SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks. (2008)
Published online in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/sec.81

An effective defensive node against jamming attacks in sensor networks

Aristides Mpitziopoulos*,† and Damianos Gavalas
Department of Cultural Technology and Communication, University of the Aegean, Mytilene, Lesvos, Greece

Summary

Jamming is defined as the act of intentionally directing electromagnetic energy towards a communication system to disrupt or prevent signal transmission. In the context of wireless sensor networks (WSNs), jamming is the type of attack which interferes with the radio frequencies used by sensor nodes and may be viewed as a special case of denial of service (DoS) attacks. Herein, we outline the possible jamming attacks a WSN may encounter. The main contribution of this paper is the outline of the design specifications of a prototype node 'Ares' that effectively defends jamming attacks. Our focus is on frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS), two of the most effective countermeasures against jamming. The main novel aspect of Ares is that it uses a hybrid FHSS–DSSS approach to defend jamming attacks. We suggest the use of a specific FHSS technique in 5 GHz band with 51 frequency channels wherein the channel sequence is generated using a key (which derives from a secret word), known only to the sink and the sensor nodes, as a seed. Each channel uses DSSS modulation with 16-bit pseudo noise (PN) code. The PN code derives from the same key used for FHSS channel generation. The pre-eminence of our method against alternative anti-jamming techniques is demonstrated through extensive simulation tests. Copyright © 2008 John Wiley & Sons, Ltd.

KEY WORDS: jamming; wireless sensor networks; FHSS; DSSS; hybrid

1. Introduction

Jamming represents a type of electronic warfare which interferes with the radio frequencies utilized by network nodes and may be viewed as a special case of denial of service (DoS) attacks. Wood and Stankovic define DoS attacks as 'any event that diminishes or eliminates a network's capacity to perform its expected function' [1]. Typically, DoS prevents or inhibits the normal use or management of communications through flooding a network with 'useless' information. In a jamming attack [2] 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.

In this article, we outline the possible jamming attack scenarios that a WSN may encounter. We propose the adaptation of a hybrid Frequency hopping spread spectrum (FHSS)–direct sequence spread spectrum (DSSS) concept on the particular requirements of WSNs (e.g., limited energy availability

*Correspondence to: Aristides Mpitziopoulos, Xarilaou Trikoypi & Faonos, 81100, Mytilene, Lesvos, Greece.
†E-mail: crmaris@aegean.gr

and transmission range) and explain a simple method to achieve fast and effective nodes' frequency synchronization.

The main contributions of this paper are:

- proposal of several methods that could be implemented in a sensor node to effectively defend jamming attacks;
- introduction of design specifications of a prototype node *Ares* that guarantees network operation even in heavily jammed environments;
- specification of a new physical layer (PHY) which borrows some features from IEEE 802.15.4 [3];
- evaluation and verification of Ares nodes operation in various jamming scenarios through extensive simulation tests that prove the pre-eminence of our method against alternative anti-jamming techniques.

The remainder of the paper is organized as follows: Section 2 reviews work related to our research. Section 3 presents the communication schemes currently used in WSNs and presents their vulnerabilities against jamming. Jamming definition, brief history of jamming and techniques are analyzed in Section 4 while Section 5 presents an overview of possible countermeasures against jamming. In Section 6, we describe the design of Ares node proposed as an efficient anti-jamming node. Section 7 presents and analyzes various simulation results, while Section 8 presents a comparison of anti-jamming techniques. Finally, Section 9 concludes the paper and presents future directions of our work.

2. Proposed Security Schemes Against Jamming in WSNs

The security schemes proposed in the WSN literature to address jamming issue can be categorized in

- detection techniques,
- proactive countermeasures,
- reactive countermeasures, and
- mobile agent (MA)-based countermeasures.

In the following lines, we will briefly present each category along with its corresponding approaches. The relevant advantages and disadvantages of each approach are highlighted and evaluated.

2.1. Detection Techniques

The purpose of detection techniques is to instantly detect jamming attacks. The approaches of this category cannot cope with jamming alone; they can significantly enhance jamming protection only when used in conjunction with other countermeasures by providing valuable data (e.g., the initiation and type of jamming attack).

2.1.1. Radio interference detection in wireless sensor network

Radio interference relations among the nodes of a wireless sensor network (WSN) and the design of a radio interference detection protocol (RID) are discussed in Reference [4]. However, jamming from external sources is not investigated, hence RID remains highly vulnerable from jamming attacks.

2.1.2. The feasibility of launching and detecting jamming attacks in WSNs

In Reference [5] Xu *et al.* claim that understanding the nature of jamming attacks is critical to assuring the operation of wireless networks, so their focus is on the analysis and detection of jamming signals and they do not deal with effective countermeasures against jamming.

2.2. Proactive Countermeasures

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. As a result, they defend more efficiently against stealth jamming attacks, which may pass undetected for a significant period of time from a reactive countermeasure.

2.2.1. DEEJAM

Wood *et al.* in Reference [6] proposed 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 have been someway corrupted. The main advantage are that

DOI: 10.1002/sec

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 [7] nodes. 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.

2.2.2. Energy-efficient link-layer jamming attacks against WSNs' MAC protocols

Law *et al.* [8] examine link-layer jamming algorithms and conclude that in typical contemporary WSN systems no effective measures against link-layer jamming are possible. They recommend: (a) encrypting link-layer packets to ensure a high entry barrier for jammers, (b) the use of spread spectrum hardware, and (c) the use of a TDMA protocol. Yet, neither specific hardware design nor a new efficient communication protocol is proposed as we do herein.

2.2.3. Solution against jamming on the physical and data link layer

Law and Havinga in Reference [9] deal with many WSN security aspects including jamming on the physical and data link layer (DLL). 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/s [2]. Furthermore the disapproval of DSSS transceivers is not really justified since DSSS presents many advantages against jamming attacks [10]. Finally the authors do not propose specific design requirements for jam-resistant nodes.

2.3. 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. Thus they 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.

2.3.1. JAM

Wood and Stankovic propose the detection and mapping of jammed regions [11] to increase network efficiency. However, this method presents several drawbacks: 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 nodes under attack.

2.3.2. Channel surfing and spatial retreat

Xu *et al.* in Reference [12] proposed two evasion strategies against constant jammers: channel surfing and spartial retreat. Channel surfing is essentially an adaptive form of FHSS. Instead of hopping continuously from one channel to another, a node switches to a different channel only when it discovers that the current channel is being jammed. Spartial retreat is an algorithm according to which two nodes move in Manhattan distances to escape from a jammed region. 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.

2.3.3. Wormhole-based anti-jamming techniques in sensor networks

Cagalj *et al.* proposed a reactive anti-jamming scheme for WSNs using wormholes [13]. 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 three types of wormholes: (a) wired pair of sensors (b) frequency hopping pairs, and (c) uncoordinated channel-hopping. In summary, wormholes may be an interesting idea to defend against jamming attacks but many problems still remain, as increased cost, the need for a large amount of time for the deployment of the sensor nodes in large scale WSNs and the fact that FHSS alone is not an effective countermeasure against fast-follower jammers [2].

DOI: 10.1002/sec

2.4. Mobile Agent-based Solutions

This class of anti-jamming approaches enables MAs to enhance the survivability of WSNs. The term MA [14] refers to an autonomous program with the ability to move from host to host and act on behalf of users toward the completion of an assigned task. MA-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.

2.4.1. Jamming attack detection and countermeasures in WSNs using ant system

Muraleedharan and Osadciw propose the use of ant system algorithm as an effective countermeasure against jamming attacks in a WSN [15]. In effect, ants may be viewed as a type of MAs. 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. 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. Notably, the authors omitted information on how quickly the 'pheromon' 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.

2.4.2. JAID algorithm

In Reference [16] we propose the jam avoidance itinerary design (JAID) algorithm which utilizes MA technology [17]. The design objective of JAID algorithm is two-fold: (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 [11] to map the jammed area(s) and identify the problematic nodes. 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).

