Cognitive radio-aided wireless sensor networks for emergency response

Stamatios Arkoulis, Dimitrios-Emmanuel Spanos, Socrates Barbounakis, Anastasios Zafeiropoulos and Nikolas Mitrou

Computer Networks Laboratory, National Technical University of Athens,
9, Heroon Polytechneiou Str., 15773 Zografou, Athens, Greece

E-mail: stark@cn.ntua.gr

Abstract. A lot of research effort has been put on Wireless Sensor Networks (WSNs) and several methods have been proposed to minimize the energy consumption and maximize the network's lifetime. However, little work has been carried out regarding WSNs deployed for emergency situations. We argue that such WSNs should function under a flexible channel allocation scheme when needed and be able to operate and adapt in dynamic, ever-changing environments coexisting with other interfering networks (IEEE 802.11b/g, 802.15.4, 802.15.1). In this paper, a simple and efficient method for the detection of a single operational frequency channel that guarantees satisfactory communication among all network nodes is proposed. Experimental measurements carried out in a real environment, reveal the coexistence problem among networks in close proximity that operate in the same frequency band and prove the validity and efficiency of our approach.
Keywords: Wireless Sensor Network (WSN), spectrum access, emergency, WiFi, Bluetooth, Coexistence Problem, 802.15.4, 802.11b/g, 802.15.1

1. Introduction

Wireless Sensor Networks (WSNs) have been recognized as one of the most promising technologies of our century [1]. Recent advances in microsensor technology have increased the availability of small, inexpensive, energy-efficient and reliable sensing devices carrying basic wireless networking capabilities and, thus, the WSN deployments worldwide. One class of applications that presents unique requirements and special challenges to the WSN design, concerns the response to emergency situations and hazardous incidents [2]. These applications are usually time critical and require the undertaking of immediate actions in case of an emergency event in order to repress the hazardous phenomenon. Thus, WSNs designed to function in emergency situations should meet some additional requirements "upon request", besides the typical ones that are associated with any WSN deployment.

An important aspect of WSN deployments that is often overlooked and can be proven critical in emergency response applications is the ability to operate and adapt in dynamic, ever-changing environments, where they may possibly coexist with other devices and WSNs operating in the same frequency band. We should point out here that the majority of WSN solutions proposed to the market are based on the IEEE 802.15.4 standard and operate in the unlicensed 2.4 GHz ISM band, where IEEE 802.11 and 802.15.1 networks operate as well. Besides the fact that its usage requires no governmental license, this band is also preferable due to its global availability, its sufficiently wide bandwidth that allows for more devices to operate in it simultaneously and its superior propagation characteristics compared to other

unlicensed bands. The previously mentioned problem is widely known as the Coexistence Problem [3] and has been both theoretically analyzed [4,5] and practically identified in real deployments [6,7]. We argue that an important feature that emergency WSNs should possess is the ability to dynamically discover a frequency channel that is able to provide acceptable communication quality among the nodes of the entire WSN, no matter how large its covering area is. Moreover, the process of dynamic channel discovery should not only be applied at the initial deployment of a WSN, but every time that a new network functioning in the same frequency band is deployed within the WSN field.

In this paper, a centralized method is proposed that turns the nodes of a WSN into "spectrum sensors", in order to detect which frequency channels are occupied by other devices' transmissions inside the deployment area and facilitate them to select a channel where an acceptable amount of interference is present and connectivity among all sensor nodes can be maintained. In order to apply the proposed method, a tool is designed and implemented that measures the Packet Error Rate for every network link and provides this information to a central entity for supporting channel selection decision. The tool is applicable to any TinyOS-compatible WSN.

The rest of the paper is organized as follows: in section 2 the coexistence problem among IEEE 802.15.4, IEEE 802.11b/g and IEEE 802.15.1 networks is detailed. Section 3 presents the related work and the motivation for the design of the proposed approach, while section 4 describes the designed algorithm and the implemented application. Section 5 confirms the coexistence problem in a real experimental setting, presents a fire detection use case that serves as a basis for a real demonstration of our approach, and discusses the experimental results. Finally, section 6 concludes the paper with a short summary of our work.

2. The Coexistence Problem

Modern WSNs operate in the unlicensed 2.4 GHz ISM band, applying the IEEE 802.15.4 (ZigBee) standard. IEEE 802.15.4 divides this band in 16 channels, each with a bandwidth of 2 MHz and a channel separation zone of 5 MHz. As shown in the middle row of figure 1, these channels are numbered from 11 to 26[1], covering the frequency band ranging from 2400 to 2483.5 MHz, while the carrier frequency for the i-th channel is given by the formula $f_{ci} = 2405 + (i - 11) \cdot 5$ (in MHz). Two WSNs deployed in the same area should operate in different, preferably non-adjacent, channels in order to avoid major co-channel interference. Unfortunately, IEEE 802.15.4 is not the only standard occupying the 2.4 GHz

[1] There are 11 additional channels numbered from 0 to 10 in the ISM 868/915 MHz band.

ISM band; both IEEE 802.11 and 802.15.1 standards operate in the same band as well.

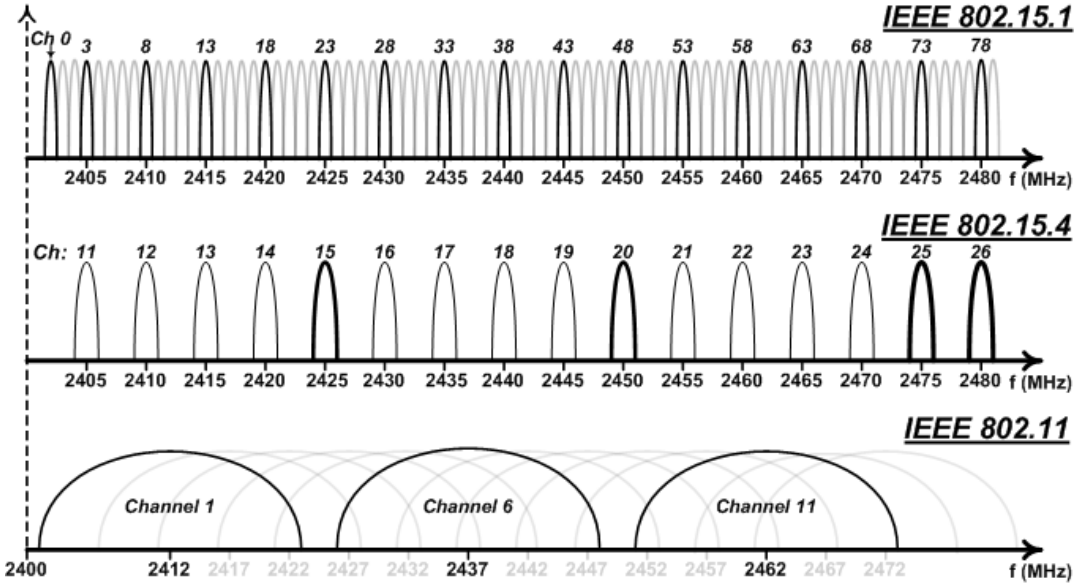


Figure 1. IEEE 802.15.1, 802.15.4 and 802.11b/g spectral maps.

On the one hand, the IEEE 802.11b/g (WiFi) standards define a total of 14 channels available in the 2.4 GHz band, numbered from 1 to 14, each with a bandwidth of 22 MHz and a channel separation zone of 5 MHz. These channels cover the entire 2.4 GHz ISM band ranging from 2400 to 2495 MHz, while the carrier frequency for the i-th channel is given by the formula[2]:

$$f_{ci} = \begin{cases} 2412 + (i-1)\cdot 5, & 1 \le i \le 13 \\ 2484 & , \ \mathrm{i} = 14 \end{cases} \text{(in MHz)}$$

According to the WLAN standards, adjacent channels overlap and signals sent over them interfere with each other. In fact, the IEEE 802.11b standard recommends the use of non-overlapping channels, namely 1, 6 and 11 for North America and 1, 7 and 13 for Europe, whereas this separation is ignored in practice and channels 1, 6 and 11 are the ones most commonly used worldwide.

