Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 834547, 8 pages
http://dx.doi.org/10.1155/2013/834547

Research Article

Evaluation, Energy Optimization, and Spectrum Analysis of an Artificial Noise Technique to Improve CWSN Security

Javier Blesa, Alvaro Araujo, Elena Romero, and Octavio Nieto-Taladriz

Electronic Engineering Department, ETSI Telecomunicación, Universidad Politécnica de Madrid, 28040 Madrid, Spain

Correspondence should be addressed to Javier Blesa; jblesa@die.upm.es

Received 1 March 2013; Accepted 4 June 2013

Academic Editor: S. Khan

This paper presents the security evaluation, energy consumption optimization, and spectrum scarcity analysis of artificial noise techniques to increase physical-layer security in Cognitive Wireless Sensor Networks (CWSNs). These techniques introduce noise into the spectrum in order to hide real information. Nevertheless, they directly affect two important parameters in Cognitive Wireless Sensor Networks (CWSNs), energy consumption and spectrum utilization. Both are affected because the number of packets transmitted by the network and the active period of the nodes increase. Security evaluation demonstrates that these techniques are effective against eavesdropper attacks, but also optimization allows for the implementation of these approaches in low-resource networks such as Cognitive Wireless Sensor Networks. In this work, the scenario is formally modeled and the optimization according to the simulation results and the impact analysis over the frequency spectrum are presented.

1. Introduction

One of the fastest growing sectors in recent years has undoubtedly been that of Wireless Sensor Networks (WSNs). WSNs consist of spatially distributed autonomous sensors that monitor a wide range of ambient conditions and cooperate to share data across the network. WSNs are increasingly being introduced into our daily lives. Potential fields of applications can be found, ranging from the military to home control commercially or industrially, to name a few. The emergence of new wireless technologies such as Zigbee and IEEE 802.15.4 has allowed for the development of interoperability among commercial products, which is important for ensuring scalability and low cost. Most WSN solutions operate on unlicensed frequency bands. In general, they use Industrial, Scientific, and Medical (ISM) bands, like the worldwide available 2.4 GHz band. This band is also used by a large number of popular wireless applications, for example, those that work over Wi-Fi or Bluetooth. For this reason, unlicensed spectrum bands are becoming overcrowded. As a result, coexistence issues on unlicensed bands have been the subject of extensive research, and in particular, it has been shown that IEEE 802.11 networks can significantly degrade the performance of Zigbee/802.15.4 networks when operating on overlapping frequency bands [1]. The increasing demand for wireless communication presents a challenge to make efficient use of the spectrum. To address this challenge, Cognitive Radio (CR) [2] has emerged as the key technology, which enables opportunistic access to the spectrum. A CR is an intelligent wireless communication system that is aware of its surrounding environment and adapts its internal parameters to achieve reliable and efficient communication. These new networks have a lot of applications, such as the cognitive use of the TV white space spectrum or making secure calls in emergency situations. Adding cognition to the existing WSN infrastructure brings about many benefits. However, cognitive technology will not only provide access to new spectrum bands but will also provide better propagation characteristics. By adaptively changing system parameters like modulation schemes, transmit power, carrier frequency, and constellation size, a wide variety of data rates can be achieved. This will certainly improve power consumption, network life, and reliability in a WSN.

The broadcast characteristic of the wireless medium makes it difficult to shield transmitted signals from unintended recipients. Security in wireless data transmission has

traditionally been performed using cryptographic techniques at the network layer. The main drawback of this approach when deployed to WSN consists in their limited resources, which cannot support the execution of complicated encryption algorithms, resulting in shorter keys that are easier to discover. WSN nodes can also be captured and by using reverse engineering, attackers can turn them for use in their own benefit.

Physical-layer security has become a very interesting approach in the past few years [3]. The main idea behind physical-layer security is to limit the amount of information that can be extracted at the bit level by unauthorized receivers with the exploitation of all available channel state information (CSI). The fundamental problem of WSN is the difficulty to obtain a full CSI. The cognitive paradigm allows for spectrum monitoring and provides this information to the network. Cognitive features such as spectrum sensing, adaptation, and collaboration involve more resources in terms of energy consumption and spectrum saturation. Security mechanisms also make these problems worse. Therefore, the analysis, but also the optimization of the technique, is essential for Cognitive Wireless Sensor Network scenarios, where computational and energy resources are very limited.

Another difference between Cognitive Networks and CWSNs is the role of Primary Users (PUs) and Secondary Users (SUs). We assume a different behavior for the SUs and PUs in CWSNs because of the nature of these networks. For example, CWSNs usually operate on ISM bands, where anyone can transmit without a license. Because of this feature, the definition of Primary Users (PUs) and Secondary Users (SUs) should be different. For this CWSNs definition, the differences between PUs and SUs are based on the priority of their functionality. For example, a fire sensor would have more priority than a temperature sensor. While PUs take preference because they are responsible for critical sensors and information; SUs only send the information when the channel is free.

