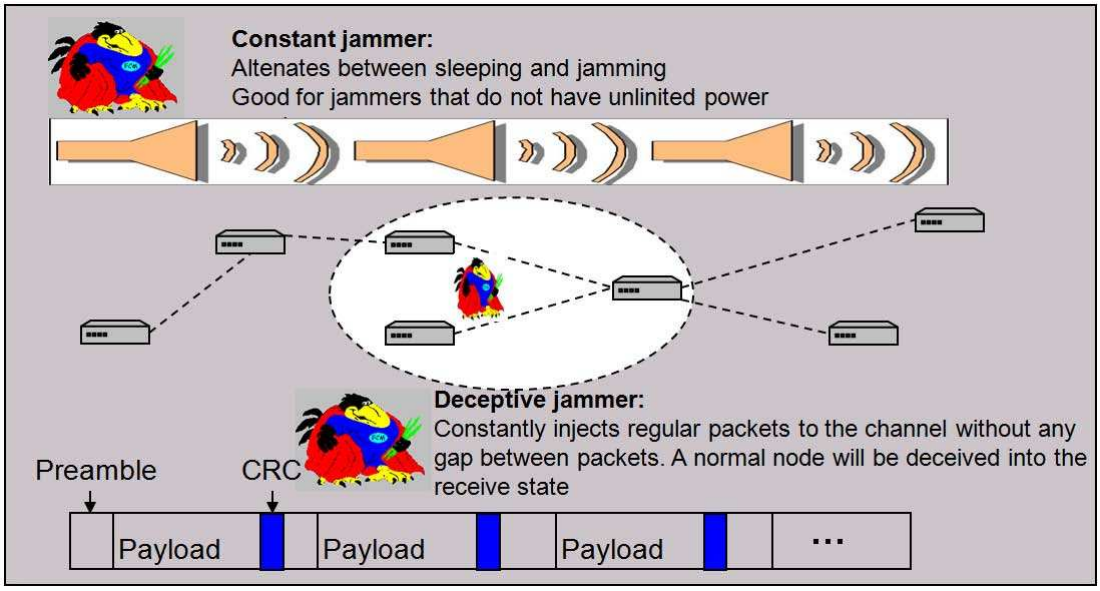

Figure 1.1: Constant and Deceptive jammers

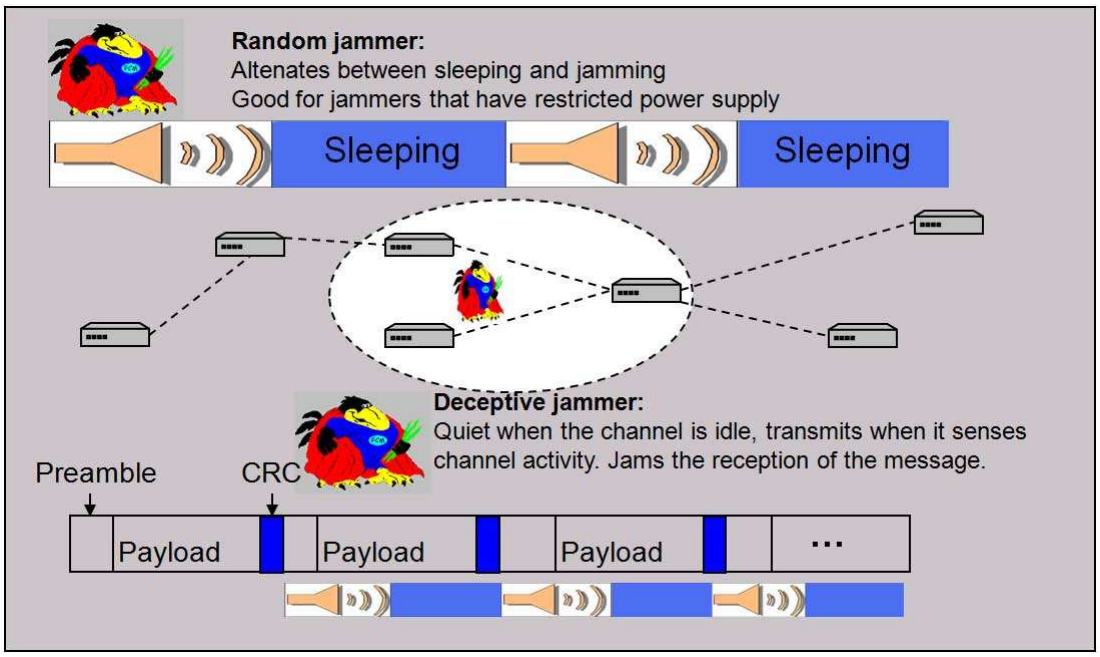

Figure 1.2: Random and Reactive jammers

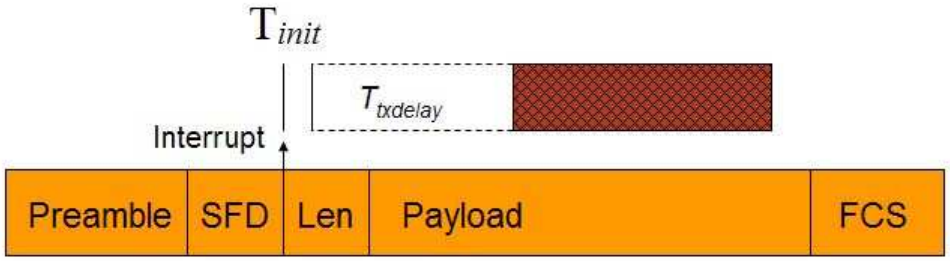

Figure 1.3: Interrupt jamming of packet, triggered by SFD reception. Fcs = Frame Check Sequence, Len = Length of Payload, T_{init} = Time needed for initialization of necessary state or radio chip registers $T_{txdelay}$= Time