On the other hand, the IEEE 802.15.1 (Bluetooth) standard specifies 79 channels in the 2.4 GHz band, each with 1 MHz bandwidth and a channel separation of 1 MHz. The carrier frequency for the i-th channel ($0 \le i \le 78$) is specified by the formula: $f_{ci} = 2402 + i$ (in MHz). It should be noted that the operating channel for Bluetooth is not fixed, but according to the IEEE 802.15.1 standard recommendations, frequency hopping is employed. Bluetooth devices have to hop in a pseudo-random manner among the 79 defined channels at about 1600 times a second, and consequently each transmission practically occupies the entire

[2] In North America, regulatory authorities prohibit the use of channels 12-14, restricting WLAN operating frequencies under 2473 MHz.

band, given that only small portions of that are occupied alternately for short periods of time. The spectral differences among the standards operating in the 2.4 GHz band are shown graphically in figure 1.

With today's steadily increasing application of the above standards, it is highly probable that in the near future, a number of different electronic devices operating in the same frequency band will be often co-located in the same area [3]. Currently, Wi-Fi and WSNs become even more popular, mainly due to the low value of service per cost that they offer, while Bluetooth devices are already commonplace. Hence, the problem of spectrum congestion and interference among different types of networks is constantly aggravated.

3. Related Work and Motivation

3.1. Related Work

Numerous approaches have been proposed so far for mitigating the interference problems caused to WSNs by spatially co-located networks which disorderly share the 2.4 GHz ISM frequency band. However, the majority of them are based either on unrealistic assumptions or on requirements that current off-the-shelf WSNs are unable to meet.

Some methods rely exclusively on the usage of special sensor devices or hardware modules to solve the coexistence problem, a requirement often expensive and not broadly available in off-the-shelf WSNs. In [8] and [9] directional and array antennas are utilized respectively, while in [10] the design of a robust to interference WSN radio chipset is presented. Approaches like [11] are developed on hybrid sensor nodes which should carry both a 802.11 transceiver for contenting with WiFi and a 802.15.4 one for communicating with other WSN nodes.

In other methods, such as in [12], centralized devices are responsible for managing the spectrum and allocating it in a non-conflicting manner. Similar distributed approaches are also proposed, e.g. the SM-MAC protocol [13], where the heterogeneous network nodes negotiate over a common control channel to make agreements regarding spectrum usage. However, synchronization and robustness issues as well as difficulties in detecting qualitative control channels in an area may affect both the efficiency and the viability of such approaches.

Alternative approaches are also proposed, such as [14] and [15], that handle interference by clustering problematic WSN nodes together and assigning a better channel to them, different from that of the entire WSN. Special border nodes are responsible for connecting the underlying cluster with the rest of the WSN by simply forwarding packets from and to its nodes. However, this could only be achieved if those nodes were either

equipped with multiple interfaces or able to switch their operating channel back and forth on a per time-slot [15] or per packet basis [14], requirements that increase cost, energy consumption and delays inside a WSN.

Methods like [16] mitigate interference by utilizing high level frequency hopping techniques. WSN nodes switch channels – together with their neighbors – on a per time-slot basis, following fixed or negotiated frequency hopping sequences. Thus, each pair of nodes communicate over different channels at every time-slot. Furthermore, in [17], a fictitious coordinator is assumed responsible for detecting interference and informing the WSN nodes to switch to a better channel, while in [18], every node randomly and independently selects a channel to operate in at each time period. However, as both delay and energy consumption of channel switching are non-negligible [19], the efficiency of such methods in terms of communication latency and resource consumption is doubtful.

Despite the breadth of the existing approaches, their application in real-life WSNs is extremely hard, mainly due to their costly requirements, the inherent restrictions of the current technological achievements as well as their simplifying assumptions (e.g. zero cost channel switching). On the contrary, real-world solutions so far focus on the detection of a qualitative channel for the WSN to operate in only during its initial deployment [20]. Such decisions are more often supported by site-surveys conducted in the deployment fields for assessing the impact of site morphology, nodes' locations, transceiver characteristics as well as interference from adjacent networks on the under consideration WSN. Although the most elegant way to conduct such site-surveys is to use spectrum analyzers, their cost and bulkiness render them unsuitable to support outdoor deployments which potentially cover large areas in harsh environments. Alternatively, portable commercial [21], or custom-made [22] channel scanning devices could be used for rapidly assessing all 16 channels defined by 802.15.4 standard in the 2.4 GHz frequency band and even measure the Packet Error Rate (PER) that a connection may potentially suffer if established at a given area. However, in both cases the conduction of complete site-surveys prior to a WSN deployment is expensive, time and resource consuming or even economically and practically infeasible in large, distant and hostile geographical areas. This statement is true especially in emergency cases, where time is a critical factor as well as the location is highly probable to be unreachable.

Furthermore, in emergency cases, it is also highly possible for some previously qualitative 802.15.4 channels to suddenly suffer from excessive external interference caused by newly deployed geographically overlapping networks operating in the same frequency ranges. As a result, the a priori selected channel may not be satisfactory anymore and the connectivity of the underlying WSN may become threatened. In such cases, a better frequency channel must be selected. This need has already been considered in newer versions

of popular standardized protocols, such as ZigBee PRO which has adopted the “Frequency Agility” feature, while so far ZigBee relied on its low duty cycle and collision avoidance algorithms to minimize data loss caused by such problems. However, this feature has not been fully implemented or standardized yet. Thus, there are still many open issues, with the most important one being the proposal of a method for the quick and efficient detection of qualitative channels in WSN's deployment fields. In order to handle this issue, a very limited number of approaches have been proposed to date including [23], [24] and [25]. However, since all these approaches require the usage of additional hardware for detecting a 802.15.4 qualitative channel, it is inevitable that the cost and energy consumption levels will increase, resulting in decreased efficiency. Finally, in [6] a channel estimation procedure is proposed for evaluating all 802.15.4 channels' quality over only a specific communication path, a limitation that renders this approach incapable of finding a globally qualitative channel for the entire WSN to operate in.

3.2. Motivation

In this paper, a method is proposed for mitigating interference caused to a WSN by either co-located WiFi, Bluetooth and WSN networks operating in overlapping frequency ranges or other external factors. The presented approach differs significantly from the work presented in section 3.1 as it does not rely on oversimplifying assumptions or on special hardware modules. Instead, it bears close resemblance to approaches that seek a channel that guarantees sufficient connectivity among the nodes of a WSN, without the need of manually conducted site surveys or monitoring architectures that necessitate the use of specialized hardware. The WSN nodes themselves are able to monitor the deployment area - either upon initialization or upon request - and detect the most sufficient channel that satisfies their communication needs. Since no firmware modification or special hardware is required, this solution may be applied on hardly any commercial WSN (although currently only TinyOS-enabled WSNs are supported). To this end, a tool is also designed that provides to a central entity (most probably a WSN’s gateway) information regarding the amount of interference that every WSN node is facing in each available frequency channel. This procedure is typically referred to as “Spectrum Sensing” in the context of Cognitive Radio technology.

The proposed solution would be extremely helpful in emergency cases where new, supportive WSNs should be rapidly deployed within tight time constraints that make the conduction of a detailed site-survey and the intervention of a network administrator unfeasible. Moreover, since the deployment of any supportive networks may alter the spectrum occupation map in a deployment field, the occasional detection of interference-free channels should help maintain connectivity among the nodes of the underlying WSNs. The

time between successive executions of the proposed tool is not formally modeled here, since it highly depends on the prevailing conditions in the considered deployment field. Indicatively, the execution of this approach may be triggered either by the WSN administrator who observes abnormal operation or excessive information loss, or even by special mechanisms like those recommended by the ZigBee PRO Stack. Such mechanisms keep track of both the number of transmitted packets by each transceiver and the received MAC level acknowledgments and, thus, are able to spot excessive failure rates and automatically trigger the appropriate corrective action.