This paper presents the evaluation, the energy optimization, and the spectrum scarcity analysis of artificial noise techniques to increase physical-layer security in Cognitive Wireless Sensor Networks (CWSNs). These approaches introduce noise in the spectrum in order to hide the real information. They can operate independently of the higher layers in order to complement security. The limitation of resources is one of the motivations in order to integrate this security approach that complements higher-level techniques, such as encryption or specific routing. In other scenarios with fewer limitations, encryption could be a good solution, but in WSNs the encryption algorithms are not strong enough and advanced attackers can decrypt the real information easily. The introduction of noise into the area makes the obtaining and decryption process much more difficult for attackers.

The organization of this paper is as follows. Section 2 shows a related work about physical-layer security strategies. Section 3 indicates the specific characteristics of the presented scenario in the work. Then, Section 4 presents in more detail the approach and Section 5 the evaluation, the optimization, and the simulation results. Finally, Section 6 summarizes the main conclusions of this work.

2. Physical-Layer Security Approaches

The physical-layer security in CWSN is a new area where the investigation is in a very early state. Moreover, the energy optimization of these techniques has not been investigated yet. There are some previous researches about efficient transmissions [4] or spectrum sensing [5], but there is not energy optimization or spectrum analysis for security approaches in CWSN.

Therefore, in this section, we introduce schemes that could be used to achieve physical-layer security against different attacks in WSNs, which share common features with CWSN.

In recent years, the main issues of secure channel capacity have drawn much attention within the information theory community. Most of the works are focused on schemes to obtain the secrecy capacity with different Channel State Information (CSI) approaches. Barros and Rodrigues [6] developed a secure communication protocol to ensure wireless information-theoretic security based on common randomness via opportunistic transmission, message reconciliation, common key generation via privacy amplification, and, finally, message protection with a secret key. It was shown that the protocol is effective in secure key renewal even in the presence of imperfect CSI.

Other methods have been proposed to avoid attacks based on the exploitation of channel characteristics. The RF fingerprinting system implemented by Sperandio and Flikkema [7] consists of a multiple sensor system that captures and extracts RF features from each receiver signal. An intrusion detector processes the feature sets and generates a dynamic fingerprint for each internal source identifier derived from a few packets. This system monitors the temporal evolution and alerts when a strange fingerprint is detected. In [8] Li and Ratazzi propose a precoding scheme, in which the transmitted code vectors are generated by singular value decomposition of the correlation matrix, which describes the channel characteristic features between the transmitter and the intended receiver. Due to the differences in the multipath structure of the transmitter-receiver channels, even intruders with a perfect knowledge of the transmission code vectors are not able to acquire the true messages due to the difference between the locations of the intruders and the legitimate users.

Code approaches improve resilience against jamming and eavesdropping. In [9], a combination of turbo coding and the Advanced Encryption Standard (AES) cryptosystem is proposed. An error in the received ciphertext can cause a large number of errors in plaintext after decoding. Depending on the channel condition, this method can be adopted to choose the number of redundant bits required to protect the information, in order to achieve high efficiency. Another technique is the Spread Spectrum Coding, in which signal is spread by a pseudo-noise sequence over a wide-frequency bandwidth much wider than that contained in the frequency ambit of the original information. The main difference between convention cryptographic systems and spread-spectrum systems lies in their key sizes. Traditional systems can have a very large key space. However, in a spread-spectrum system, the key space is limited by the range of carrier frequencies

and the number of different sequences. In [10], a method is proposed to enhance the physical-layer security of a CDMA system by using AES operations to generate the scrambling sequences. Data protection can also be provided using power approaches. The method proposed in [11] ensures secure communications depending on the channels condition. This method shows that a good secrecy can be achieved when the intruders channel is noisier than the receiver's channel. Artificial noise is generated using multiple antennas or the coordination of helping nodes and is injected into the null subspace of the intended receivers channel.

Discriminatory channel estimation is performed by injecting artificial noise to the left null space of the legitimate receivers channel to degrade the estimation performance of the eavesdropper [12]. By exploiting the channel feedback information from the legitimate receiver at the beginning of each communication stage, a multistage training-based channel estimation scheme is proposed [13]. It focuses on minimizing the normalized mean squared error of the channel estimation at the legitimate receiver subject to a constraint on the estimation performance attainable by the nonlegitimate receiver.

Most of these approaches can be improved using cognitive capabilities. The cognitive paradigm [14] provides a new scenario thanks to spectrum sensing, protocols to share information, and collaboration to optimize the communications.

The works presented in this section support the idea of artificial noise as a possible security option both in WSN and CWSN, but energy optimization and spectrum saturation are two fundamental keys in CWSNs that should be analyzed.

3. Assumptions and CWSN Scenario

In this section, the network and adversary models studied in this paper are described. This is necessary in order to define where the proposed technique is applicable.