2.5. Summary From Existing Research Effort

In summary, existing research efforts attempted to solve jamming attacks based on existing hardware and communications protocols [4–6,8,11–13,15,16,18]. To the best of our knowledge, there is no previous work discussing the design requirements of nodes that can effectively defend jamming attacks. Herein, we propose the implementation of innovative hardware that incorporates the most efficient countermeasures against jamming attacks along with a new communication scheme which inherits some characteristics from IEEE 802.15.4 [19,20].

3. Communication Schemes Used in WSNs and their Vulnerabilities Against Jamming

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 PE *via ad hoc* connections with neighbor sensor nodes. A sensor node consists of five basic parts: a sensing unit, a central processing unit (CPU), storage unit, a transceiver unit, and a power unit [21]. It may also have additional application-dependent components attached, such as location finding system (GPS), mobilizer, and power generator.

DOI: 10.1002/sec

3.1. Communication Protocol Stack

The protocol stack used in sensor nodes contains physical, data link, network, transport, and application layers defined as follows [21]:

- Physical layer: responsible for frequency selection, carrier frequency generation, signal deflection, data encryption 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 [8,22] sophisticated jammers can take advantage of the data link layer (DLL) 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.

3.2. ZigBee Protocol and 802.15.4 Standard Overview

A considerable percentage of the nodes currently used in WSN environments comply with the ZigBee [23] 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 802.15.4-2003 [19] or IEEE 802.15.4-2006 [20] low-rate wireless personal area network (WPAN) standard. The standard only specifies the lower protocol layers, the physical layer (PHY), and the MAC portion of the 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, $\mathrm{FC} = (2400 + 5k)\mathrm{M}$, where $k = 1, 2, \ldots$. In 902–928 MHz, there are 10 channels (extended to 30 in 2006) with 2 MHz channel spacing and in 868 MHz 1 channel (extended to 2 in 2006).

The radios use direct-sequence spread spectrum (DSSS) [10] coding in which the transmitted signal takes up more bandwidth than the information signal that is being modulated. In IEEE 802.15.4-2003 [19] two physical layers are specified: BPSK [24] in the 868 MHz and 902–928 MHz, and orthogonal O-QPSK [24] that transmits 2 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, [20] 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 m (33 and 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).

3.3. 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 [19,20] (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 [7] 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.

DOI: 10.1002/sec

4. Jamming Definition, Brief History and Techniques

Jamming is defined as the emission of radio signals aiming at disturbing the transceivers' operation [25]. The main difference between jamming and RF interference (RFI) is that the former is intentional and against a specific target while the latter is unintentional, as a result of nearby transmitters that transmit in the same or very close frequencies (for instance, the coexistence of multiple WSNs on the same area using the same frequency channel may result in RFI).

4.1. Brief History of Jamming

The first occasions of jamming attacks were recorded back in the beginning of the 20th century against military radio telegraphs. Germany and Russia were the first to engage in jamming. The jamming signal most frequently consisted of co-channel characters.

The first wartime jamming activities can be traced back to the World War II, when allied ground radio operators attempted to mislead pilots by giving false instructions in their own language (an example of deceptive jamming). These operators were known by the code name 'Raven' which soon became 'Crow'. The crow represents the universal sign of jamming ever since. Also during World War II the first jamming operations were initiated against a new at that time invention, the radar.

Jamming of foreign radio broadcast stations has been often used during periods of tense international relations and wartime to prevent the listening of radio broadcasts from enemy countries [26]. This type of jamming could be relatively easy to be addressed by the stations with the change of transmitting frequency, adding of additional frequencies and by increasing transmission power.

4.2. Jamming Techniques

The key point in successful jamming attacks is SNR, $\mathrm{SNR} = P_{\mathrm{signal}}/P_{\mathrm{noise}}$ 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 $\mathrm{SNR} < 1$.

Existing jamming methods are described below.

4.2.1. *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.

4.2.2. *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.

4.2.3. *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.

4.2.4. *Deceptive jamming*

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.

In addition to the above-mentioned jamming techniques, techniques for identifying potential jamming targets have also emerged. In particular, RF fingerprinting (RFF) techniques used to identify the subtle and unique characteristics of radio transmission caused by random production differences between RF devices. These unique characteristics can be used to create a unique signature, similar to human fingerprints, for a specific transmission device [27]. In the context

DOI: 10.1002/sec

of jamming attacks, RFF technology may be used by the attacker to identify the adversary's wireless devices identities. For instance, an electronic warfare aircraft that carries RFF equipment can identify a radar by its fingerprint (given that its fingerprint is stored in its database) even if the radar moves to another location and similar radars are scattered in the same area.

5. Countermeasures Against Jamming

In this section, we present countermeasures that deal with possible radio jamming scenarios aiming at informing and familiarizing the reader with the most effective countermeasures against jamming; the latter will be referred to in the next section, while presenting Ares node.

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.

5.2. Frequency-hopping Spread Spectrum (FHSS)

FHSS [10] 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;[‡]
- multiple WSNs can coexist in the same area (such environments would raise serious interference problems using only DSSS modulation).

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 only one carrier frequency. However, transmission in each frequency lasts for a very limited period of time so the frequency is not occupied for long.

5.3. Direct Sequence Spread Spectrum (DSSS)

DSSS [10] 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 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. Also since the transmitted signal of DSSS resembles white noise, radio direction finding of the transmitting source is a difficult task.

5.4. Hybrid FHSS/DSSS

Hybrid FHSS/DSSS [10] 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 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

[‡] 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 [28,52]. FHSS, when the hop rate is quite fast, it 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) is not received at all.

the original signal. Thus hybrid FHSS/DSSS improves the ability to combat the near-far problem [30] [§] which arises in DSSS communications schemes. Another invited feature is the ability to adapt to a variety of channel problems. In the remainder of the paper, we will analyze how hybrid FHSS–DSSS and some of the above-mentioned anti-jamming techniques could be combined in a sensor node and make it almost invulnerable to jamming. We named this prototype node Ares.

5.5. Ultra Wide Band Technology

Ultra wide band (UWB) technology is a modulation technique based on transmitting very short pulses [31] 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.* [32] 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.

5.6. Antenna Polarization

The polarization of an antenna [33] 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 right circular polarization is not able to receive left circularly polarized signals and *vice versa*. 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 incommodes the jamming process because it makes necessary to use specialized jamming equipment with the capability to change its signal polarization rapidly during the jamming.

5.7. Directional Transmission

Today's sensor nodes typically use omni-directional antennas [33]. The use of directional antennas [33] could dramatically improve jamming tolerance in WSNs. In general, directional antennas/transmission provide better protection against eavesdropping, detection, and jamming than omni-directional transmission [34–36]. 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 [37,38] and (b) multipath routing becomes more complex [39,40].

Two types of directional antennas are commonly used in wireless ad hoc networks (sensor networks are not included): sectored [33] and beamforming [41]. 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 WNSs, Noubir [42] proposed the use of sectored antennas for increased resistance to

[§] An example of near–far problem is the following: consider a receiver and two transmitters (one close to the receiver and the other far away). If both transmitters transmit simultaneously at equal powers, the receiver will receive more power from the nearby transmitter. This makes the signal from the distant transmitter more difficult to resolve.

jamming, however the specific antennas are not yet widely available.

6. The Ares Node

Ares nodes use an advanced radio unit capable of hybrid FHSS–DSSS communication. Ares will also have the ability to regulate its transmitted power. [‖] In LPD, operation transmission power will be kept low (0 DBm). In case of strong received signal or interference it will boost transmitted power into anti-jam (AJ) mode with 4 DBm transmitting power.

It is noted that contemporary fast-follower military jammers are capable of jamming FHSS communications that perform even thousands of hops/s [2]; Nevertheless specialized small circuits can make Ares able of performing up to 100 000 frequency hops/s and less vulnerable to jamming by fast follower jammers. To further hinder potential attackers, the use of DSSS modulation is proposed. The main advantage of this approach is that the attacker receives a signal that resembles white noise and cannot detect the communication radio band. As a result, the attacker will monitor the entire band not being aware whether the received signal is noise or actual data (the attacker should discover not only the frequency-hopping sequence but also and the direct sequence PN code). Furthermore, taking into account the limited transmitting power of Ares in LPD mode, the task of the attacker is even more difficult since a very sensitive radio receiver required; even then, it would not be feasible to monitor the entire WSN but only a part of it, unless a number of receivers are scattered in the WSN field.