4. The Proposed Solution

In this section, we describe our solution for the detection of a suitable operation channel for a newly or already deployed WSN in case of an emergency situation. As mentioned before, the problem of locating a single channel for the whole network to operate in is a challenging one, considering that WSNs are often deployed in wide areas where other networks may be in-range, especially in emergency cases. The rationale of our approach is to assess the quality of all links of a considered WSN for specific IEEE 802.15.4 channels, by turning its nodes to "spectrum sensors". Toward this direction, we calculate the PER value for every link of the network and proceed until an acceptable 802.15.4 channel is found.

4.1. Indicators of link quality

The quality of an IEEE 802.15.4 WSN link is mainly characterized by the Packet Error Rate (PER) value (equation 1), defined as the ratio of the number of packets that are not successfully received by a node divided by the number of packets sent to it over that link.

$$PER = \frac{\text{Number of lost packets} + \text{Number of packets received with CRC errors}}{\text{Total number of packets sent}} \quad (1)$$

As the computation of PER imposes considerable overhead to the underlying WSN, several other hardware indicators have been proposed for estimating it, with the most common of them being the Received Signal Strength Indicator (RSSI) and the Link Quality Indicator (LQI). However, recent studies [26, 27] have shown the inadequacy of both RSSI and LQI as reliable link quality indicators. In fact, it has been found that the correlation coefficients between these metrics and PER are significantly lower than 1 (0.433 and 0.731, respectively) [28], unless they are computed over several packet exchanges in order to mitigate variations in the RSSI/LQI readings, mainly caused by fading issues and the background noise. RSSI correlation with PER is also significantly affected when interference is present [29], since RSSI measures only the strength of the received signal, regardless of the surrounding noise, the precise estimation of which is often difficult. Thus, a low-strength signal in a noiseless environment presents lower RSSI than a high-strength signal in a noisy

environment, although the probability of a successful transmission in the latter case is higher. This is also demonstrated in experiments that have been conducted in rural as well as indoor environments [30, 31] and have shown that external interference is the main cause of unpredictable link behavior. Similar problems with RSSI arise when the signal strength at a receiver is close to its sensitivity level and link quality is highly unstable. In such cases, RSSI fails to account for this instability as it remains constant [7].

We should finally note that we do not rely on typical hardware-based approximations of PER since they take into account only 8 symbols of each packet as well as only the received ones. Therefore, in case a link suffers from excessive interference, they could underestimate the packet error rate value by not considering the number of lost ones.

4.2. Scanning Sequence of IEEE 802.15.4 channels

We argue that the order in which the IEEE 802.15.4 channels are going to be scanned is critical for the efficiency and execution time of our method. In fact, we chose to form a priority queue containing the 16 IEEE 802.15.4 channels in descending order according to their probability of being interference-free. This choice decreases both the number of channels examined before a suitable one is detected (in other words, the channel discovery time is decreased) as well as the inter-network communication overhead imposed by the procedure. This channel sequence is determined by the overlapping structure of the IEEE 802.15.4 and 802.11 spectral maps shown in the last two rows of figure 1. The IEEE 802.15.1 spectral map is not taken into consideration, because, as noted in section 2, a Bluetooth device does not occupy a limited portion, but the entire 2.4GHz ISM band, during its operation.

Based on this, we argue that IEEE 802.15.4 channels 25 and 26 are the most probable channels to be free of interference, since they do not overlap with any IEEE 802.11 channel, and they are usually referred to as “primary” channels. Note, however, that, although the use of IEEE 802.11 channels 12-14 by commercial devices is prohibited, there is always the possibility for a WSN to suffer from interference problems in these frequencies in case some other nearby WSNs are operating on channels 25 or 26. Similarly, IEEE 802.15.4 channels 15 and 20 - also referred to as “secondary” channels - correspond to frequency ranges that do not overlap with IEEE 802.11 most commonly occupied channels 1, 6 and 11. Again, although the IEEE 802.11 standard recommends the usage of only channels 1, 6 and 11 by all modern devices, there is no rule preventing a device from occupying another IEEE 802.11 channel. Therefore, the probability for these two channels to experience interference problems is low, but still non-negligible.

The IEEE 802.15.4 channels that follow in the priority queue are channels 11, 16, 21, 14, 19 and 24 in the order that they appear. It can be observed by simple inspection of figure 1

that these channels are located near the tails of IEEE 802.11 channels 1, 6 and 11. As it has been shown that there should be at least a 7 MHz offset between the operational frequencies of a IEEE 802.11 and a IEEE 802.15.4 channel for a satisfactory performance to be achieved [7], it is expected that IEEE 802.15.4 channels located near the tails of a WiFi channel suffer from less interference problems than those spanning across a WiFi channel's central frequency. Hence, the former ones are assigned a higher scanning priority than the latter ones. Regarding the relative order of these six "tail" channels, it should be noted that their sequence is not strictly assigned, as it cannot be known a priori which one has a greater probability of being interference-free (or at least, of limited interference). However, a rational assumption would be to first scan three "tail" channels that are not contained by the same IEEE 802.11 channel, followed by the remaining three.

The scanning sequence is completed with the rest of the IEEE 802.15.4 channels in no particular order, namely channels 12, 13, 17, 18, 22 and 23. These channels are the least probable to provide acceptable communication quality, as their frequency ranges contain the central channel frequencies of WiFi's most commonly used channels 1, 6 and 11.

4.3. Detection Algorithm

In this section, the proposed algorithm for optimal channel selection in a WSN is described in detail. In order to better illustrate the applicability of the algorithm, the network topology shown in figure 2 is used as a reference point. In this case, communication may be established among the gateway and the existing nodes either directly or via multi-hop paths.

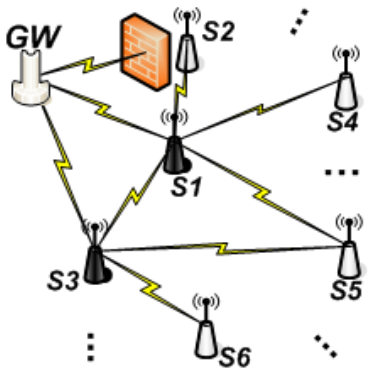


Figure 2. Indicative network topology.

The basic steps that are followed during the execution of the proposed algorithm are depicted in figure 3. Initially, the primary 802.15.4 channel that is examined is either the default operating channel of the under deployment WSN or the currently operating channel in case of an existing network, regardless of its actual position in the channel priority queue ChPrio. This channel is denoted as ChPrio[0] in figure 3, while ChPrio[i] ($1 \le i \le 15$) refer to the rest of the elements of the priority queue, excluding the aforementioned channel.