3.1. Network Model. In our model, a CWSN consists of a set $S = \{s_1, s_2, \ldots, s_n\}$ of n cognitive wireless sensor nodes. Each node can communicate with other nodes within certain range.

All nodes have cognitive capabilities. Thus, each node has N_W different wireless configurations (physical channels and modulations). All sensors run some discovery routine and they can record the current spectrum state. We also assume that all these nodes can collude among themselves, sharing information and selecting the best available communication configuration. We further assume the existence of a Virtual Control Channel (VCC) to share this information, with no extra overhead over regular cognitive communications.

We consider a four-terminal system composed of a legitimate source (S) that sends the message to a legitimate destination (D), one or more relay nodes (R), and one or more eavesdroppers (E). Because of the cognitive capabilities there are no multipath routing schemes; only one path is chosen each time for the communication.

The above assumptions are light and realistic, considering usual WSN scenarios such us house monitoring, military, and infrastructure protection.

Table 1: Power consumption with different measurement methods.

	TX/RX mode (0 dBm)	Sleep mode
An ammeter	28 mA	160 uA
Dig. ammeter	27,7 mA	146,6 uA
Oscilloscope	26,7 mA	0 mA

3.2. Adversary Model. In this system model the adversaries are eavesdroppers. We assume a global adversary controlling some eavesdroppers which can collaboratively overhear all messages on the incoming and outgoing channels of the closer sensor nodes. Our eavesdropper model is captured by the following set of assumptions for the eavesdropper E: (i) E is a wireless node with N_K wireless configurations (where $N_K \leq N_W$); (ii) E can perform sophisticated spectrum processing with its available elements; (iii) network does not have any information about the position of E or its strategy; (iv) the eavesdroppers communicate among themselves via a separate channel invisible to the rest of the network. We point out that the assumption of a global eavesdropper who can monitor the entire network traffic is realistic for some applications.

We also assume that the eavesdroppers are passive; hence they cannot transmit noise signals. One eavesdropper can sense the spectrum using its different wireless configuration. They can collude among themselves, sharing information to obtain a global spectrum state.

We define the behavior of the eavesdroppers according to these assumptions:

(i) the eavesdroppers have cognitive capabilities, such as multiple interfaces or spectrum sensing,

(ii) the eavesdroppers sense the available channels and interfaces during a period of time. If they do not locate any signal they commute to the next channel or interface,

(iii) if an eavesdropper detects a signal, it will listen during a period of time in the same channel.

3.3. Power Consumption Model. The power consumption model used in this work represents the Texas Instruments CC2530 System-on-Chip Solution for 2.4 GHz IEEE 802.15.4 and ZigBee Applications transceiver [15] and the rest of the hardware consumptions. The hardware power consumption, excluding the radio interfaces, is modeled constantly because we assume it is negligible against the wireless transceivers ones.

The model has been completed with real data extracted from measurements in the Texas Instruments SmartRF05 evaluation board. These measurements include power consumption in transmission, reception, and sleep modes. Moreover, the model includes the power consumption in the transition between modes and the time spent on it.

The measurements in Table 1 are consistent with the theoretical values supported by the company. This table presents the measures captured in real devices that complement the simulator. The theoretical transmission power in 0 dBm is between 28.1 and 29.2 mA. The sleep mode consumption

Table 2: Delay transition matrix in CC2530.

	TX	RX	Sleep
TX	—	192 ms	120 ms
RX	192 ms	—	120 ms
Sleep	120 ms	120 ms	—

measure was the mode 2. Theoretically, the consumption in this mode is 190 uA. As we can see the transmission and reception modes consume the same energy, indicating the activation of the RF module.

Switch times among modes are based on the hardware specification. The delay transition matrix can be observed in Table 2.

4. Cooperative Artificial Noise Scheme

The key idea in this paper is that a transmitter, in cooperation with helper nodes, can artificially generate noise to conceal the secret message that it is transmitting. The noise is generated in such a way that only the eavesdropper is affected but the intended receiver is not because noise is generated in an orthogonal channel or modulation. This technique creates a difficulty in obtaining real information and also in the decryption process in the worst case, when the eavesdropper senses real packets.

CWSNs avoid one of the main constraints when using artificial noise injection techniques, the knowledge of the channel state information (CSI). In this approach, otherwise inactive nodes in the relay network can be used as cooperative artificial noise sources to confuse the eavesdropper and provide better performance in terms of security. In addition, we allow noncolluding eavesdroppers (E) to individually overhear the communication between S and D without any central processing. Based on [16] idea, adapting these concepts to new scenarios, a formal modeling is presented. Zhou and McKay present the base of this modeling in a multiantenna scenario. In this work, the scenario is formally modeled based on this mathematical base and adapted to a cognitive scenario, where the collaboration and the spectrum sensing can be used to improve the technique. Moreover, in [16] there are no relay nodes; the nodes can transmit at the same time for more than one antenna and there is no any presented optimization according the spectrum saturation or the energy consumption.