The band that we propose for communication among Ares nodes is the unlicensed 5 GHz band (5470–5725 MHz for Europe). Since the 2.4 GHz band is heavily used (802.11 b/g WLANs, bluetooth devices, cordless phones, pagers) using the 5 GHz band gives Ares the advantage of restricted interference. Also, as the frequency raises the transmitted signal beam becomes narrower and more directional and covers less distance than for example, a same output power signal in 2.4 GHz band. Some other advantages of 5 GHZ band compared to 2,4 GHZ band are better penetration-scatter of the signal and no abnormal signal absorption by water or damp. In the 5 GHz band that we propose, there is 255 MHz of bandwidth available for spread-spectrum transmission. The same digital modulation that IEEE 802.15.4 incorporates will be used (O-QPSK for 5 GHz band). Ares will have 51 frequency channels for FHSS with 5 MHz of bandwidth each available for DSSS. Each channel will use 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. Ares node as noted above will have the ability to perform frequency hops up to 100 000 times/s.

The sequence of channels used will be determined by a channel sequence generation algorithm that will use as a seed a secret key. This secret key will be derived from a secret word, known only to the nodes and the sink, using password-based key derivation function 2 (PBKDF2) [44]. We would like to note here that the secret key scheme is used for enhanced security. Even if the secret word leaks the adversary would not be able to compromise the security of the entire WSN because she would not know the derivation function parameters of the secret key, (salt[¶] iterations, and key length). The above parameters will be adjusted according to the used nodes capabilities (energy and computational power). The salt used in PBKDF2 will be 2 to 8 bits long, the number of iterations 500– 1000 and the number of bytes for derived keys 16–32 bytes long. The encryption key may change upon sink request or in specific time intervals or arbitrary, depending to nodes computational power and available energy. For security reasons the initial secret word (which the sink can change any time) it will be 'hard-coded' onto nodes prior to the WSN deployment.

A fast and secure way for the generation of sequence is to employ the Mersenne Twister or MT19937 algorithm [45]. The desirable properties of MT19937 in our scheme are: (a) its colossal period of $2^{19937} - 1$; (b) very high order of dimensional equidistribution; (c) the fact that it uses less computationally intensive mathematical functions which means lower energy consumption for the nodes; (d) it passes numerous tests for statistical randomness, including the stringent Diehard tests. Because MT19937 in its native form is

[‖] Many of the contemporary sensor nodes (e.g., Sunspots [43]) posses this ability.

[¶] 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 plain text. The use of a salt value is a defensive measure used to protect encrypted passwords against dictionary attacks.

DOI: 10.1002/sec

not suitable for cryptography (observing a sufficient number of iterates, 624 in the case of MT19937, allows one to predict all future iterates) we combined the algorithm with a hash function (SHA-1) which solves this problem. MT19937 for a word x with w bit width is expressed as the recurrence relation:

$$x_{k+n} = x_{k+m} \otimes \left(x_k^u \,|\, x_{k+1}{}^{l}\right) A \quad k = 0, 1, \ldots \qquad (1)$$

where

- u, l: additional Mersenne Twister tempering bit shifts;
- n: degree of recurrence;
- m: middle word or the number of parallel sequences, $1 \leq m \leq n$;
- A is a sparse matrix ($w \times w$) for fast multiplication.

In our proposed scheme, each character of the secret key is first converted to its corresponding ASCII code. The sum of the individual ASCII codes generate the seed $X(0)$. Each output of MT19937 is hashed with SHA-1. Then the sum of the individual ASCII codes $mod51$ gives the random channel to be used in each iteration.

To illustrate, if the secret word is 'Ares' the secret key is '91fd7303a0942644b13783ae0f16009f'. The parameters used for PBKDF2 function are: Salt = 2008, number of iterations = 1000 and key length = 128 bit. The seed for MT19937 will be $X(0) = [\text{ASCII}(9) + \text{ASCII}(4) + \cdots + \text{ASCII}(9) + \text{ASCII}(f)] = 2041$.

It should be emphasized that despite the limited number of channels (51) used by Ares, the frequency hop rate is 100 000 channels per second, so its very difficult for an adversary to monitor the frequency changes, to log and analyze them in order to reverse engineer the used algorithm. In addition, the use of DSSS modulation makes the intercept of channels used for FHSS even more difficult.

Ares node will have a DSSS chip with 5 MHz chip rate. The PN code, 16 bit long, will also be derived from the seed as follows: For each of the first 16 frequency channels $X(1), \ldots, X(16)$ generated based on the Mersenne Twister Equation (1), we map the corresponding bit of the 16-bit PN code. If the channel number is odd the corresponding PN code bit will equal to 1; if the channel number is even the bit will equal to 0. Using 'Ares' again as the secret word the first 16 generated channels are 40, 15, 19, 16, 20, 51, 3, 32, 20, 42, 19, 22, 9, 49, 5, 3 so the PN code is 0110011000101111. For even more enhanced security, the PN code may periodically change, using different channel numbers at a time for generating the PN bit code. This will make intercepting and jamming of transmitted signal even harder.

Post the deployment of the WSN, the sink will be able to change the secret word or the parameters of PBKDF2 for the secret key derivation using the secure hybrid FHSS/DSSS data scheme. A problem that will arise is that once the network has been deployed, any new joining nodes will not be able to communicate with their peers since they will not be aware of the secret word, the parameters of PBKDF2 and thus the PN code. To overcome this problem, we propose to hard-code the above data on any new joining node. This method also guarantees that the administrator that deploys new nodes in the WSN is authorized and is aware of the confidential data that can acquire directly from the sink.

In order to avoid node compromises and leak of secure data each node will have a unique serial which will transmit initially and upon request to the sink. The sink will keep a map of the deployed nodes and at arbitrary times it will check if they status (i.e., whether they respond to requests). In the scenario that a node does not respond after a specified time interval, the sink will assume failure or compromise and for security reasons will instantly change the parameters of PBKDF2. This is the more cost-efficient way to secure the WSN since tamper proofing would considerably increase the cost of Ares nodes. Furthermore tamper-resistant hardware itself is not always absolutely safe due to various tampering techniques (e.g., microprobing).

Clearly, our proposed scheme requires precise synchronization of communicating nodes so as to perform simultaneous frequency hops. The use of the flooding time synchronization protocol (FTSP) [46] in a specific frequency channel which will be predefined for all the nodes and the sink could solve this problem. FTSP is designed especially for sensor networks and it has an average precision of 0.5 μs per hop in a multi-hop case. It uses low communication bandwidth and is proven to be robust against node and topology changes since no topology is maintained and the algorithm can adapt to the failure of a root node by utilizing periodic flooding of synchronization messages. Its high precision performance is reached by utilizing MAC-layer time stamping and comprehensive error compensation including clock skew estimation.

We would like to stress here that we rejected the use of GPS for synchronization purposes in our scheme because of the fact that GPS signals are highly vulnerable to jamming. In addition, GPS receivers would drastically increase the cost of Ares.

6.1. Discussion About Ares Energy Consumption

The main difference between Ares and IEEE 802.15.4-compatible nodes lies in the addition of an FHSS radio unit along with a DSSS unit (hybrid FHSS/DSSS transmission). DSSS radios use PSK modulation, while FHSS radios use FSK modulation. PSK implementations are more complex (coherent demodulation, AGC, etc); hence, they require additional circuitry than FHSS radios [47,48], which implies higher manufacturing cost. However, FHSS systems cannot achieve the same S/N ratio as DSSS systems [49]. DSSS and FHSS radios result in comparable power consumption, although the energy expenditure of FHSS largely depends on the frequency hopping rate.