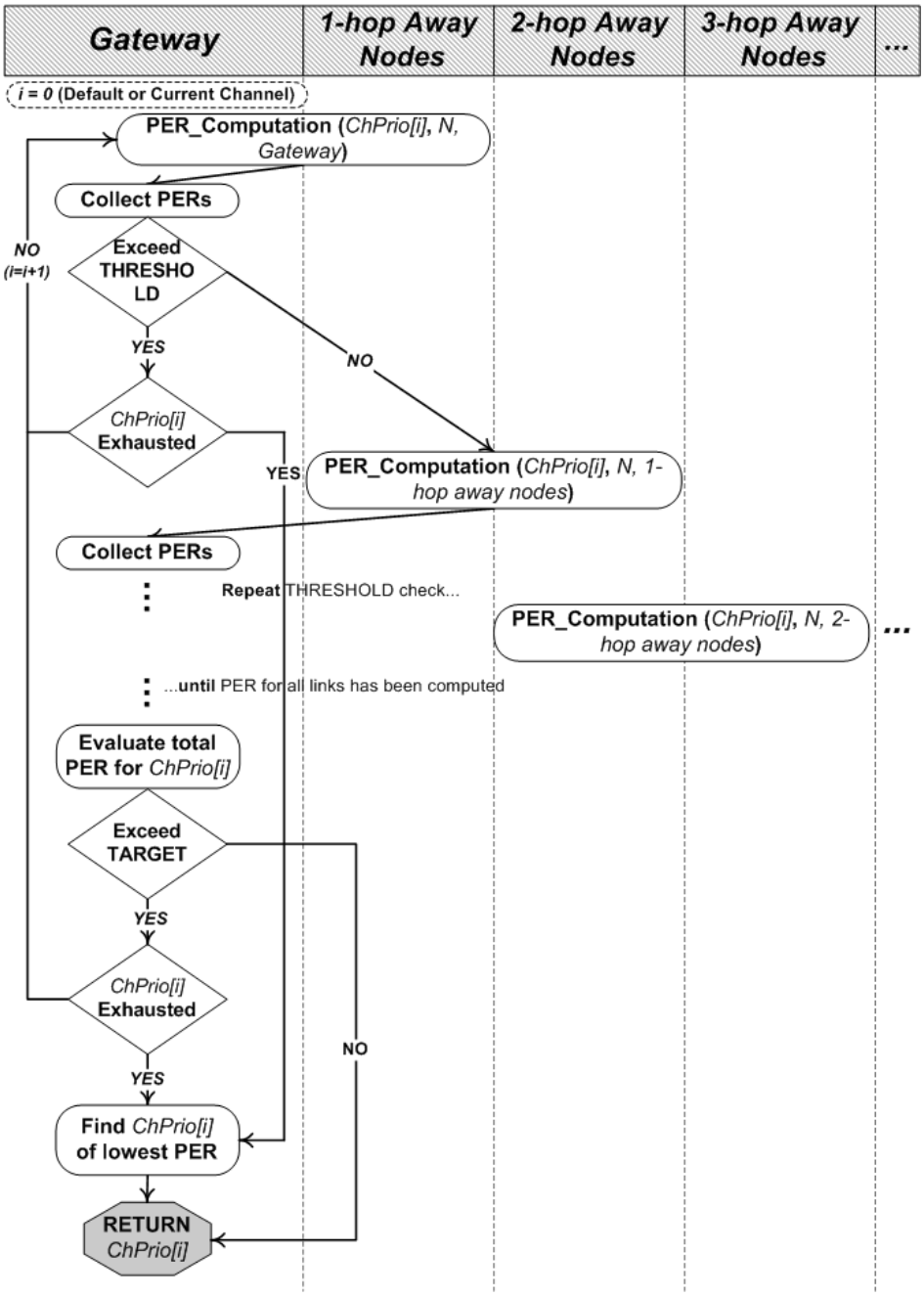


Figure 3. Algorithm steps.

The first step of the proposed algorithm is the computation of the PER for the links that interconnect the first node acting as Initiator, referred to also as Initial in the rest of this section, and the nodes that are within its transmission range (In-range nodes). In case of the topology shown in figure 2, PER is computed for the links between the gateway GW (Initiator node) and nodes S1 and S3 (In-range nodes). This calculation is performed by the PER_Computation function (see figure 4), which is a modified, tailored to our needs version of the TestRadio method [32]. PER_Computation receives as arguments the under examination frequency channel, the number of packets to be sent during the procedure, as well as the identifier of the Initiator node. Primarily, the Initiator node informs the In-range

nodes to switch to the appropriate channel. Each such node responds either with an acknowledgement for participation in the procedure, or with a negative acknowledgement in case the PER of the specified link has already been computed for this channel within a specified time period. Then, the Initiator node switches as well to the under examination channel and broadcasts a number of packets, while the In-range ones being engaged to participate in this procedure have to report back the number of successfully received packets. At the end of this procedure, the Initiator node is able to compute the PER values for each one hop away link.

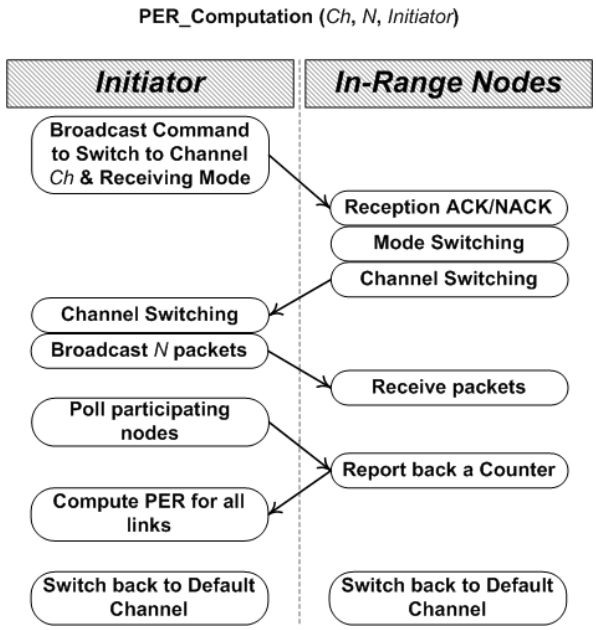


Figure 4. PER computation procedure.

After the computation of the PER values, the Initiator node sends them back to the Initial one (which is the gateway itself in figure 2) that is responsible to compare them with a specified threshold PER called *THRESHOLD*, above which communication quality is considered unacceptable. If there is at least one link with an unacceptable PER value, the channel is rejected and the next frequency channel is examined according to the ChPrio priority queue. This process is crucial since the algorithm is referring to emergency scenarios where connectivity has to be guaranteed between the Initiator and each WSN node. Furthermore, unnecessary PER calculations for the rejected channels in the rest network are avoided and significant network resources are preserved.

On the contrary, if all the examined links present acceptable PER values, the algorithm proceeds with the consideration of the remaining WSN links in a similar way (nodes more than three hops away from the gateway are not shown in figure 3). In this case, the In-range nodes of the existing Initiator nodes, undertake sequentially the role of the Initiator and compute the PER values for their In-range nodes. For example, in the considered topology in figure 2, nodes S1 and S3 become sequentially Initiator nodes. The sequential

order is imposed in order to avoid interference caused by simultaneous transmissions in the same channel. Upon completion of the PER values estimation from an Initiator node, these values are forwarded to the Initial node (the gateway in case of the topology in figure 2). A timeout value has also to be specified for the PER values estimation by each Initiator node. In case of no response within the specified time period, the process has to be repeated for this node.

In order to coordinate the definition process of the active Initiator node, a tree based representation is used where the parent node is responsible to provide sequentially the capability for PER values computation to each child node. Furthermore, by using the negative acknowledgement feature of the PER_Computation function, possible loops in the computation during the selection of different initiator nodes are avoided. Finally, the sequence of the PER_Computation function calls in the indicative network topology of figure 2 are shown in figure 5, supposing that all the computed values are below the aforementioned threshold PER, so as no link assessment is pruned.