imposed by the radio hardware for switching on transmitter circuits and oscillator stabilization

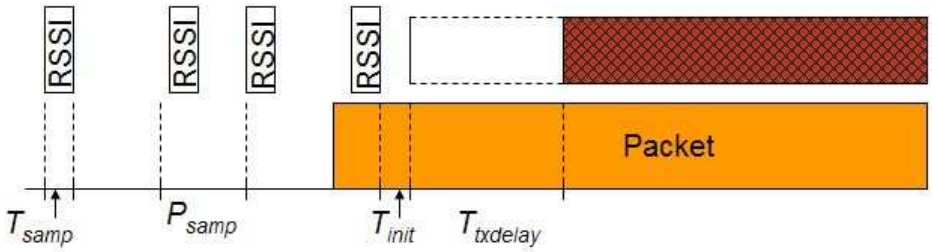

Figure 1.4: Activity jamming attack. RSSI in a single channel is periodically sampled every P_{samp} for T_{sam} time and jamming begins upon packet detection

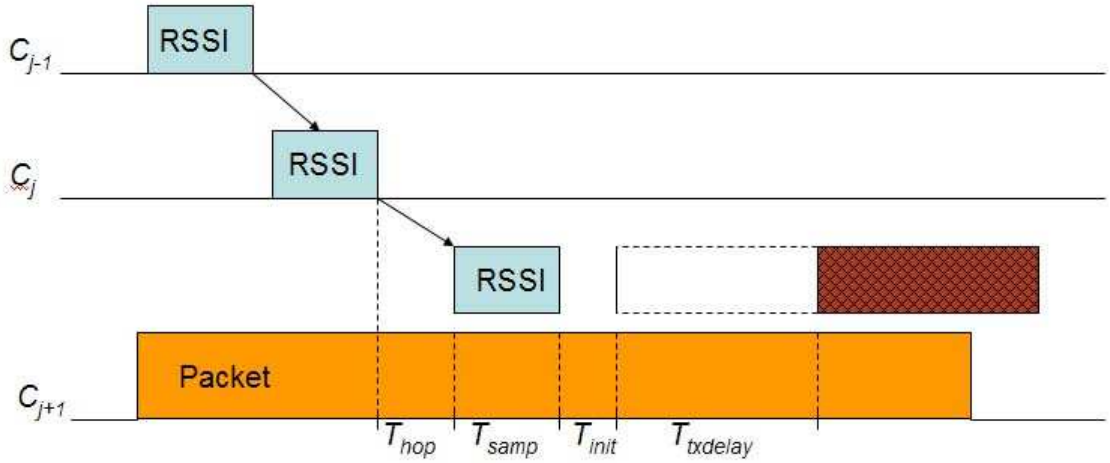

Figure 1.5: Channel scanning for activity, followed by jamming of the message found on C_{j+1} channel