We denote the possible wireless configurations between S and D and between S and E as h and g, respectively, both of which are $1\times N_W$ vectors, where N_W is the number of different wireless configurations in S:

$$h = \left\{h_1, \ldots h_{N_W}\right\}, \quad g = \left\{g_1, \ldots g_{N_W}\right\}. \tag{1}$$

The elements of h and g are independent and identically distributed complex Gaussian random variables:

$$h_i, g_i = h_i(t), g_i(t) = \frac{1}{\sigma\sqrt{2\pi}} e^{-t/2\sigma}. \tag{2}$$

Knowledge of h is obtained using spectrum sensing capabilities. We assume that the knowledge of h and g is available at E, which makes the secrecy of the communication independent of the wireless configuration and the channel. S utilizes multiple wireless configurations to transmit the information-bearing signal into the receiver's channel, while simultaneously generating a noise-like signal into the null space of the receiver's channel. We let an $N_W \times N_W$ matrix $W = [w_1\ W_2]$ be an orthonormal basis of $\mathbb{C}^{N_W}$, where $w_1 = h/\|h\|$ and W_2, is orthonormal to h. The transmitted symbol vector at S is given by $x = w_1 u + W_2 v$, where the variance of the information symbol u is σ_u^2 and the $N_W - 1$ elements of v are independent and identically distributed complex Gaussian random variables, each with a variance of σ_v^2. The information-bearing signal is represented by u and v represents the artificial noise. Therefore, the received symbols at D and E are given, respectively, by

$$y_D = hx + n = hw_1 u + hW_2 v + n = \|h\|^2 u + n, \tag{3}$$

$$y_E = Gx + e = Gw_1 u + GW_2 v + e, \tag{4}$$

where n and e are the additive white Gaussian noises (AWGN) in D and E with variances of σ_n^2 and σ_e^2, respectively. G is a matrix $N_E \times N_w$, where the N_E is the number of eavesdroppers. We see in (3) that w_1 spans the null space of h; hence the artificial noise v does not affect the received signal at D.

However, the received signal in E is a combination of two unknown Gaussian distributions. Even though E knows h and G channel affection, it does not know the weights W, so it is impossible for it to distinguish the signal u and the noise v. We consider a total power per transmission denoted by P:

$$P = \sigma_u^2 + \left(N_W - 1\right)\sigma_v^2. \tag{5}$$

We refer to P/σ_n^2 as the transmission signal-to-noise ratio (SNR). As an important characteristic of this scheme and a conclusion of the model, the artificial noise is always generated in the orthonormal channels of the information. Therefore, we assume that the noise does not affect the legitimate transmissions.

5. Results

In order to compare the security using this cooperative artificial noise technique with systems without physical-layer security strategies, metrics are necessary. For this purpose the secrecy rate and the secrecy outage probability are defined. The secrecy rate is the rate of transmission on the main channel that remains undecodable to the eavesdropper. When larger networks with multiple transmitters/receivers/eavesdroppers, as well as additional nodes such as relays, are considered, we can define the corresponding secrecy rate regions, or the aggregate secrecy sum rate.

A performance metric suitable for nonergodic channels is the secrecy outage probability (SOP), which describes the probability that a target secrecy rate is not achieved. The SOP characterizes the likelihood of simultaneously reliable and secure data transmission.

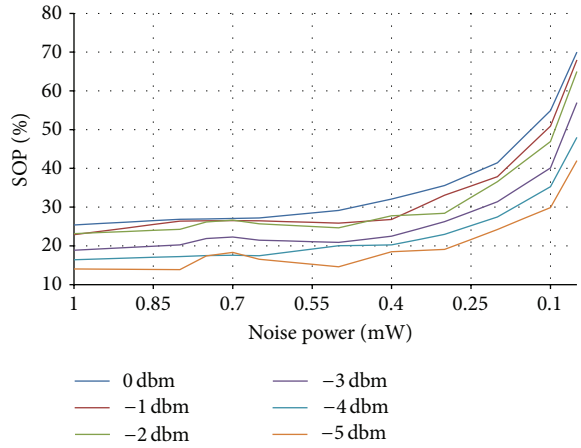

Figure 1: SOP for different emitter and noise power with 5 jamming nodes.

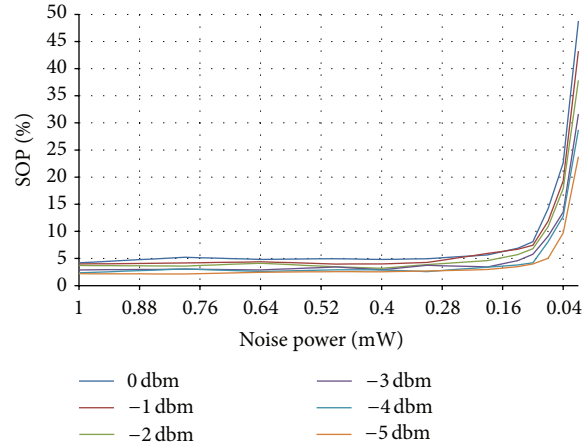

Figure 2: SOP for different emitting and noise power with 20 jamming nodes.