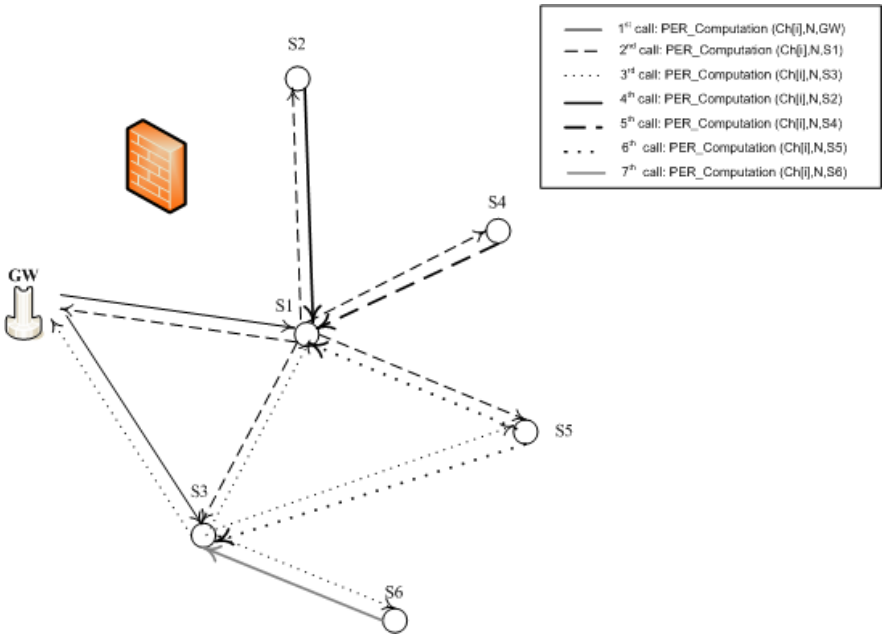


Figure 5. Map illustrating the sequence of function calls.

As soon as the PER values in a specific channel for all WSN links are computed and sent back to the Initial node (the gateway in the topology shown in figure 2), they are compared to a target constant PER value called *TARGET*, that represents the required communication quality. If all computed values are below this target PER, then the current frequency channel is selected as a suitable one for the considered topology and the execution of the algorithm is stopped. Otherwise, the same procedure is executed for the next channel in the priority queue ChPrio. In case all 802.15.4 channels of ChPrio are checked, but none satisfies the target PER condition, the one with the lowest mean PER among all WSN links is selected. Obviously, various alternative selection policies may be applied at this point: for

example, one could opt for the channel where the maximum PER among all WSN links is minimized. It should be noted that the *THRESHOLD* and *TARGET* parameters and the timeout periods mentioned above are considered constant and defined a priori, according to each application's requirements in terms of link quality and nodes' connectivity. However, the above parameters can vary among consecutive execution cycles of our algorithm adapting to the possible variations in the interference levels. This adaptation may be performed manually by a network administrator or using self-learning techniques the description of which is considered out of scope for the present work.

5. Measurements

5.1. Experimental validation of the Coexistence Problem

The theoretical foundations of IEEE 802.15.4-based WSN's performance under IEEE 802.11 and IEEE 802.15.1 interference have been laid in [4,5]. Furthermore, numerous practical studies [6,7] have examined the coexistence problems of 802.15.4 WSNs with 802.11b/g and 802.15.1 networks. However, to the best of our knowledge, considering Packet Error Rate (PER) as the main performance indicator of real-life WSNs' operation under the interference of 802.11 as well as 802.15.1 networks has not been extensively studied yet. Little existing work is also available for the interference that is caused between WSNs that operate in the same area and in the same channel. In this subsection, specific measurements are presented that demonstrate the existence of interference at 802.15.4 WSNs from 802.11b/g, 802.15.1 networks and 802.15.4 WSNs, in terms of PER. These measurements are considered necessary in order to highlight in practice the need for the application of the proposed algorithm, as well as empower the validation scenario described above.

Table 1 shows the equipment used during the experiments, while the topology of the testbed is shown in figure 6. The behavior of PER being present at a Sensor Node when receiving packets from another one (a Gateway in this case) is evaluated under the existence of interference from various sources. The transmission range of both nodes is 30 meters, while their transmission power varies from -24dBm to 0dBm. Both nodes utilize the Clear Channel Assessment (CCA) mode 1 technique [33]. In all the conducted experiments, both Gateway and Sensor Node are placed within one meter from the ground and interference is introduced from IEEE 802.11, 802.15.4 and 802.15.1 devices being placed in variable distances from the latter. Interference is caused through exchange of files in case of 802.11 (PCI Wireless Cards) and 802.15.1 devices (Bluetooth dongles), and continuous exchange of packets in case of coexisting WSNs. All interfering networks transmit at the maximum power that is supported by their hardware, as it is shown in table 1. Finally, PER computation for the

Sensor Node is done by executing the PER_Computation function (see figure 4) with arguments $Freq = 22$ (for examining the PER at IEEE 802.15.4 channel 22) and $N = 100$, while the Gateway undertakes the role of the Initiator.

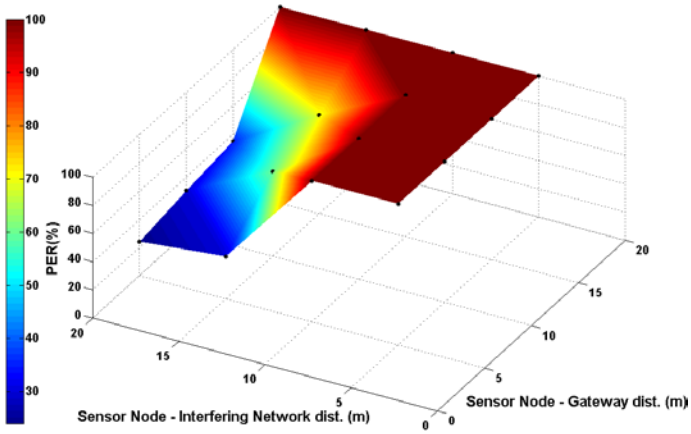
Table 1. Equipment used in the experiments.

	Imote2 Sensors	Bluetooth Dongles	Intel PRO /Wireless 2200BG NIC
Frequency	2400.0 – 2483.5 MHz	2400 – 2483.5 MHz	2400-2483 MHz (DSSS-OFDM)
Processor	PXA271 XScale® Processor at 13–416MHz	-	-
Memory	256kB SRAM, 32MB FLASH, 32MB SDRAM	-	-
Chassis	Thin, plastic film bags	Laptop/Netbooks	Laptop/Netbook
Radio	Integrated 802.15.4 Radio	Bluetooth Class 2	802.11g
Antenna	Integrated 2.4GHz Antenna	2dBi PCB Antenna	Integrated 2.4GHz Antenna
Transmission Power	-24 – 0 dBm	Class 2	20dBm
Transmission Rate	250 Kb/s	3 Mb/s	54 Mb/s
Transmission Range	30 m	10 m	30 m
Power Supply	Imote2 Battery Board	USB	Battery

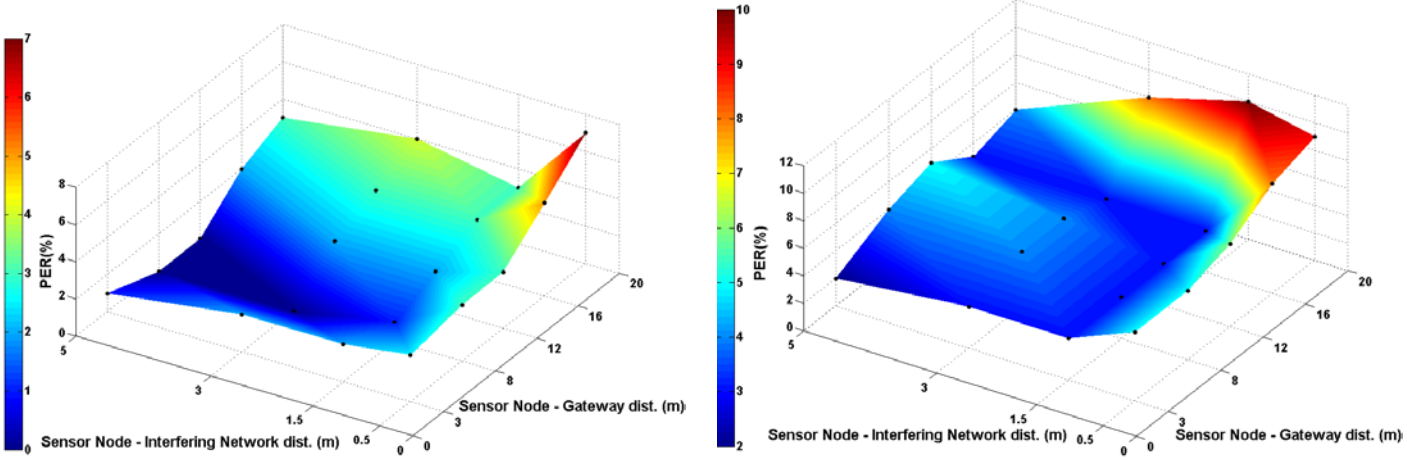
Figure 6. Testbed Topology.