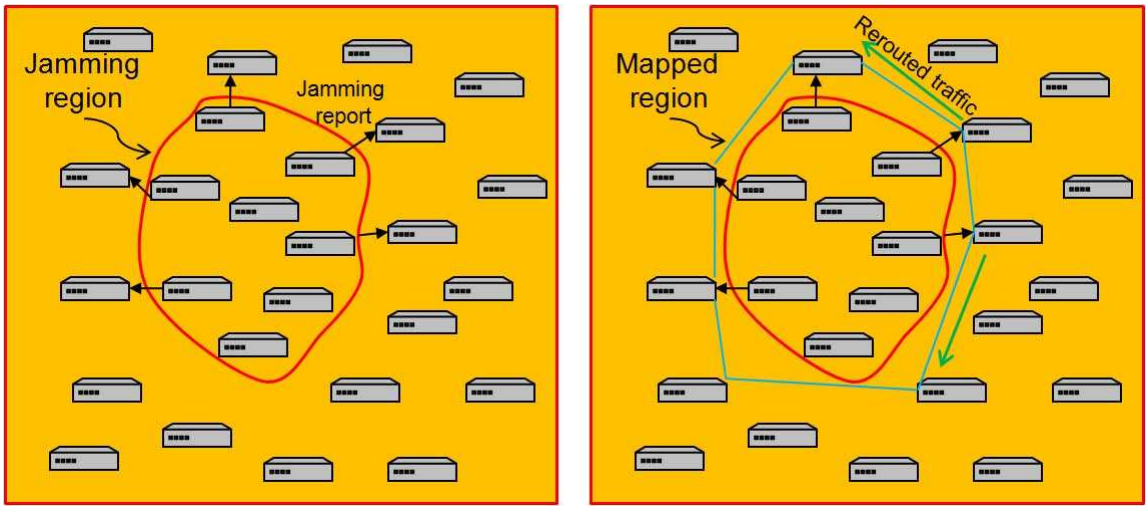

Figure 1.6: Detection and Mapping of jammed region

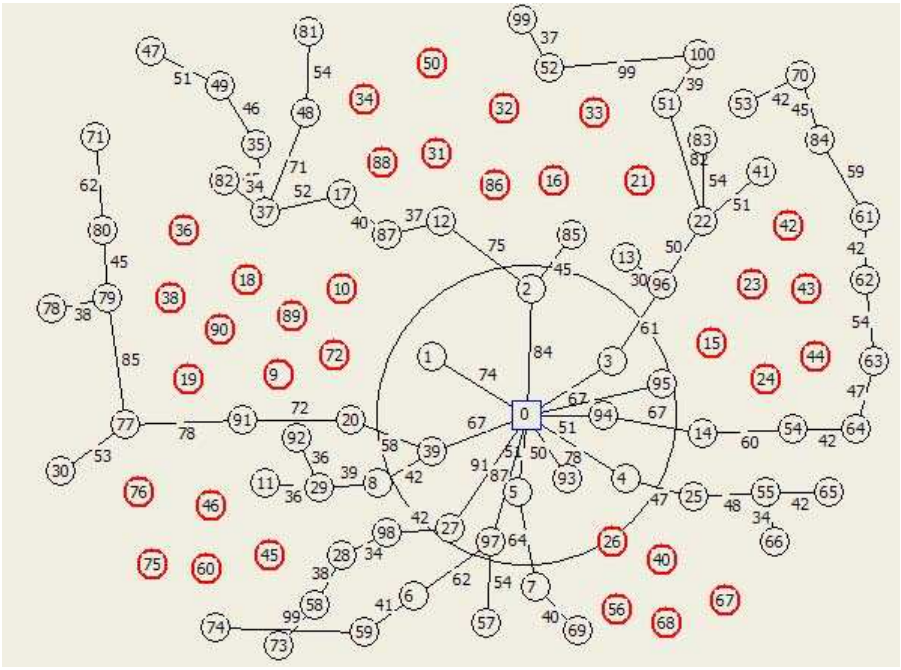

Figure 1.7: Delphi-based simulation of JAID algorithm in case of jamming. The PE is denoted with the blue square and the nodes with the black and red outlined circles. The big circle around PE is its effective transmission range. The red outlined circles represent the jammed nodes

	Proposed countermeasures against jamming	Type of countermeasures	Defence effectiveness	Compatibility with existing hardware	Expected implementation/ deployment cost
Feasibility of Launching and Detecting Jamming Attacks in WSNs	• Detection of jamming using signal strength • Detection of jamming using location information	Proactive Software Proactive Software	Low Low	Yes Yes	Low Low
Energy-Efficient Link-Layer Jamming Attacks against WSN MAC Protocols	• S-MAC: High duty cycle • L-MAC: Shorter data packets • Encryption of link-layer packets. • TDMA protocol • Transmission in randomized intervals	Proactive Software Proactive Software Proactive Software Proactive Software Proactive Software	Low Low Low Low Low	Yes Yes Yes Yes Yes	Medium Medium Low Low Low
Radio Interference Detection Protocol (RID)	a. High-Normal Packet Detection b. Information Sharing c. Interference Calculation	Proactive Software	Low	Yes	Medium
DEEJAM: **Defeating Energy-Efficient Jamming**	a. Frame Masking b. Frequency hopping c. Packet fragmentation d. Redundant encoding	Proactive Software	Medium	Yes	High
Hermes II node	Hybrid FHSS-DSSS	Proactive Software-Hardware	High	No	High
How to Secure a Wireless Sensor Network by Law and Havinga	• FHSS • L-MAC	Proactive Software-Hardware Proactive Software	Medium Low	Partial Yes	High Medium
JAM: A Jammed-Area Mapping Service for Sensor Networks	a. Detection of Jamming b. Mapping of Jammed Area	Reactive Software	Medium	Yes	Medium
Channel Surfing and Spatial Retreat	• Channel Surfing (Adaptive FHSS) • Spatial Retreat	Reactive Software Hardware Reactive Software Hardware	Medium Medium	Partial Partial	High High
Wormhole-Based Anti-Jamming Techniques in Sensor Networks	• Wired pair of sensors • Frequency hopping pairs • Uncoordinated channel-hopping	Reactive Software Hardware Reactive Software Hardware Reactive Software Hardware	High Medium Medium	Partial Partial Partial	High High High
Jamming Attack Detection and Countermeasures in WNS Using Ant System	Ants (Mobile Agents)	Mobile Agent Based	Medium	Yes	Medium
JAID: An Algorithm for Data Fusion and Jamming Avoidance on WSNs	Mobile Agents	Mobile Agent Based	Medium	Yes	Medium

Figure 1.8: Characteristics and features of proposed anti-jamming schemes