The efficacy of this scheme for different example scenarios using these metrics is presented. In order to simulate the attacks and the countermeasures, a CWSN simulator [17] has been used. This simulator has been developed over the well-known Castalia simulator [18]. Our modifications improve Castalia and include new cognitive features. The CWSN simulator responsibilities are scenario definition, simulation of the spectrum state, communications between nodes, and implementation of cognitive behaviors, attacks, and countermeasures.

Ten scenarios have been executed in the simulator to extract results and to draw conclusions from the work. The scenarios have some common characteristics.

(i) The scenario area is a 50 m × 50 m square.

(ii) The complete simulation time is 100 seconds.

(iii) The number of nodes in the simulation varies between 4 and 53, including one emitter node (S), one destination node (D), one eavesdropper attacker (E), and a variable number of secondary users that implement the relay and the jamming functions (R).

(iv) The emitter node sends 1 packet/s.

(v) The attack starts at the beginning of the simulation.

(vi) The eavesdropper nodes sense each channel for 50 ms. If in this time they do not detect a signal, they change to the next channel. However, if a signal is detected the eavesdropper will listen to the same channel for five seconds.

The variable parameters in the scenarios are as follows:

(i) the number of relay nodes (R),

(ii) the power transmission of the relay nodes (R),

(iii) the power transmission of the emitter node (S).

We have developed some graphics that summarize the results. In Figure 1, SOP for different emitter and noise power is presented. The number of nodes in the simulation is (7), including one source user, one destination node, and one eavesdropper in a 50 × 50 meters scenario. As we can see in the graph, there is a zone that provides the optimal relation between security SOP metric and noise power. Less noise power implies higher SOP rates. More noise power does not improve the security enough, and it affects the energy consumption and the spectrum performance.

In order to determine the influence of collaboration nodes over the network behavior, a new scenario has been simulated. Using the same 50 × 50 meter zone, the number of nodes in the simulation is 23, including one source user, emitting 1 packet/s, one destination, and one eavesdropper with 20 jamming nodes, emitting a rate between 1 and 1.1 packet/s. The shape in Figure 2 is similar to the one in the previous scenario. For high noise power the SOP level is lower than the one with 5 jamming nodes, between 2 and 5%, depending on the transmission power. This SOP is maintained for very low noise power, beyond 0.1 mW. There is also a zone where the relation between emission and noise power is optimal. This zone is shown in Figure 2.

Once the technique has been validated for security reasons and the results have been analyzed, the optimization and the impact in energy consumption should be analyzed. The next results show the energy optimization that consists of searching for the minimum resource utilization in order to achieve the security goals.

Figure 3 represents the additional power consumption that the jamming nodes introduce into the network. As we can see, there is almost no dependence between the emitter power and the power consumption of the jamming nodes. The quadratic form of the curve is derived from the omnidirectional antenna that simulates the nodes, with a circular range. The number of nodes affected by the transmissions of the others increases with r^2. In Figure 3 it can be appreciated that the network without using the noise technique has an energy consumption over 65 joules. This value can be increased to 250 Jules if the sensors that emit noise transmitted 1 mW. This is an additional energy consumption of more than 350%.

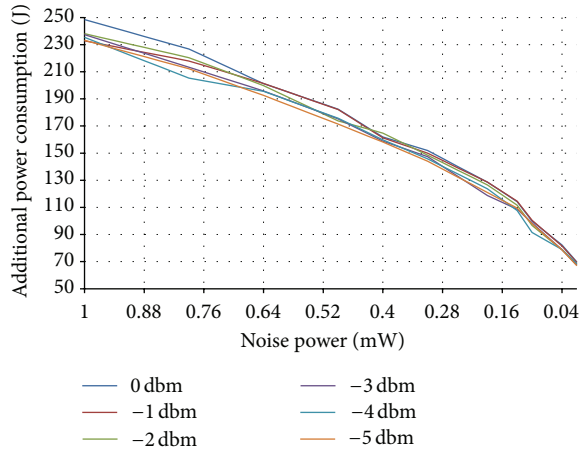

Figure 3: Additional power consumption in the network with 20 jamming nodes.

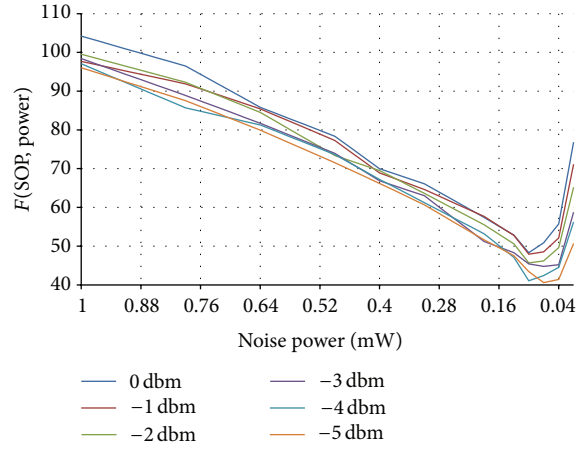

Figure 4: Jamming power variable. Function of SOP and additional power with $A = 1$ and $B = 1$.