The experimental PER results regarding the interference caused to the 2-node WSN operating in channel 22 from the considered interference sources are presented in figure 7, for various distances between the *Sensor Node – Gateway* and the *Sensor Node – Interfering Network*. For every interference source, two transmission power levels are considered for our 2-node WSN: 0 dBm and -10dBm. In figure 7(a) interference is caused by an adjacent 802.11

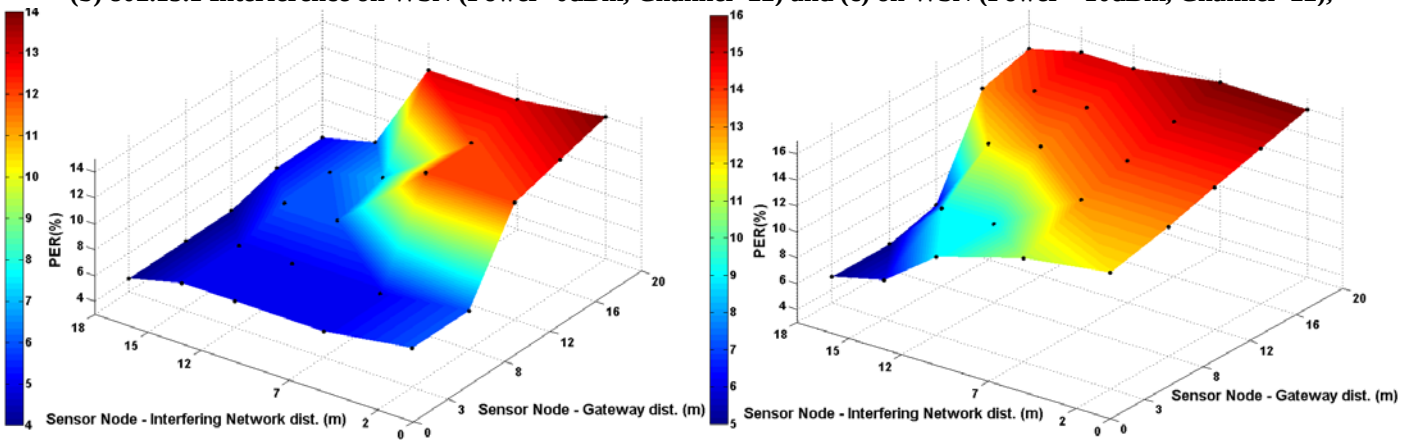
network, in figures 7(b) and 7(c) interference is caused by a 802.15.1 network, while in figures 7(d) and 7(e) interference is caused by another co-located 802.15.4 network transmitting at 0dBm and also operating in channel 22. In the case of interference caused by an adjacent 802.11 network, results are not shown for the -10dBm case, since all the PER values are 100%. This means that either no successful packet transmission from the Gateway to the Sensor Node was achieved during the PER_Computation function's execution or the required by this function synchronization failed due to severe interference problems.



(a) 802.11 Interference (Power=20dBm, Channel=11) on WSN (Power=0dBm, Channel=22),



(b) 802.15.1 Interference on WSN (Power=0dBm, Channel=22) and (c) on WSN (Power=-10dBm, Channel=22),



(d) 802.15.4 Interference (Power=0dBm) on WSN (Power=0dBm) and (e) on WSN (Power=-10dBm)

Figure 7. PER values under interference from IEEE 802.11, 802.15.1 and 802.15.4 networks.

From figure 7, it is shown that in all cases, the PER increases while the distance between the Sensor Node and Gateway increases and the distance between the Sensor Node and the Interfering Network decreases. This is reasonable since the received power is greater closer to the Gateway and, thus, fewer messages are dropped, while greater interference is existent when the Interfering Network is closer to the Sensor Node. In addition to the distance of the Interfering Network from the considered WSN, PER is also influenced by the transmission power of the Gateway; as the latter decreases, PER increases. Furthermore, it is evident that the most important problems from interference are created from an 802.11 network, while the effect of the existence of another 802.15.4 WSN is much smaller. Finally, 802.15.1 devices create significant interference problems only when they are placed very close to the Sensor Node.

5.2. A Fire Detection Use Case

As a proof of concept for the proposed solution in section 4, we use our implementation in the context of a fire detection use case scenario that fits well with the concept of WSN-monitored emergency situations. Forest fires constitute a case of natural disaster that is present in an increasing number of countries all over the world, partly due to the latest climatic changes affecting the planet. They usually occur in sparsely inhabited areas, and as a result, both their detection and suppression tasks are extremely hard. Due to the nature of this phenomenon, fast and efficient detection of a wildfire is deemed as extremely important for its timely and successful suppression. Moreover, several fire detection systems give emphasis to post-disaster and rescue operations support and management, with the most representative example being the FireNet architecture [34]. According to this approach, firefighters should be equipped with sensors for providing a central node with data regarding the total time they participated in the fire rescue, their location, and their physical condition, as well as measurements regarding the environment they act in, including the humidity and temperature of the fire field, the wind speed, the density of the smoke, and so on. Such data could allow for optimal real-time firefighter assignments and simultaneously, for the protection of firefighters' life. In a similar fashion, approaches like [35] utilize WSNs for post-disaster human life or rare animal species detection and their efficient rescue. Unfortunately, the majority of the current forest fire detection systems[3] and relevant approaches in the literature [36-38] rely on the oversimplifying assumptions of a known

[3] Notable examples include Firewatch (http://www.fire-watch.de/), a surveillance and analysis system for the purpose of early fire detection and GeoMAC Wildfire Support (http://www.geomac.gov/), an online system for information support of fire personnel with respect to the location and extent of wildfires in the United States.

operating frequency channel, selected a priori, overlooking the possibility that other devices or networks may as well operate in the same geographic area, especially during emergency cases.

Our use case WSN topology is shown in figure 8. This topology supports all the required functionality for the realization of our scenario and suffices for showcasing the proposed algorithm. It consists of an already deployed small-scale WSN being assigned with the tasks of environmental data collection and early fire detection, while several other interfering networks are on-the-fly deployed when an emergency event suddenly appears. We should point out here that our methodology may also be applied in larger scale WSNs. Thus, the validation procedure in this paper is based on a small scale real-life topology that may be considered as a miniature of a larger real deployment.

Figure 8. Use Case WSN Topology.

The experiments were carried out in open space in a wooded area where no interference from wireless phones (DECT) or other devices operating in the 2.4 GHz band was present. We used the same equipment (see table 1) and assumptions (e.g. all nodes are placed at about one meter above the ground) with those presented in the previous subsection. As shown in figure 8, a gateway is placed in the center of the deployment area, while six other sensor nodes are placed in various distances from that, ensuring that each node can communicate with the gateway only, and thus a star topology is formed. The considered WSN operates at channel 26 of 802.15.4 protocol and no interference was present (PER at all links was 0%) at the deployment phase.

As stated before, when an emergency case appears, the on-the-fly deployment of several emergency response networks is usually triggered. In our case, six interfering

networks (namely, three WSNs, two 802.11 networks and one 802.15.1 network) were deployed in the considered geographical area. Figure 8 depicts both their operating frequency channels as well as their distance from our WSN's nodes. As a consequence, some 802.15.4 channels will no longer be usable due to severe interference problems. Table 2 depicts which channels are expected to face potential interference problems for the transmission links connecting the gateway with each of the six WSN nodes. This estimation is based on the theory presented in section 2 as well as in figure 1.