The difference of energy expenditure among Ares and IEEE 802.15.4-compatible nodes derives from the FHSS radio unit operation in Ares (the higher chip rate of Ares DSSS radio unit is assumed to have minor impact upon the overall energy consumption).

Most importantly, it should be stressed that under heavy jamming conditions IEEE 802.15.4-based nodes are expected to rapidly exhaust their energy resources due to high rate of lost packets and the resulting re-transmissions. In contrast, the robust Ares scheme ensures high packet delivery rate thereby avoiding unnecessary packet re-transmissions. As evidenced in Section 7, the improvement of packet delivery rate achieved in the Ares scheme guarantees its precedence in terms of power consumption compared to alternative approaches.

7. Simulation Results

Our simulation tests have been carried out using a simulation tool (Figures 1, 2, and 5) developed in Borland Delphi programming language. We have examined a variety of scenarios taking into account various aspects (e.g., jammer and nodes antenna gain, path loss, etc.). Unless otherwise specified, the parameters used throughout the simulation tests, along with the configuration of jammer and nodes/sink, are those shown in Table I. As mentioned in Section 4.2, if SNR < 1 then jamming is considered as effective and therefore packet loss reaches 100%. In our simulations, the power output of the nodes radio unit is 4 dBm and simulation runs last one simulated minute.

Table I. Simulation parameters.

Parameter	Value
Terrain dimensions $x * y$ (m)	800 × 550
# Sensors (including sink)	150
Network transfer rate (Kbps)	250
Frequency (MHz)	2405
Transmitter power (W)	100
Transmitter ant gain (dbi)	15
Node's system gain (dbm)	85
Node's antenna gain (dbi)	2
Node's output power (dbm)	4

Path loss has been modeled using Friis transmission equation (2) [50]. This equation gives a more complete accounting for all the factors from the transmitter to the receiver. Path loss simply reflects the power loss of spreading the energy of an RF signal of a given frequency f out equally over a sphere whose radius d is equal to the distance between the transmitter and receiver.

$$P_{\mathrm{R}_x} = P_{\mathrm{T}_x} \frac{\mathrm{G}_{\mathrm{T}_x} \mathrm{G}_{\mathrm{R}_x} \lambda^2}{16\pi^2 d^2 L} \tag{2}$$

where $\mathrm{G}_{\mathrm{T}_x}$: transmitter antenna gain, $\mathrm{G}_{\mathrm{R}_x}$: receiver antenna gain, λ: wavelength (same units as d), d: distance between T_x and R_x antennas, and L: system loss factor (≤ 1)

The topology of jammer and nodes/sink is random (see Figure 1) and is used throughout all our simulation tests. We assume absence of obstacles and also line-of-sight between the jammer and the nodes. The blue outlined rectangle with caption '0' represents the attacker (jammer), the red outlined circle with caption '1' is the sink while the other numbered circles denote the sensor nodes.

In our first simulation, the WSN follows the IEEE 802.15.4 standard (DSSS modulation) and the nodes are using the first IEEE 802.15.4 channel with center frequency 2405 and 3 MHz bandwidth. We assume that the attacker has the capability for barrage jamming in the entire channel and the output power is 100 W for every MHz in the 3 MHz range. Figures 2 and 3 illustrate the simulation results and the SNR ratio, respectively. The SNR for the sink and the nodes is far below 1, therefore the WSN is completely out of order and the packet loss is 100%.

DOI: 10.1002/sec

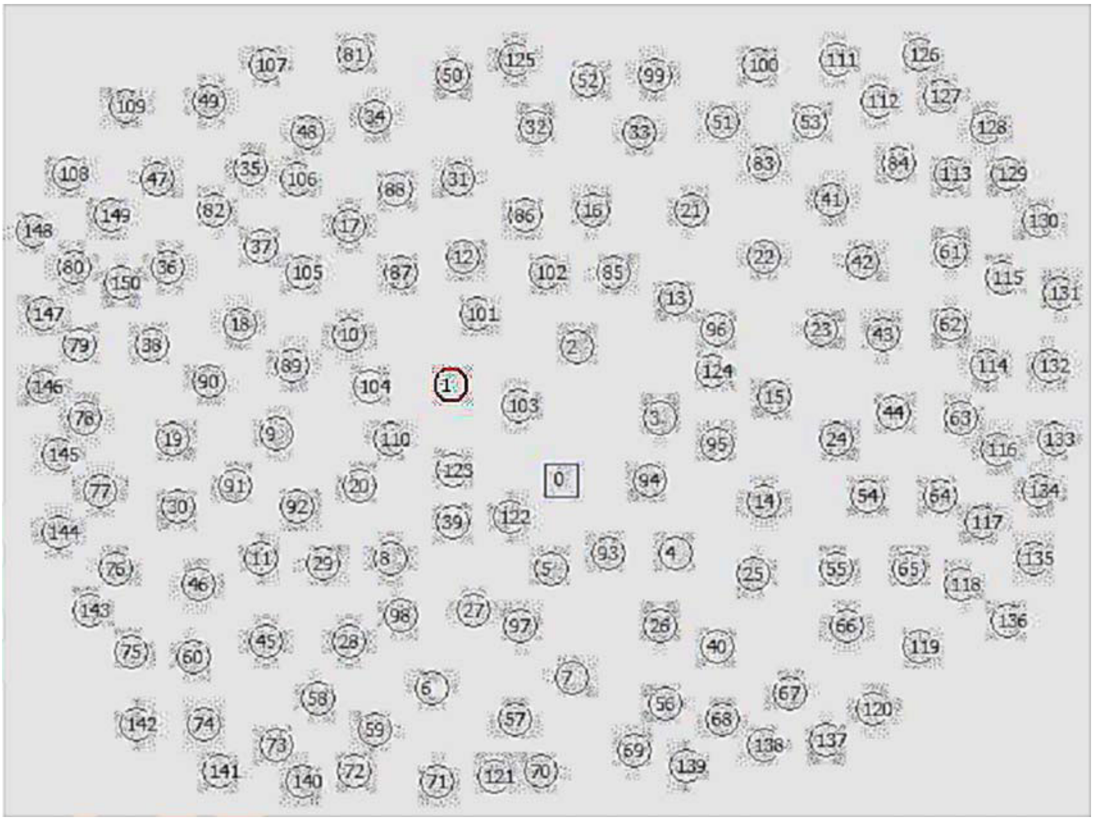
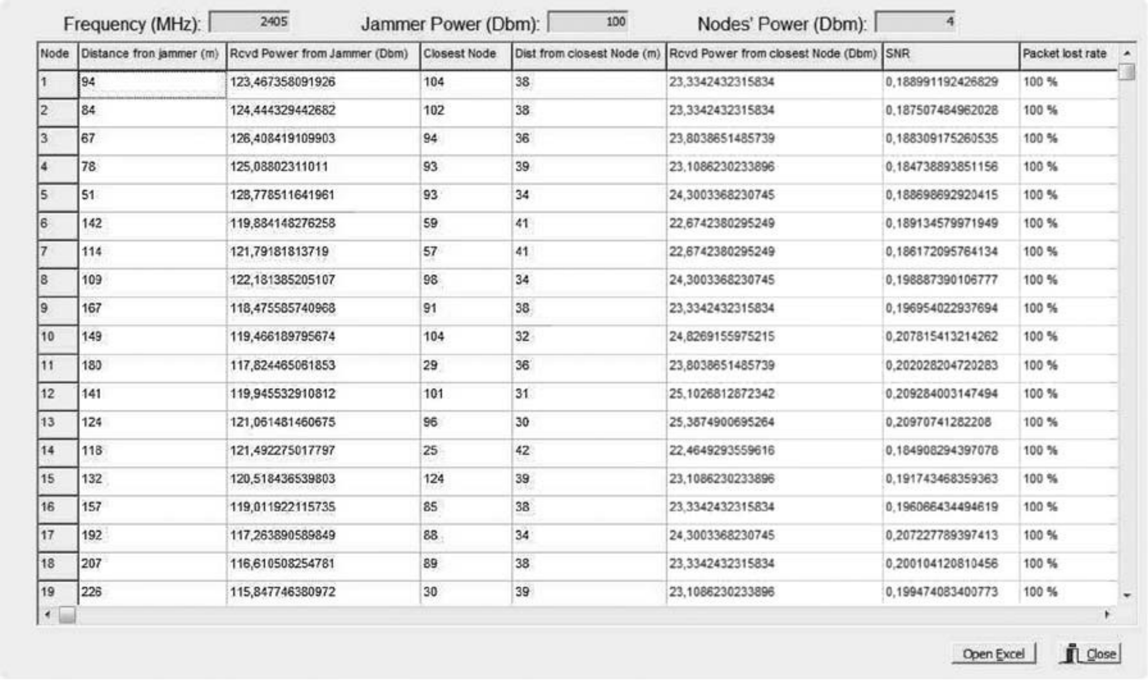


Fig. 1. Jammer and WSN simulated topology.