If we can weigh the security and the consumption of the system, a formula similar to the next one will be a good solution:

$$F(\text{SOP}, \text{POWER}) = A \cdot \text{SOP} + B \cdot \text{POWER}, \quad (6)$$

where POWER is the additional consumption ponderated to 100 like the SOP. A and B are the weights that the designer can control to give more importance to the security or the power consumption. Depending on these weights, Figure 4 has a different minimum. Figure 4 represents formula (6) with $A = 1$ and $B = 1$. Table 3 summarizes some optimum results for different values of A and B. As we can appreciate, using a power noise transmission of 0.07 mW, the SOP can be reduced to 4.5% in the best case.

A different approach is to modify the number of jamming nodes keeping the jamming power constant. Figure 5 shows the SOP for different simulations with a variable number of jamming nodes, from 1 to 19. As in the previous simulations, there is a zone where the SOP is very high, when the number

Table 3: Optimum values for different weights.

A	B	Pjamming	SOP	Power
1	3	0,01 mW	48,8%–23,76%	69 J
1	2	0,04 mW	22,6%–11,73%	77 J
1	1	0,07 mW	11%–4,5%	95 J
3	1	0,1 mW	8,1%–4%	100 J
10	1	0,19 mW	5,6%–3%	128 J

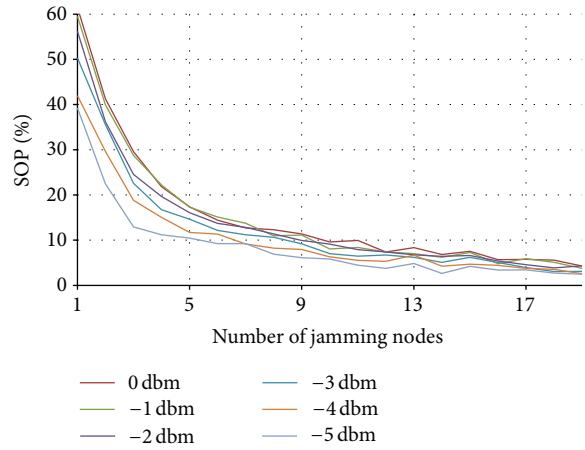

Figure 5: SOP for different number of jamming nodes.

of jamming nodes is low, and a zone where the SOP does not decrease a lot, with more than 5 nodes.

The additional power consumption has a quadratic form, similar to that in Figure 3. It increases with the number of jamming nodes. If we create the same formula as in the first experiments, the results are shown in Figure 6.

A conclusion extracted from Figure 6 is that the use of more than 5 jamming nodes does not provide improvements in the optimizer function.

Figure 7 represents the curves for different values of A and B when we select a constant emitter power of 0 dBm. It can be seen that if the security (A) has more weight in the formula than the consumption (B), the minimum solution requires a higher number of jamming nodes. It can be observed that the optimal solutions for the weights represented in Figure 7 are between 3 and 7 jamming nodes. This indicates that increasing the number of jamming nodes makes the network consume more energy without benefits in security.

Finally, to complete the analysis with power consumption, we have simulated a new scenario in order to analyze the behavior of the system when spectrum saturation is higher. In this case, the simulation has 10 emitter nodes transmitting 10 packets/s. This is 100 times more traffic than in the previous simulations. We have observed that the results have a similar distribution with the difference that in this case the SOP decreases drastically. However, this is due to the attack model in which the listening time in a channel with signal is much longer than the sensing time for each channel. This is an important result because spectrum efficiency is the most important goal of cognitive radio. If this approach

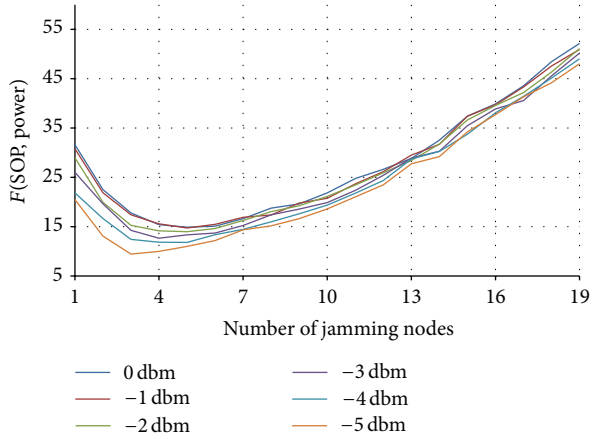

Figure 6: Number of jamming nodes variable. Function of SOP and additional power with $A = 1$ and $B = 1$.