Prior to the emergency case, no interference was apparent and, thus, the PER in the operating channel (IEEE 802.15.4 channel 26) of the considered WSN was 0% for all links. However, after the deployment of the aforementioned networks, the spectrum occupation map changed radically. Figure 9 depicts the PER suffered by all WSN nodes over all available 802.15.4 channels, which is in full agreement with the theoretical results depicted in table 2 (in order to obtain this map, all 16 channels - for each node with the respective interfering networks being obviously active - were scanned using our proposed methodology while ignoring some special stopping conditions).

Table 2. Interference existence in each 802.15.4 channel.

Channel /Link	**IEEE 802.15.4 Channel**															
	11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**
N1					x	x	x	x								
N2	x	x	x	x												
N3																x
N4											x	x	x	x	x	
N5											x	x	x	x		
N6	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
GW																

Our goal is to apply the proposed methodology in order to detect with sufficient confidence (this is why we chose to compute the PER directly with equation 1 instead of estimating it based on some hardware indicator) a “qualitative” – in terms of interference – channel for the entire WSN to operate in, by scanning the least possible number of 802.15.4 channels. In our example, the *TARGET* and *THRESHOLD* parameters have been arbitrarily set to the rather strict values 5% and 15%, respectively. With the *TARGET* value being equal to 5%, the first assessed channel that achieves PER values in all WSN links lower than 5% is automatically considered “qualitative”, and our algorithm terminates suggesting the use of that channel. On the other hand, in case a simple WSN link shows PER value higher than 15%, the channel under assessment is automatically discarded and considered inappropriate for usage in the considering WSN. Although the latter check does not result in significant

benefits here, the pruning of several links that do not have to be considered in large multihop topologies would save a significant amount of network resources. Last but not least, when PER values in a channel lay inside the (*TARGET*, *THRESHOLD*) range, this channel's assessment is completed and the respective measurements are stored in the gateway for future retrieval, e.g. in a case when none of the 16 channels satisfied the *TARGET* threshold and hence, the best channel should be selected.

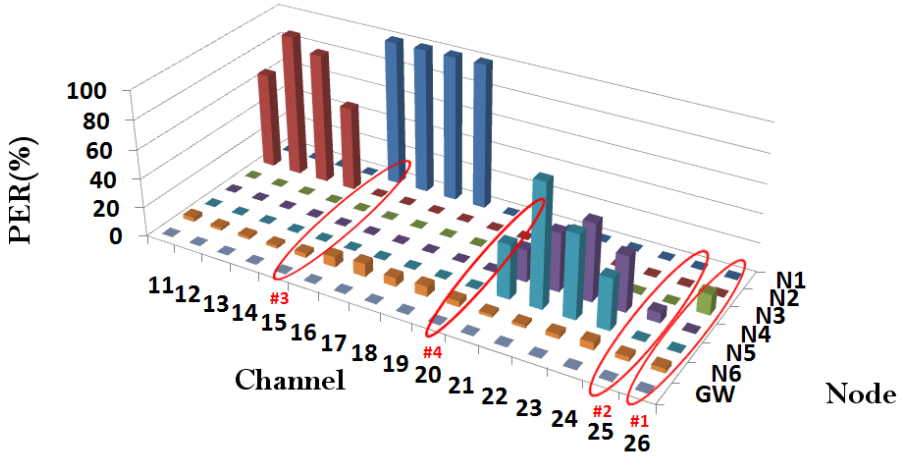


Figure 9. WSN Topology Spectrum Map.

Regarding our algorithm's execution sequence, channels 26 and 25 are firstly investigated, but none of them is considered satisfactory enough for the considered WSN as some links (i.e., those connecting the gateway with Nodes 3 and 4, respectively in the two cases) present a PER higher than 5%. However, since all PER values of all links in both cases are less than 15%, the extracted measurements are stored for future potential usage. Investigation continues with channel 15, which is unsatisfactory as well, since Node 1 is experiencing significant interference problems with PER values in some links to exceed even the 15% threshold. These collected measurements are completely discarded from the Gateway, while our algorithm's execution proceeds with channel 20. This channel is the first satisfactory channel to be found which is also perfectly acceptable, given that the PER values of all WSN's links are below the *TARGET* value of 5%. The complete spectral map of all 16 802.15.4 channels in figure 9 justifies this channel choice and reflects the accuracy of our algorithm.

What is important to note is that the proposed methodology accomplishes suitable channel detection in fewer steps than checking all 16 IEEE 802.14.5 in a sequential manner. The use of the scanning sequence imposed by the ChPrio queue resulted in checking only 4 of them, in comparison with the sequential scanning case where 10 channels would be checked instead (assuming that the first channel to be scanned is 802.15.4 channel 11). Reducing algorithmic iterations is considered important, since it leads into significant cost savings by

shrinking our algorithm's execution time and link checks. To make things clearer, in each channel inspection procedure in the topology shown in figure 8, the total number of packets transmitted is 253. 49 of these packets (19 control messages and 30 dummy packets for error rate computation) are transmitted during the execution of the PER_Computation function which is called by the gateway (playing the role of the Initiator) to compute the PER over all of its links with Nodes 1 to 6 (which act as In-Range Nodes). The rest 204 packets are transmitted during the six sequential calls of the PER_Computation function by each of the six WSN nodes for assessing the opposite direction of the aforementioned links over the considered channel. Since our algorithm requires the assessment of only 4 channels for detecting a qualitative channel for the underlying WSN to operate in, the total number of packet transmissions is $4 \cdot 253 = 1012$, while in case the sequential channel scanning was conducted, 10 channels would be assessed by transmitting $10 \cdot 253 = 2530$ packets. Furthermore, in case the *TARGET* and *THRESHOLD* parameters were not defined and, thus, no stopping conditions were defined for our algorithm, all 16 channels would be checked, resulting in $16 \cdot 253 = 4048$ packet transmissions. It is evident that our approach is more efficient regarding the use of existing network resources, compared with the sequential and the complete scanning approach. This reduction in the exchanged messages would be even more beneficial in large scale WSNs where each channel assessment iteration implies a large number of message exchanges among the nodes of the underlying WSN.

6. Conclusions

In this paper, the coexistence problem of IEEE 802.15.4, 802.11b/g and 802.15.1 networks is analyzed in detail and an efficient method for addressing this problem in the context of real-life WSN deployments is proposed and implemented. According to this method, an estimation of the existing interference in a WSN field is conducted by the participating sensor nodes and an operational frequency channel that guarantees satisfactory communication among all WSN nodes is detected. An important characteristic of the proposed approach is that it can be applied either at the initial deployment or during the lifetime of a WSN. It is argued that the described methodology is suitable for emergency response applications, since, in addition to the optimization in the operation of the WSN, it accomplishes suitable channel detection in few steps.

By conducting a set of experiments on a real testbed, we presented in practice the coexistence problem among the most common type of networks operating in the 2.4GHz ISM band, considering Packet Error Rate (PER) as the indicating parameter in terms of link quality assessment. In addition, we validated both the accuracy and the efficiency of the proposed algorithm in a real-life scenario.

Acknowledgments

Stamatios Arkoulis and Dimitrios-Emmanuel Spanos wish to acknowledge the financial support from “Special Account of Funds and Research, NTUA” and “Alexander S. Onassis Public Benefit Foundation” respectively, under their Scholarships Programmes.