Frequency (MHz): 2405 Jammer Power (Dbm): 100 Nodes' Power (Dbm): 4

Node	Distance fron jammer (m)	Rcvd Power from Jammer (Dbm)	Closest Node	Dist from closest Node (m)	Rcvd Power from closest Node (Dbm)	SNR	Packet lost rate
1	94	123,467358091926	104	38	23,3342432315834	0,188991192426829	100 %
2	84	124,444329442682	102	38	23,3342432315834	0,187507484962028	100 %
3	67	126,408419109903	94	36	23,8038651485739	0,188309175260535	100 %
4	78	125,08802311011	93	39	23,1086230233896	0,184738893851156	100 %
5	51	128,778511641961	93	34	24,3003368230745	0,188698692920415	100 %
6	142	119,884148276258	59	41	22,6742380295249	0,189134579971949	100 %
7	114	121,79181813719	57	41	22,6742380295249	0,186172095764134	100 %
8	109	122,181385205107	98	34	24,3003368230745	0,198887390106777	100 %
9	167	118,475585740968	91	38	23,3342432315834	0,196954022937694	100 %
10	149	119,466189795674	104	32	24,8269155975215	0,207815413214262	100 %
11	180	117,824465061853	29	36	23,8038651485739	0,202028204720283	100 %
12	141	119,945532910812	101	31	25,1026812872342	0,209284003147494	100 %
13	124	121,061481460675	96	30	25,3874900695264	0,20970741282208	100 %
14	118	121,492275017797	25	42	22,4649293559616	0,184908294397078	100 %
15	132	120,518436539803	124	39	23,1086230233896	0,191743468359363	100 %
16	157	119,011922115735	85	38	23,3342432315834	0,196066434494619	100 %
17	192	117,263890589849	88	34	24,3003368230745	0,207227789397413	100 %
18	207	116,610508254781	89	38	23,3342432315834	0,200104120810456	100 %
19	226	115,847746380972	30	39	23,1086230233896	0,199474083400773	100 %

Fig. 2. Simulation results of jamming 2405 MHz (IEEE 802.15.4).

DOI: 10.1002/sec

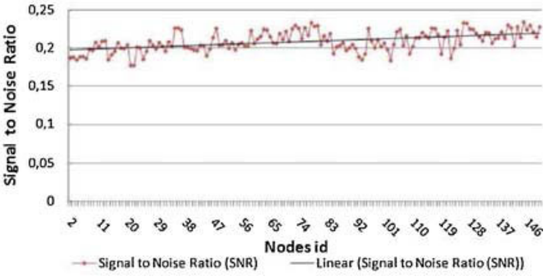
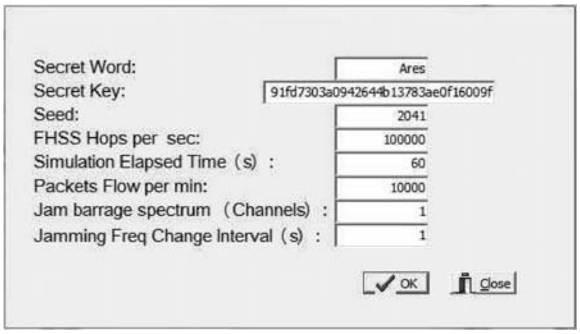


Fig. 3. SNR ratio for simulated WSN (2405 MHz).



Secret Word: Ares
Secret Key: 91fd7303a0942644b13783ae0f16009f
Seed: 2041
FHSS Hops per sec: 100000
Simulation Elapsed Time (s) : 60
Packets Flow per min: 10000
Jam barrage spectrum (Channels) : 1
Jamming Freq Change Interval (s) : 1

Fig. 5. Ares jamming parameters.

Figure 4 illustrates the results of jamming in the 915 MHz. The jamming is once again very effective with SNR far below 1. Consequently, the packet loss is 100%. The final conclusion from the two simulations we have conducted so far is that for a WSN that follows the IEEE 802.15.4 standard (2003 or 2006), a powerful jamming attack can be disastrous for the network, even if the output power of the nodes reaches 4 dBm (typically the output power is 0 dBm).

In the following simulation, we consider a network of Ares nodes. We investigate a jamming scenario wherein the attacker is able to generate 5 MHz barrage jamming with equal output power of 100 W per MHz. Therefore, one channel of the 51 at a time can be jammed. In our simulation, the time interval is 1 s (the jammer changes jamming frequency spectrum every 1 s). The secret word used for generating FHSS channels and DSSS PN code is ‘Ares’. Ares simulation parameters are depicted in Figure 5.

The overall packet traffic for the first simulation is 10 000 packets/min for the entire WSN (packets inter-arrival times follow a gausian distribution). In the second simulation, the packet traffic is 30 000 packets/min and in the third, 60 000 packets/min. Simulation results are illustrated in Figures 6–8 for the first, second, and third simulation, respectively. Notably, Ares nodes achieve a rather high packet success delivery rate (≃98%) and a limited number of jammed channels. It is also shown that the increment of the total packet traffic does not seriously affect the measured packet success ratio. The main conclusion from the simulations is that a WSN composed of Ares nodes is expected to operate efficiently even under heavy barrage jamming attacks.

In the next simulation, we evaluate Ares nodes under a ‘heavy’ jamming scenario where the packet traffic is 50 000 packets/min and the attacker is able to generate 150 MHz barrage jamming with equal output power of 100 W per MHz. Therefore, 30 channels of the 51 at a time can be jammed. The time interval for this simulation is 1 s and jamming lasts for 1 min. Figure 9 illustrates the simulation results (packet success delivery rate for Ares nodes). As we can see even in such a hard jamming scenario the WSN equipped with Ares nodes manages to attain a packet success delivery ratio equivalent to ≈45%.

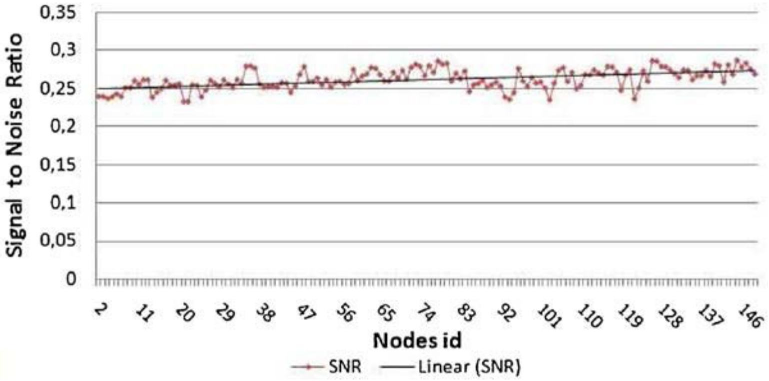


Fig. 4. SNR ratio for simulated WSN (915 MHz).