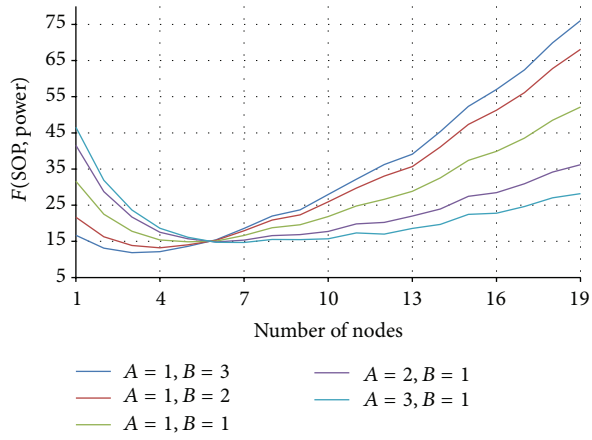

Figure 7: Number of jamming nodes variable and emitter power 0 dBm. Function of SOP and additional power with different values of A and B.

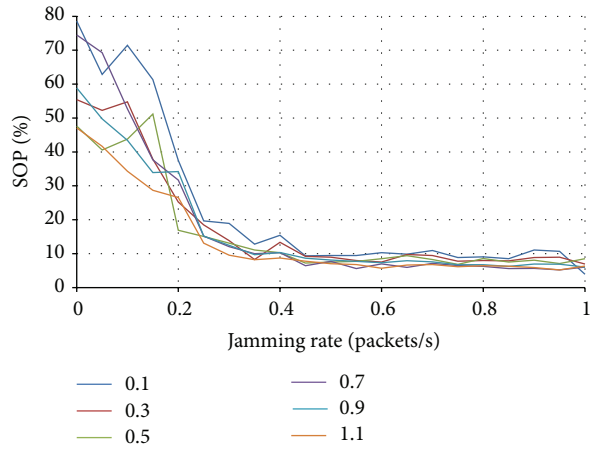

Figure 8: SOP for different emitter and jamming rates.

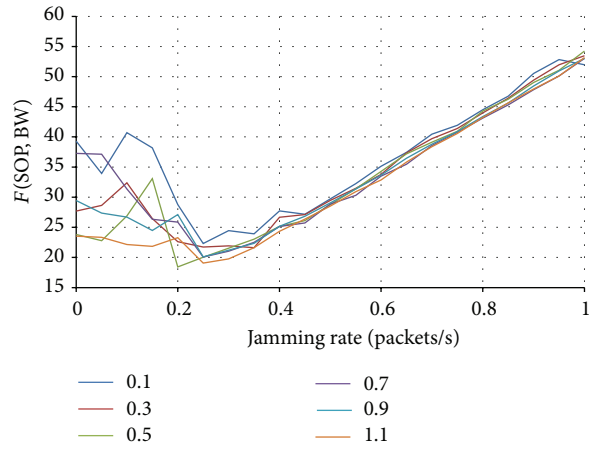

Figure 9: Function of SOP and jamming rate with $A = 1$ and $B = 1$.

significantly affects the spectrum occupancy, it would not be feasible.

A similar analysis has been made with spectrum utilization. This is an important resource that cognitive radio tries to use in a more efficient way. Therefore, this approach should be analyzed in order to have the minimum possible affect.

Figure 8 shows the SOP results for a variable jamming and emission rate. As we can appreciate, for low jamming rates (<0.2 packets/s) the SOP decreases quickly, but for higher values (>0.4 packets/s) the SOP is constant. This indicates that the optimum value in order to preserve the spectrum will be between 0.2 and 0.4 packets/s.

Figure 9 shows the conclusions specified before. Here, as in the power consumption experiments, an objective function is represented by (7). The figure shows that the optimal jamming rate for all the simulated scenarios is between 0.20 and 0.30 packets/s when $A = B = 1$. To increase the jamming rate above 0.30 packet/s costs more spectrum saturation than security benefits:

$$F(\text{SOP}, \text{POWER}) = A \cdot \text{SOP} + B \cdot \text{BW}. \quad (7)$$

Finally, Figure 10 and Table 4 show the optimum values for the objective function when the emission rate is constant and the weights A and B change. Here have been analyzed low packet rates, under 1 packet/s. The SOP rates are under 10% with a jamming rate over 0.45 packet/s.