References

[1] Chong C and Kumar S 2003 Sensor Networks: Evolution, Opportunities, and Challenges *Proc. of the IEEE* **91** 1247-56

[2] Lorincz K, Malan D J, Fulford-Jones T, Nawoj A, Clavel A, Shnayder V, Mainland G, Welsh M and Moulton S 2004 Sensor Networks for Emergency Response: Challenges and Opportunities *IEEE Pervasive Computing* 16-23

[3] Zhou G, Stankovic J and Son S 2006 Crowded Spectrum in Wireless Sensor Networks *Proc. of the 3rd Workshop on Embedded Networked Sensors (Em-Nets) 2006*

[4] Shin S Y, Choi S, Park H S and Kwon W H 2005 Packet error rate analysis of IEEE 802.15.4 under IEEE 802.11b interference *Proc. of WWIC 2005 (Springer)* 279–88

[5] Shin S Y, Kang J S and Park H S 2009 Packet Error Rate Analysis of ZigBee under Interferences of Multiple Bluetooth Piconets *Proc. of IEEE VTC ‘09*

[6] Musaloiu E R and Terzis A 2008 Minimising the Effect of WiFi Interference in 802.15.4 Wireless Sensor Networks *Int. J. of Sensor Networks* **3** 43–54

[7] Petrova M, Riihijarvi J, Mahonen P and Labella S 2006 Performance study of IEEE 802.15.4 using measurements and simulations *Proc. of 2006 IEEE Wireless Communications and Networking Conf. (WCNC)* 487–92

[8] Giorgetti G, Cidronali A, Gupta S and Manes G 2007 Exploiting Low-Cost Directional Antennas in 2.4 GHz IEEE 802.15.4 Wireless Sensor Networks *European Conf. on Wireless Technologies* 217-20

[9] Nakao Y, Watanabe K, Sato T and Kohno R 2007 A Study on Coexistence of WLAN and WPAN Using a PAN coordinator with an Array Antenna *SDR Forum Workshop '07*

[10] Seo H, Park Y, Park W, Kim D, Lee M, Kim H and Choi P 2008 System Design Considerations for a ZigBee RF Receiver with regard to Coexistence with Wireless Devices in the 2.4GHz ISM-band *KSII Transactions on Internet and Information Systems* **2** 37-50

[11] Hou J, Chang B, Cho D and Gerla M 2009 Minimizing 802.11 interference on ZigBee medical sensors *In Proc. of the Fourth int. Conf. on Body Area Networks’09*

[12] Ferrari P, Flammini A, Marioli D, Sisinni E and Taroni A 2008 Synchronized Wireless Sensor Networks for coexistence *In Proc. of IEEE Int. Conf. on Emerging Technologies and Factory Automation, 2008 (ETFA 2008)*

[13] Kwong K, Wu T, Michie C and Andonovic I 2007 A Self-Organizing Multi-Channel Medium Access Control (SMMAC) Protocol for Wireless Sensor Networks *Second Int. Conf. on Communications and Networking* 845-9

[14] Chulho W, Jong-Hoon Y, Ali H, Sharif H and Deogun J 2005 Adaptive radio channel allocation for supporting coexistence of 802.15.4 and 802.11b *IEEE Vehicular Technology Conf.* 2522-26

[15] Xu W 2007 Channel Surfing: Defending Wireless Sensor Networks from Interference *6th Int. Symp. Information Processing in Sensor Networks* 499-508

[16] Dust Networks, Inc., "Technical overview of time synchronized mesh protocol (TSMP)," http://www.dustnetworks.com/docs/TSMP_Whitepaper.pdf, 2006
[17] Yun J, Lee B, Li J and Hanr K 2008 A Channel Switching Scheme for Avoiding Interference of between IEEE 802.15.4 and Other Networks *Int. Multisymposiums on Computer and Computational Sciences* 136-9
[18] Pollin S, Ergen M, Timmers M, Dejonghe A, et al 2006 Distributed cognitive coexistence of 802.15.4 with 802.11 *1st Int. Conf. on Cognitive Radio Oriented Wireless Networks and Communications* 1-5
[19] Chen H, Cui L and Lu S 2009 An Experimental Study of the Multiple Channels and Channel Switching in Wireless Sensor Networks *Int. J. of Distributed Sensor Networks* (to appear)
[20] Barrenetxea G, Ingelrest F, Schaefer G and Vetterli M 2008 The Hitchhiker's Guide to Successful Wireless Sensor Network Deployments *In the 6th ACM Conf. on Embedded Networked Sensor Systems (SenSys 2008)* 43-56
[21] Jennic - Site Survey Tool, Jennic Microcontrolers, http://www.jennic.com/download_file.php?supportDocument=JN-AN-1014-Site-Survey-Tool-2v4.pdf (*accessed June 2010*)
[22] Liu H, Selavo L and Stankovic J 2007 SeeDTV: deployment-time validation for wireless sensor networks *In Proc. of the 4th Workshop on Embedded Networked Sensors* 23-7
[23] Gummadi R, Balakrishnan H and Seshan S 2009 Metronome: Coordinating spectrum sharing in heterogeneous wireless networks *1st Int. Conf. on Communication Systems and Networks* 1-10
[24] Gatani L, Re G L and Ortolani M 2005 Monitoring wireless sensor networks through logical deductive processes *IEEE Military Communications Conf.* 93-8
[25] Planning Site Surveys for 6LoWPAN deployments, Intel Corporation, http://edc.intel.com/Download.aspx?id=2583&returnurl=/Applications/Energy/Commercial-Energy-Monitoring-System/default.aspx (*accessed June 2010*)
[26] Jiménez V P G and Armada A G 2009 Field Measurements and Guidelines for the Application of Wireless Sensor Networks to the Environment and Security *Sensors* **9**
[27] Woo A, Tong T and Culler D 2003 Taming the underlying challenges of reliable multihop routing in sensor networks *Proc. of the 1st int. Conf. on Embedded Networked Sensor Systems (SenSys '03)* 14-27
[28] Tang L, Wang K-C, Huang Y and Gu F 2007 Channel characterization and link quality assessment of IEEE 802.15.4-compliant radio for factory environments *IEEE Transactions on Industrial Informatics* **3** 99-110
[29] Zhao J and Govindan R 2003 Understanding packet delivery performance in dense wireless sensor networks *In Proc. of the 1st int. Conf. on Embedded Networked Sensor Systems (SenSys '03)* 1-13
[30] Gokhale D, Sen S, Chebrolu K and Raman B 2008 On the Feasibility of the Link Abstraction in (Rural) Mesh Networks *Proc. of the IEEE INFOCOM 2008* 61-5
[31] Srinivasan K, Dutta P, Tavakoli A and Levis P 2010 An empirical study of low-power wireless *ACM Transactions on Sensor Networks* **6** 1-49
[32] Rice J A and Spencer Jr B F 2009 Flexible Smart Sensor Framework for Autonomous Full-scale Structural Health Monitoring *NSEL Report No. 18* (University of Illinois at Urbana-Champaign)
[33] CC2420 Data Sheet 2006, Texas Instruments

[34] Sha K, Shi W and Watkins O 2006 Using Wireless Sensor Networks for Fire Rescue Applications: Requirements and Challenges *IEEE Int. Conf. on Electro/information Technology* 239-44

[35] IEEE Humanitarian Technology Network, http://www.ieeehtn.org/htn/index.php/Life-Saving_Sensor_networks_for_post_disaster_applications (*accessed June 2010*)

[36] Hefeeda M and Bagheri M 2009 Forest Fire Modeling and Early Detection using Wireless Sensor Networks *Ad Hoc & Sensor Wireless Networks* **7** 169-224

[37] Yu L, Wang N and Meng X 2005 Real-time Forest Fire Detection with Wireless Sensor Networks *Proc. of the 2005 Int. Conf. on Wireless Communications, Networking and Mobile Computing* **2** 1214–17

[38] Son B, Her Y and Kim J 2006 A Design and Implementation of Forest-Fires Surveillance System based on Wireless Sensor Networks for South Korea Mountains *Int. J. of Computer Science and Network Security (IJCSNS)* **6** 124–30