DOI: 10.1002/sec

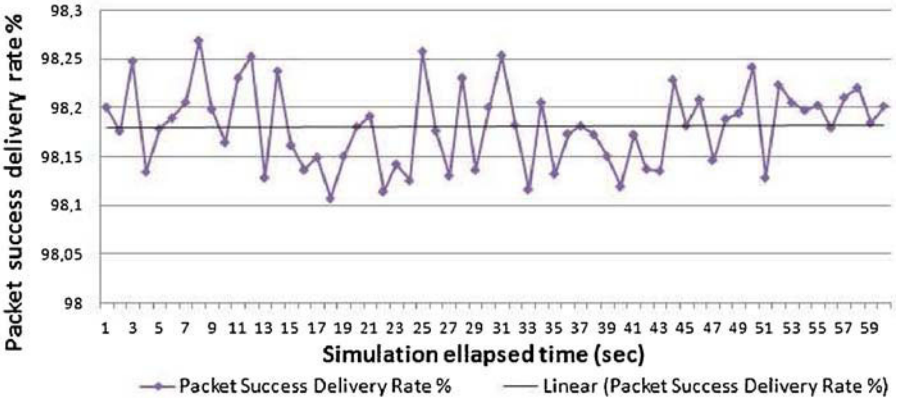


Fig. 6. Simulation results for packet success delivery rate with 10 000 packets/s (Ares jamming).

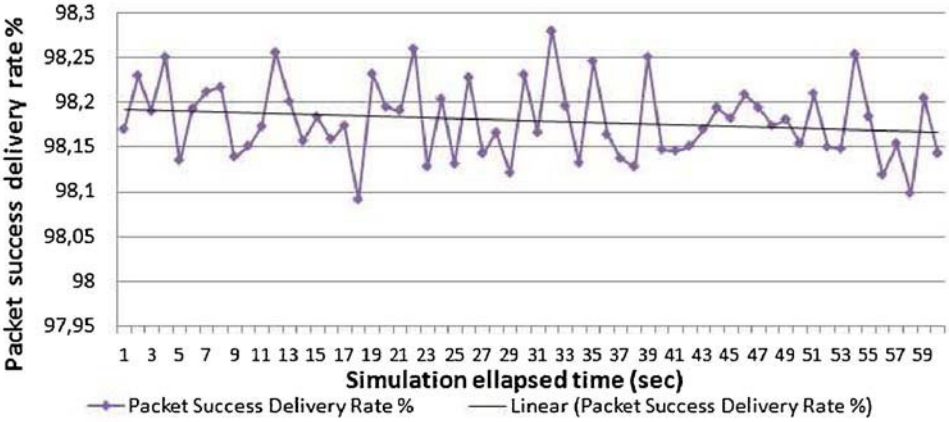


Fig. 7. Simulation results for packet success delivery rate with 30 000 packets/s traffic (Ares jamming).

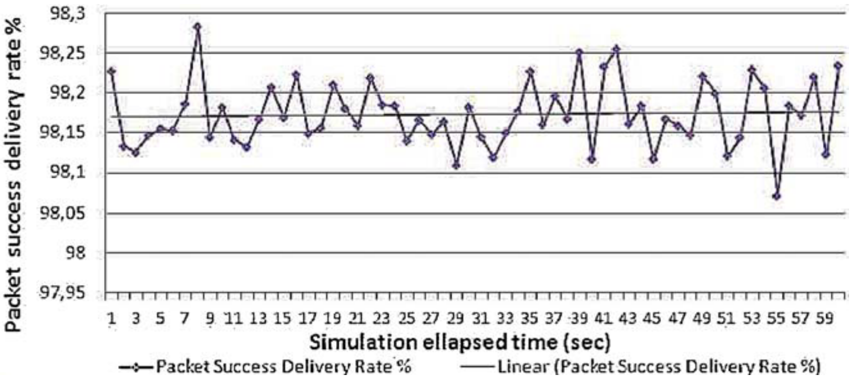


Fig. 8. Simulation results for packet success delivery rate with 60 000 packets/s traffic (Ares jamming).

The next simulation evaluates Ares nodes under a ‘heavy’ jamming scenario, similar to the one used in the previous simulation, for variable number of sensors (100–300 SNs). The results shown in Figure 10 demonstrate a statistical independence of the network’s anti-jamming performance from the network scale. Figure 11 illustrates the average SNR ratio of IEEE 802.15.4-based nodes under

DOI: 10.1002/sec

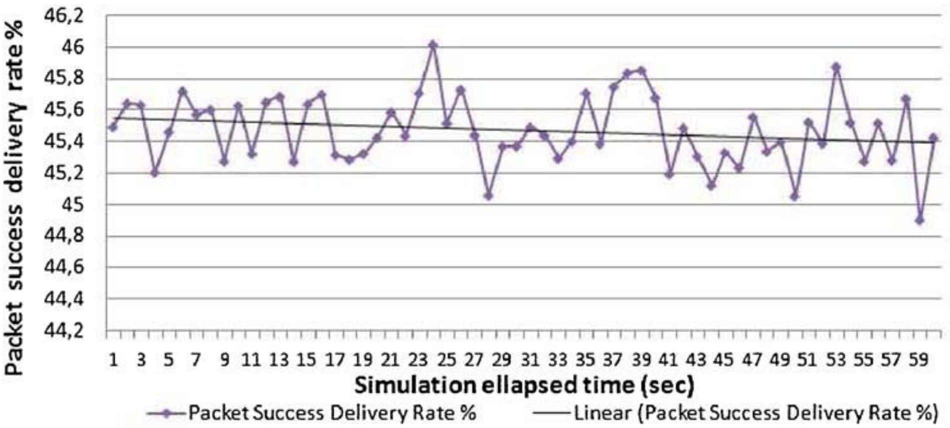


Fig. 9. Simulation results under ‘heavy’ jamming (Ares jamming).

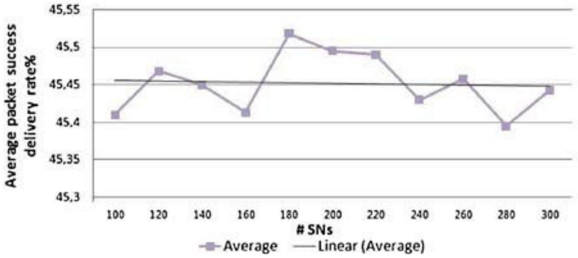


Fig. 10. Simulation results under ‘heavy’ jamming (Ares jamming) and variable number of SNs.

the same jamming scenario. Measuring the SNR steadily below 1, it is concluded that the average packet success delivery rate reaches 0%. Notably, the SNR ratio increases proportionally with the network’s scale. This is due the wider field needed for nodes deployment, so the jammer has to cover a larger area; consequently, the more distant nodes suffer less from jamming as the jamming signal degrades.

The last set of simulation tests evaluate the energy consumption of Ares and IEEE 802.15.4-based nodes in two different scenarios: (a) under normal conditions (assuming no jamming or interference), (b) in the same jamming scenario used in the previous simulations. The energy consumption model used is based on the findings and the energy models detailed in References [51,52]. As shown in Figure 12, Ares poses higher energy demands in normal conditions, due to the operation of the FHSS radio. However, under jamming conditions Ares outperforms 802.15.4-based nodes in terms of energy consumption with sufficient distinct (see Figure 13), due to the higher packet delivery rate achieved by Ares. [#] It should be stressed that the results illustrated in Figure 13 do not take into account the energy spent for the re-transmitted packets which would further increase the energy expenditure gap in favor of the Ares scheme.

8. Comparison of Anti-jamming Techniques

Table II summarizes the relevant characteristics and features of all anti-jamming approaches reviewed in this paper, including our proposal (Ares), and compares them in a scenario that involves a considerable number of constant jammers with unlimited power supply, that perform barrage jamming attacks (100 MHz spectrum with equal output power of 100 W per MHz) upon large-scale WSNs. We also assume that all WSN nodes are concurrently jammed. In the ‘defense effectiveness’ column we evaluate the defense capability that each countermeasure provides with respect to the above-mentioned jamming scenario while in ‘compatibility with existing hardware’ column we comment on whether the proposed countermeasures are compatible with existing hardware or require a specialized hardware platform. Finally in ‘expected

[#] For comparison’s sake, the performance of IEEE 802.15.4-based nodes have received a bounty assuming that their average packet success delivery rate reaches 5% (we have proved that their delivery rate in this jamming scenario drops down to 0%, as shown in Figure 11).