6. Discussion and Conclusion

In this paper, we present an evaluation and energy consumption optimization and spectrum scarcity analysis of a cooperative artificial noise injection strategy for physical-layer security in multiuser cognitive wireless sensor networks as a supplement to encryption at higher layers. The generation of artificial noise makes the extraction of information from the spectrum difficult but also complements the upper layers security mechanisms, such as cryptography, making more difficult the decryption process of a noisy signal. According

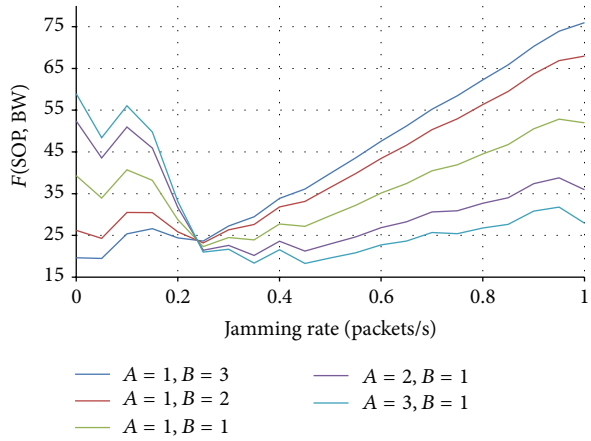

Figure 10: Function of SOP and jamming rate with different values of A and B and emitter rate 0.1 packets/s.

Table 4: Optimum values for different weights with jamming rate variable.

A	B	Jamming rate	SOP
1	3	0,05 pps	62,8–41,6%
1	2	0,25 pps	19,6–11,1%
1	1	0,25 pps	19,6–11,1%
2	1	0,35 pps	12,8–8,2%
3	1	0,45 pps	9,35–77,75%

to the CWSN scenario it is necessary to optimize the noise generation. Because of the CWSN nature noise affects power consumption and spectrum occupancy.

Cooperative artificial noise strategies with assistance from external helpers or inactive neighboring nodes are seen to be highly effective for increasing the secrecy of the transmitted data. Of course, a trade-off between energy consumption (additional sensor power consumption spent on transmission of noise), spectrum scarcity, and security level is necessary.

A cognitive simulation framework has been used to simulate the different scenarios. The eavesdropper attack model is always the same. The work is focused on the artificial noise strategy and energy optimization but in the future it will be interesting to hold a study with different attack models.

From the simulation results, we showed that there are different optimum solutions according to an objective function with different weights for energy consumption, spectrum scarcity, and security.

References

[1] J. Huang, G. Xing, G. Zhou, and R. Zhou, "Beyond co-existence: exploiting WiFi white space for Zigbee performance assurance," in *Proceedings of the 18th IEEE International Conference on Network Protocols (ICNP '10)*, pp. 305–314, October 2010.

[2] J. Mitola III and G. Q. Maguire Jr., "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[3] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, 2011.

[4] J. Mao, G. Xie, J. Gao, and Y. Liu, "Energy efficiency optimization for cognitive radio mimo broadcast channels," *IEEE Communications Letters*, vol. 99, pp. 1–4, 2013.

[5] A. Sultan, "Sensing and transmit energy optimization for an energy harvesting cognitive radio," *IEEE Wireless Communications Letters*, vol. 1, no. 5, pp. 500–503, 2012.

[6] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proceedings of IEEE International Symposium on Information Theory (ISIT '06)*, pp. 356–360, July 2006.

[7] C. Sperandio and P. G. Flikkema, "Wireless physical-layer security via transmit precoding over dispersive channels: optimum linear eavesdropping," in *Proceedings of Global Information GRID—Enabling Transformation Through 21st Century Communications (MILCOM '02)*, vol. 2, pp. 1113–1117, October 2002.

[8] X. Li and E. P. Ratazzi, "Mimo transmissions with information-theoretic secrecy for secret-key agreement in wireless networks," in *Proceedings of Military Communications Conference (MILCOM '05)*, vol. 3, pp. 1353–1359, October 2005.

[9] Y. Hwang and H. C. Papadopoulos, "Physical-layer secrecy in AWGN via a class of chaotic DS/SS systems: analysis and design," *IEEE Transactions on Signal Processing*, vol. 52, no. 9, pp. 2637–2649, 2004.

[10] G. Noubir, "On connectivity in ad hoc network under jamming using directional antennas and mobility," in *Proceedings of International Conference on Wired /Wireless Internet Communications*, Lecture Notes in Computer Science, pp. 186–200, Springer, 2004.

[11] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *Proceedings of Military Communications Conference (MILCOM '05)*, vol. 3, pp. 1501–1506, October 2005.

[12] T. H. Chang, Y. W. Hong, and C. Y. Chi, "Training signal design for discriminatory channel estimation," in *Proceedings of Global Telecommunications Conference (GLOBE-COM '09)*, pp. 1–6, IEEE, 2009.

[13] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[14] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, 2005.

[15] "CC2530—2.4 GHz System-on-Chip for ZigBee, RF4CE, Smart Energy applications," Texas Instruments, 2013, http://www.ti.com/ww/en/analog/cc2530/.

[16] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, 2010.

[17] J. Blesa, E. Romero, J. Vallejo, D. Villanueva, and A. Araujo, "A cognitive simulator for wireless sensor networks," in *Ubiquitous Computing and Ambient Itelligence*, 2011.

[18] A. Rastegarnia and V. Solouk, "Performance evaluation of Castalia Wireless Sensor Network simulator," in *Proceedings of the 34th International Conference on Telecommunications and Signal Processing (TSP '11)*, pp. 111–115, August 2011.