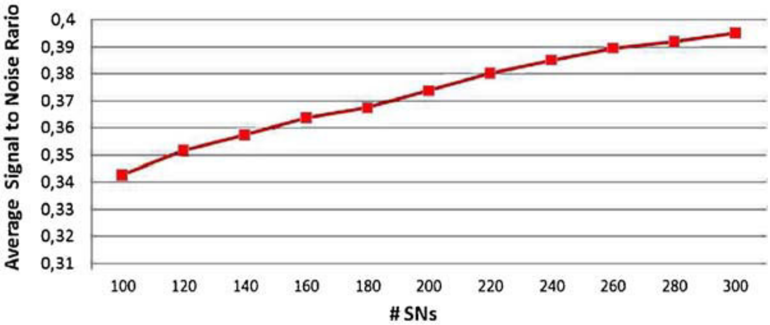


Fig. 11. Simulation results under ‘heavy’ jamming (IEEE 802.15.4-based nodes jamming) and variable number of SNs.

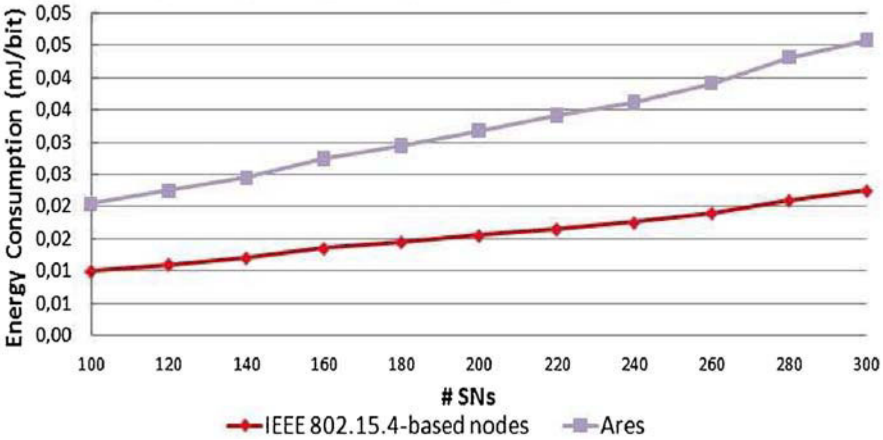


Fig. 12. Energy consumption of IEEE 802.15.4-based nodes and Ares under normal conditions (no jamming/interference) for variable number of SNs.

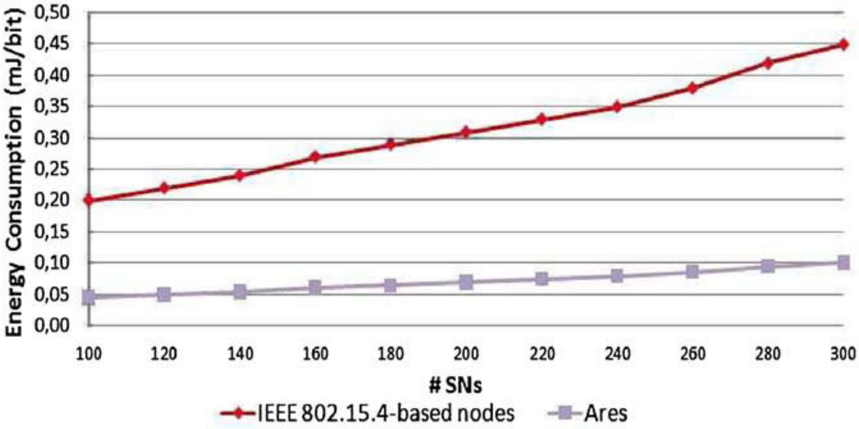


Fig. 13. Energy consumption IEEE 802.15.4-based nodes and Ares under jamming for variable number of SNs.

DOI: 10.1002/sec

Table II. Characteristics and features of other proposed anti-jamming schemes in comparison with ARES.

	Proposed countermeasures against jamming	Type of countermeasures	Defence effectiveness	Compatibility with existing hardware	Expected implementation/ deployment cost	Impact to energy efficiency
DEEJAM: defeating energy-efficient jamming	a. Frame masking b. Frequency hopping c. Packet fragmentation d. Redundant encoding	Proactive software	Low (medium for FHSS)	Yes	High	Medium
Energy-efficient link-layer jamming attacks against WSNs' MAC protocols	• S-MAC: high duty cycle	Proactive software	Low	Yes	Low	Low
	• L-MAC: shorter data packets	Proactive software	Low	Yes	Low	Low
	• Encryption of link-layer packets	Proactive software	Low	Yes	Low	Low
	• TDMA protocol	Proactive software	Low	Yes	Low	Low
	• Transmission in randomized intervals	Proactive software	Low	Yes	Low	Low
Solution against jamming on the physical and DLL by Law and Havinga	• FHSS	Proactive soft–hard	Medium	Partial	High	Medium
	• L-MAC	Proactive software	Low	Yes	Medium	Low
JAM: A jammed-area mapping service for sensor networks	a. Detection of jamming b. Mapping of jammed area	Reactive software	Low	Yes	Medium	Low
Wormhole-based anti-jamming techniques in sensor networks	• Wired pair of sensors	Reactive soft–hard	High	Partial	High	Low
	• Frequency hopping pairs	Reactive soft–hard	Medium	Partial	High	Medium
	• Uncoordinated channel-hopping	Reactive soft–hard	Medium	Partial	High	Low
Jamming attack detection and countermeasures in WNS using ant system	Ants (mobile agents)	Mobile agend-based	Low	Yes	Medium	Low
JAID	Mobile agents	Mobile agent-based	Low	Yes	Medium	Low
ARES node	Hybrid FHSS–DASS	Proactive soft–hard	High	No	High	Medium

implementation/deployment cost' column we evaluate the implementation and deployment cost of each countermeasure.

9. Conclusion

Typical WSNs in use today are highly vulnerable to jamming attacks. In this paper, we presented Ares, a prototype node capable of performing frequency hopping along with DSSS to effectively defend jamming attacks. Our simulations have shown that Ares nodes guarantee a satisfactory packet delivery rate and decreased energy requirement in heavily jammed environments, as opposed to typical sensor nodes communication schemes.

Admittedly, the implementation of Ares node is not a straightforward task due to the technologies that are incorporated, hence a significant amount of research is needed in various fields. First, a radio unit that complies with Ares standards needs to be designed along with a new communication protocol that uses the 5 GHz band.

Our future research will focus on the implementation of Ares node, along with its testing in heavily jammed environments.

References

1. Wood AD, Stankovic JA. Denial of service in sensor networks. *Computer* 2002; **35**(10): 54–62.
2. Schleher DC. *Electronic Warfare in the Information Age*. Artech House, Boston, MA, USA, 1999.
3. Gutierrez JA, Callaway EH, Barrett R. IEEE 802.15.4 Low-Rate Wireless Personal Area Networks. ISBN 0-7381-3677-5 SS95127, October 2003.
4. Zhou G, He T, Stankovic JA, Abdelzaher TF. RID: radio interference detection in wireless sensor networks. In *Proceedings of the IEEE INFOCOM'2005*, 2005.
5. Xu W, Trappe W, Zhang Y, Wood T. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Urbana-Champaign, IL, USA, ISBN:1-59593-004-3, 2005, 46–57.
6. Wood AD, Stankovic JA, Zhou G. DEEJAM: defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks. In *The 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, San Diego, CA, June 2007.
7. Crossbow Technology Inc. http://www.xbow.com/
8. Law Y, van Hoesel L, Doumen J, Hartel PH, Havinga PJM. Energy-efficient link-layer jamming attacks against wirelesssensor network MAC protocols. *Proceedings of SASN'2005*, 2005, 76–88.
9. Law Y, Havinga P. How to secure a wireless sensor network. In *Proceedings of the 2005 International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, December 2005, 89–95.
10. Pickholtz RL, Schilling DL, Milstein LB. Theory of spread spectrum communications-a tutorial. *IEEE Transactions on Communications* 1982; **20**(5): 855–884.
11. Wood AD, Stankovic JA, Son SH. JAM: a jammed-area mapping service for sensor networks. *24th IEEE Real-Time Systems Symposium (RTSS'2003)*, 2003, 286–297.
12. Xu W, Wood T, Trappe W, Zhang Y. Channel surfing and spatial retreats: defenses against wireless denial of service. In *WiSe'04: Proceedings of the 2004 ACM Workshop on Wireless Security*, New York, USA, 2004, 80–89.
13. Cagalj M, Capkun S, Hubaux J-P. Wormhole-based anti-jamming techniques in sensor networks. *IEEE Transactions on Mobile Computing*, May, 2006.
14. Pham V, Karmouch A. Mobile software agents: an overview. *IEEE Communications Magazine* 1998; **36**(7): 26–37.
15. Muraleedharan R, Osadciw L. Jamming attack detection and countermeasures in wireless sensor network using ant system. *2006 SPIE Symposium on Defense and Security*, Orlando, FL, April 2006.
16. Mpitziopoulos A, Gavalas D, Konstantopoulos C, Pantziou G. JAID: an algorithm for data fusion and jamming avoidance on distributed sensor networks. *Pervasive and Mobile Computing*, (in press).
17. Mobile Agents White Paper. General Magic, 1998.
18. Xu W, Ma K, Trappe W, Zhang Y. Jamming sensor networks: attack and defense strategies. *IEEE Network Magazine* 2006; **20**: 41–47.
19. 802.15.4-2003. http://standards.ieee.org/getieee802/download/802.15.3-2003.pdf
20. 802.15.4-2006. http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf
21. Akyildiz F, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. *IEEE Communications Magazine* 2002; 102–114.
22. Law Y, Hartel P, den Hartog J, Havinga P. Link-layer jamming attacks on S-MAC. In *2nd European Workshop on Wireless Sensor Networks (EWSN 2005)*. IEEE, 2005, 217–225. [Online]. Available: http://ieeexplore.ieee.org/iel5/9875/31391/01462013.pdf
23. Zigbee. http://www.zigbee.org/en/index.asp
24. Proakis JG. *Digital Communications*. McGraw Hill: Singapore, 1995.
25. Adamy DL, Adamy D. *EW 102: A Second Course in Electronic Warfare*. Artech House Publishers, Boston, MA, USA, 2004.
26. Radio Jamming Info. http://www.radiojamming.info/ (Accessed 10/5/2008).
27. Hall J, Barbeau M, Kranakis E. Detection of transient in radio frequency fingerprinting using signal phase. *Proceedings of IASTED International Conference on Wireless and Optical Communications (WOC'2003)*, 2003.
28. Cramer RJ, Win MZ, Scholtz RA. Impulse radio multipath characteristics and diversity reception. *IEEE International Conference on Communications ICC'98*, 1998, 1650–1654.

52. Lee H, Han B, Shin Y, Im S. Multipath characteristics of impulse radio channels. *IEEE Vehicular Technology Conference Proceedings*, 2000, 2487–2491.

30. Mohammed AF. Near-far problem in direct-sequence code-division multiple-access systems. In *Proceedings of the 7th IEEE European Conference on Mobile and Personal Communications*, 1993, 151–154.

31. Siwiak K. Ultra-wide band radio: introducing a new technology. *Vehicular Technology Conference, 2001. VTC 2001 Spring. IEEE VTS 53rd*, Vol. 2, 2001, 1088–1093.

32. Oppermann I, Stoica L, Rabbachin A, Shelby Z, Haapola J. Uwb wireless sensor networks: Uwen—a practical example. *IEEE Communications Magazine* 2004; **42**(12): 27–32.

33. Stutzman W, Thiele G. *Antenna Theory and Design* (2nd edn). John Wiley & Sons, New York, USA, ISBN: 978-0-471-02590-0, 1997.

DOI: 10.1002/sec

34. Murthy CSR, Manoj BS. Transport layer and security protocols for ad hoc wireless networks. In *Ad Hoc Wireless Networks: Architectures and Protocols*. Prentice Hall PTR, Eaglewood, Cliffs, NJ, 2004.
35. Ramanathan R. On the performance of ad hoc networks with beamforming antennas. *ACM International Symposium on Mobile Ad Hoc Networking and Computing (Mobi-Hoc'01)*, Long Beach, California, USA, October 2001, 95–105.
36. Spyropoulos A, Raghavendra CS. Energy efficient communications in ad hoc networks using directional antennas. *IEEE Conference on Computer Communications (INFOCOM'02)*, Vol. 1, NY, USA, June 2002, 220–228.
37. Bandyopadhyay S, Hasuike K, Horisawa S, Tawara S. An adaptive MAC and directional routing protocol for ad hoc wireless network using directional ESPAR antenna. In *Proceedings of the ACM Symposium on Mobile Ad Hoc Networking & Computing 2001 (MOBIHOC 2001)*, Long Beach, California, USA, October 2001, 243–246.
38. Ko YB, Shankarkumar V, Vaidya NH. Medium access control protocols using directional antennas in ad hoc networks. In *Proceedings of the IEEE INFOCOM 2000*, Vol. 1, March 2000, 13–21.
39. Li Y, Man H. Analysis of multipath routing for ad hoc networks using directional antennas. *Vehicular Technology Conference, IEEE 60th*, Vol. 4, September 2004, 2759–2763.
40. Roy S, Bandyopadhyay S, Ueda T, Hasuike K. Multipath routing in ad hoc wireless networks with omni directional and directional antenna: a comparative study. In *Proceedings of the 4th International Workshop of Distributed Computing, Mobile and Wireless Computing, IWDC 2002*, Calcutta, India, December 2002, 184–191.
41. Gross FB. *Smart Antennas for Wireless Communications with Matlab*. McGraw-Hill, New York, USA, 2005.
42. Noubir G. On connectivity in ad hoc networks under jamming using directional antennas and mobility. In *Proceedings of the Wired/Wireless Internet Communications Conference*, LNCS Vol. 2957, 2004, 186–200.
43. Sun Microsystems, Sun Spot project home page, http://www.sunspotworld.com/
44. RFC 2898. PKCS #5: Password-based cryptography specification version 2.0: http://rfc.net/rfc2898.html
45. Matsumoto M, Nishimura T. Mersenne Twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Transactions on Modeling and Computer Simulation* 1998; **8**: 3–30.
46. Maroti M, Kusy B, Simon G, Ledeczi A. The flooding time synchronization protocol. *Technical Report ISIS-04-501*, Institute for Software Integrated Systems, Vanderbilt University, Nashville Tennessee, 2004.
47. Min J. 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
48. Pottie GJ, Clare LP. 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, 1999, 86–95. [Online]. Available: http://wins.rsc.rockwell.com/publications/spie3577-12.pdf
49. Morrow RK Jr. A peek into pandora's box: direct sequence vs. frequency hopped spread spectrum. In *Wireless Personal Communications: Emerging Technologies For Enhanced Communications*, Tranter WH, Rappaport TS, Woerner BD, Reed JW (eds). Kluwer Academic Publishers: Norwell, MA, 2006; 305–314.
50. Friis HT. In *Proceedings of IRE*, Vol. 34, 1946, 254.
51. Jabs JL, Chang CH, Tingley R. Performance of a very low power wireless protocol. *Global Telecommunications Conference, GLOBECOM'01*. IEEE, Vol. 5, 2001, 2825–2831.
52. Lee TH, Marshall A, Zhou B. *Modeling Energy Consumption in Error-prone IEEE 802.11-based Wireless Ad-hoc Networks, 9th IFIP/IEEE International Conference on Management of Multimedia and Mobile Networks and Services, MMNS 2006*, Dublin, Ireland, 25–27 October 2006.

DOI: 10.1002/sec